

---

# Management Guide

## NetIQ® AppManager® for UNIX and Linux Servers

May 2019

## **Legal Notice**

For information about NetIQ legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see <https://www.netiq.com/company/legal/>.

**Copyright (C) 2019 NetIQ Corporation. All rights reserved.**

<b>About this Book and the Library</b>	<b>7</b>
<b>About NetIQ Corporation</b>	<b>9</b>
<b>1 Introduction to AppManager for UNIX and Linux Servers</b>	<b>11</b>
1.1 Key Benefits of AppManager for UNIX	11
1.2 What AppManager for UNIX Monitors	11
1.3 Understanding the AppManager Architecture	12
1.4 Setting Properties for UNIX Knowledge Script Jobs	14
<b>2 Installing AppManager for UNIX and Linux Servers</b>	<b>15</b>
2.1 System Requirements	16
2.2 Installing and Upgrading UNIX Agent Manager	18
2.3 Installing and Upgrading the UNIX Agent and Module	19
2.4 Applying Patches	24
2.5 Discovering UNIX and Linux Computers	25
2.6 Upgrading Knowledge Script Jobs	26
2.7 Uninstalling UNIX Agents and UNIX Agent Manager	28
<b>3 Working with AppManager for UNIX</b>	<b>31</b>
3.1 Management Sites	31
3.2 Understanding Communication Security Levels	32
3.3 Starting and Stopping the UNIX Agent	32
3.4 Changing Options for the Agent Computer and the Management Server	36
3.5 Saving UNIX Agent Information to a File	39
3.6 Managing Users in UNIX Agent Manager	40
<b>4 UNIX Knowledge Scripts</b>	<b>43</b>
4.1 Creating Filters with Regular Expressions	46
4.2 AIXLparUtil	47
4.3 ApplicationProcessMonitor	49
4.4 AsciiLog	51
4.5 CpuByProcess	54
4.6 CpuLoaded	55
4.7 CpuResources	58
4.8 CpuUtil	59
4.9 DNSConnectivity	61
4.10 DNSHealth	62
4.11 DNSReplication	63
4.12 DynamicFileSystemSpace	65
4.13 ExecUtil	66
4.14 FailedLogon	69
4.15 FileSystemSpace	71
4.16 FileSystemSpaceLC	72
4.17 FindFiles	74
4.18 GeneralCounter	76
4.19 HTTPHealth	79
4.20 LargeDir	80
4.21 LogicalDiskBusy	81
4.22 LogicalDiskIO	82
4.23 LogicalDiskIO26	83

4.24	LogicalDiskUtilization	83
4.25	MemByProcess	84
4.26	MemShortage	85
4.27	MemUtil	86
4.28	NetInterfacesCollision	89
4.29	NetInterfacesConnectivity	90
4.30	NetInterfacesDown	91
4.31	NetInterfacesErrors	93
4.32	NetInterfacesIO	94
4.33	OpenFiles	95
4.34	PagingHigh	96
4.35	PhysicalDiskBusy	97
4.36	PhysicalDiskIO	98
4.37	PhysicalDiskStats	100
4.38	PingMachine	101
4.39	PortHealth	103
4.40	PrinterQueue	104
4.41	PrivilegedProcs	105
4.42	ProcessDown	106
4.43	Processes	107
4.44	ProcessUp	108
4.45	RemoteProcessDown	109
4.46	Report_CPULoad	113
4.47	Report_DiskUsageSummary	115
4.48	Report_MemoryUtilization	119
4.49	Report_NetInterfacesIO	121
4.50	Report_SystemUpTime	123
4.51	Report_TopMemoryProcs	125
4.52	RunAwayProcs	127
4.53	RunCommand	128
4.54	SmartCPULoad	129
4.55	SmartMemoryStats	130
4.56	SmartPhysicalDiskStats	132
4.57	SwapLow	134
4.58	Syslog	135
4.59	SystemUpTime	138
4.60	TopCpuProcs	139
4.61	TopMemoryProcs	140
4.62	UserSessions	141
4.63	WAMAgentConfiguration	142
4.64	ZFSDataset	143
4.65	ZFSPoolHealth	145
4.66	ZFSPoolSnapshot	146
4.67	ZFSPoolStats	148
4.68	ZombieProcs	149

## **5 HardwareUNIX Knowledge Scripts 151**

5.1	HardwareUNIX Object Properties	151
5.2	AIXHWLog	155
5.3	Fan	161
5.4	LogicalDrive	163
5.5	PhysicalDrive	164

5.6	PhysicalMemory	165
5.7	PowerConsumption	166
5.8	PowerSupply	167
5.9	SmartArrayController	169
5.10	SolarisHWLog	170
5.11	Temperature	175
5.12	Voltage	176
<b>6</b>	<b>AMAdminUNIX Knowledge Scripts</b>	<b>179</b>
6.1	AgentHealthProxy	179
6.2	AgentInstallProxy	182
6.3	AgentUpdate	186
6.4	AgentUpdateSecurityLevel	189
6.5	SchedMaint	190
6.6	SetPrimaryMS	192
<b>7</b>	<b>Counter Reference</b>	<b>195</b>
7.1	Specifying Instances	195
7.2	UX Processor	196
7.3	UX Virtual Memory	198
7.4	UX Disk	199
7.5	UX Swapping	200
7.6	UX Paging	201
7.7	UX Block IO	201
7.8	UX Networking	203
7.9	UX NFS	205
7.10	UX File Access System	206
7.11	UX Terminal IO	207
7.12	UX System Calls	207
7.13	UX Processes	208
<b>8</b>	<b>Reporting with Reporting Center</b>	<b>211</b>
8.1	System Requirements for the UNIX Reports	211
8.2	Installing the UNIX reports on Reporting Center	211
8.3	UNIX Report Templates	212



# About this Book and the Library

The NetIQ AppManager product (AppManager) is a comprehensive solution for managing, diagnosing, and analyzing performance, availability, and health for a broad spectrum of operating environments, applications, services, and server hardware.

AppManager provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager, administrative staff can monitor computer and application resources, check for potential problems, initiate responsive actions, automate routine tasks, and gather performance data for real-time and historical reporting and analysis.

## Intended Audience

This guide provides information for individuals responsible for installing an AppManager module and monitoring specific applications with AppManager.

## Other Information in the Library

The library provides the following information resources:

### **Installation Guide for AppManager**

Provides complete information about AppManager pre-installation requirements and step-by-step installation procedures for all AppManager components.

### **User Guide for AppManager Control Center**

Provides complete information about managing groups of computers, including running jobs, responding to events, creating reports, and working with Control Center. A separate guide is available for the AppManager Operator Console.

### **Administrator Guide for AppManager**

Provides information about maintaining an AppManager management site, managing security, using scripts to handle AppManager tasks, and leveraging advanced configuration options.

### **Upgrade and Migration Guide for AppManager**

Provides complete information about how to upgrade from a previous version of AppManager.

### **Management guides**

Provide information about installing and monitoring specific applications with AppManager.

### **Help**

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

The AppManager library is available in Adobe Acrobat (PDF) format from the [AppManager Documentation](#) page of the NetIQ Web site.





# About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

## Our Viewpoint

### **Adapting to change and managing complexity and risk are nothing new**

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

### **Enabling critical business services, better and faster**

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

## Our Philosophy

### **Selling intelligent solutions, not just software**

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

### **Driving your success is our passion**

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

## Our Solutions

- ◆ Identity & Access Governance
- ◆ Access Management
- ◆ Security Management
- ◆ Systems & Application Management
- ◆ Workload Management
- ◆ Service Management

## Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>North and South America:</b>	1-713-418-5555
<b>Europe, Middle East, and Africa:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at [www.netiq.com/documentation](http://www.netiq.com/documentation). You can also email [Documentation-Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

## Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit [community.netiq.com](http://community.netiq.com).

# 1 Introduction to AppManager for UNIX and Linux Servers

The AppManager Suite provides comprehensive system and operations management capabilities to cover a wide range of applications, platforms, and devices. This chapter introduces the key benefits of using AppManager to monitor UNIX and Linux computers, a brief review of the AppManager architecture, and an overview of how the AppManager for UNIX and Linux (AppManager for UNIX) module works.

## 1.1 Key Benefits of AppManager for UNIX

AppManager for UNIX allows you to monitor and diagnose potential problems in your UNIX and Linux environments and integrate this information into the Operator Console or Control Center to provide a more complete view of your entire system.

With AppManager, you can gather performance, operation, and availability information for your managed systems, set thresholds for raising alerts, automate responses to system events, and view detailed information about your environment and server health through real-time and historical charts and reports.

Through the AppManager consoles, the information about your UNIX and Linux computers integrates with other important management information, such as the status of your Windows computers, the health of system services and processes, the operation of your mission-critical applications, and the performance of key hardware components. In addition, all of this detailed information can be stored in the AppManager repository, making it available for charts, service-level reports, trend analysis, and capacity planning.

Exception-based monitoring of server operation and performance keeps you up-to-date about new or potential problems while minimizing management overhead. AppManager provides broad support for monitoring both applications and hardware, giving you a complete picture of network resources, server status, and application availability.

## 1.2 What AppManager for UNIX Monitors

AppManager for UNIX monitors operating system performance to provide you with visibility into the overall health of your network and the current status of your UNIX and Linux computers.

For example, you can use AppManager to:

- ◆ Gather information about system statistics, such as CPU usage, processing time, queue lengths, memory usage, swap space, and I/O operations
- ◆ Monitor system and application log files to check for messages that indicate problems or alert you to critical conditions
- ◆ Monitor AIX and Solaris hardware log files to check for messages that indicate problems or alert you to critical AIX and Solaris hardware conditions
- ◆ Monitor hardware status on Dell and HP computers running Linux, such as fan speed (Dell and HP), physical memory (Dell and HP), power consumption (Dell), and Voltage probe status (Dell)

You can configure AppManager to send notifications in the console, e-mail the IT administrator, or automatically perform an action when the system performance degrades or the system generates critical messages.

With AppManager, you can proactively manage servers and applications across your enterprise by checking for critical conditions, or operational errors, such as:

- ♦ CPU, memory, or other system performance measurements that cross acceptable thresholds
- ♦ Logon failures that might indicate a security violation
- ♦ Network activity and communication failures
- ♦ Processes that are running as `root`, hung, stopped, or consuming the most CPU and memory
- ♦ Fan speed, power consumption, voltage probe, and physical memory changes that might indicate hardware failures

## 1.3 Understanding the AppManager Architecture

AppManager for UNIX support extends the standard operations management capabilities of AppManager to your UNIX and Linux environments. The AppManager for UNIX module includes an agent for the computer that you want to monitor, Knowledge Scripts you use to specify what you want to monitor, and console components to make managing your environment easier.

### 1.3.1 How AppManager for UNIX Works

When you install AppManager for UNIX on a UNIX or Linux computer, that computer becomes an **agent computer** (sometimes called a managed client) that you can monitor. The module includes several components that provide support for application monitoring, called **managed objects**. You can then run Knowledge Script monitoring jobs to manage your environment.

At regular intervals, the agent computer initiates communication with the **management server** to see if there is a new job to run, if the job status has changed (for example, to see if a job has been stopped), or if any of the job properties have been modified. If there is a new job or any changes to a job's status, properties, or schedule, the management server delivers the new job to the agent computer.

When a job is received from the management server, the UNIX agent component of the module runs the job at a regular interval to retrieve the information requested and then passes the information back to the management server. When the management server receives data or events from the agent computer, it processes the information and takes the appropriate action, for example, by raising an event if a specific threshold is met.

From the Operator Console or Control Center, the managed UNIX server is the same as any other managed computer, and the workflow through AppManager is the same as for any managed Windows computer if you want to respond to events, create charts, modify job properties, or run reports.

### 1.3.2 How the UNIX Agent Works

The NetIQ UNIX Agent includes the following components:

- ♦ NetIQ UNIX Agent Manager: A user interface that you can use to manage all your UNIX agents components across your enterprise. UNIX Agent Manager runs on Windows and Linux operating systems. You can store information about your agent computers in one UNIX Agent Manager server, then access the information through one or numerous UNIX Agent Manager consoles.

- ♦ The AppManager UNIX Agent: A component of the NetIQ UNIX Agent that enables support for AppManager and provides the managed objects for UNIX and Linux AppManager modules.
- ♦ Common components: Components that are shared by the AppManager UNIX Agent and the Security Agent for UNIX.

The key processes used by the UNIX agent are:

- ♦ **VigilEntAgent:** The process that UNIX Agent Manager uses to communicate with the common components of the agent. This process should run continuously once the agent is installed.
- ♦ **Agent:** The process that AppManger for UNIX uses to run Knowledge Script jobs. This process should run continuously once the agent is installed and configured to be used with AppManager.
- ♦ **Nqmagt:** The process that monitors the status of the other agent processes and restart them if necessary. This process should run continuously once the agent is installed.

### 1.3.3 Agent Heartbeat and Job Status

AppManager for UNIX sends a periodic **heartbeat** to the management server to determine if the jobs are operating properly and whether any new job information is available. When the agent computer contacts the management server, the management server identifies updates to any Knowledge Script jobs on the agent computer.

If job properties have changed or new jobs have been added since the last interval, the management server delivers the revised job information to the agent computer. If there is no change to the Knowledge Script job, the management server simply acknowledges the heartbeat, then waits for the next heartbeat signal.

Events and data returned by AppManager for UNIX are inserted by the management server into the standard AppManager workflow, so that events are displayed in the Operator Console TreeView or the Navigation Pane in Control Center, and data is stored in the AppManager repository in the same way that events and data are handled for Windows computers.

For information about creating and modifying Knowledge Script jobs, responding to events, and using collected data in charts and reports, see the *User Guide* for AppManager or the online Help.

### 1.3.4 Working with Multiple Management Servers

You can specify multiple management servers for each agent computer. However, you can only specify one primary and one secondary management server for each repository. If you define both a primary and a secondary management server, AppManager for UNIX periodically signals both servers but only accepts job requests from and sends data to the primary management server. The secondary management server can only submit job requests and receive data when communication with the primary management server is interrupted.

Agent installation prompts you to designate the management servers that can communicate with the agent computers. You can include management servers from multiple management sites. You can designate the primary and secondary management server for the agent computer either during installation or by running the `AMAdminUNIX_SetPrimaryMS` Knowledge Script.

### 1.3.5 Using UNIX Agent Manager

UNIX Agent Manager provides a server and console that allows you to view and manage all AppManager UNIX agent computers across your environment. You can use UNIX Agent Manager to remotely install, uninstall, or upgrade AppManager components on agent computers running UNIX or

Linux operating systems. UNIX Agent Manager provides a robust patch management system that allows you to apply or remove upgrades to the agent computers. You can also define users with limited access to view or change agents on specific computers. If you use UNIX agents for other products provided by NetIQ Corporation, the UNIX Agent Manager console allows you to manage those agents across multiple products.

## 1.4 Setting Properties for UNIX Knowledge Script Jobs

You start and configure UNIX Knowledge Script jobs exactly as you start and configure Knowledge Script jobs for other servers and applications, including setting the Advanced properties for event handling and data collection. Keep in mind, however, that not all of the UNIX Knowledge Scripts are applicable on all UNIX and Linux platforms. The Knowledge Script description in the Properties dialog box usually provides information about platform support if any platforms are not supported by that Knowledge Script or by a particular Knowledge Script parameter.

When you configure UNIX Knowledge Script jobs to run Actions in response to events, you can:

- ♦ Select the Action\_UXCommand Knowledge Script and configure it to run as a Managed Client Action to be performed on the UNIX agent computer.
- ♦ Select any other Action to run as a Management Server Action to be executed on the Management Server computer.

You cannot configure an action schedule for UNIX actions. The action runs in response to the first event raised.

# 2 Installing AppManager for UNIX and Linux Servers

This chapter provides installation instructions and describes system requirements for AppManager for UNIX and Linux Servers (AppManager for UNIX), which includes the AppManager UNIX agent (the UNIX agent). The information in this chapter describes how to install version 8.0 of the UNIX agent. However, the AppManager for UNIX module also supports the UNIX agent 7.5 and 8.1.0.11. This chapter includes instructions for using the module on all supported configurations.

This chapter assumes you have an AppManager repository, console, and management server installed. For more information about installing AppManager or about AppManager system requirements, see the *Installation Guide for AppManager*, which is available on the [AppManager Documentation](#) page.

To install AppManager for UNIX including the AppManager UNIX agent, complete the following checklist:

<input type="checkbox"/>	Ensure you have the necessary environment as described in <a href="#">Section 2.1, “System Requirements,”</a> on page 16.
<input type="checkbox"/>	Install or upgrade UNIX Agent Manager. Ensure you export your existing information before upgrading. For more information, see <a href="#">Section 2.2, “Installing and Upgrading UNIX Agent Manager,”</a> on page 18.
<input type="checkbox"/>	Install the agent on the computer you want to monitor (the agent computer). <ul style="list-style-type: none"><li>◆ For information about how to install on a local computer, see <a href="#">Section 2.3.3, “Installing Locally on a UNIX or Linux Computer,”</a> on page 20.</li><li>◆ For information about how to install using an answer file, see <a href="#">Section 2.3.4, “Silently Installing on the Agent Computer,”</a> on page 21.</li><li>◆ For information about how to install to one or more computers from the console, see <a href="#">Section 2.3.1, “Deploying the UNIX Agent Components Using UNIX Agent Manager,”</a> on page 19</li></ul>
<input type="checkbox"/>	Install agent updates that are applicable to your environment. For information about how to install patches to the console and the UNIX agent, see <a href="#">Section 2.4, “Applying Patches,”</a> on page 24. For a list of available hotfixes, see the <a href="#">AppManager Hotfixes for UNIX and Linux Operating Systems</a> page.
<input type="checkbox"/>	Install AppManager for UNIX on the repository and console computers, see <a href="#">Section 2.3.5, “Installing the Module on AppManager Repository and Console Computers,”</a> on page 24.
<input type="checkbox"/>	Begin managing your UNIX and Linux computers, see <a href="#">Section 2.5, “Discovering UNIX and Linux Computers,”</a> on page 25.

## 2.1 System Requirements

For the latest information about supported software versions, and the availability of module updates, visit the [AppManager Supported Products](#) page. Unless noted otherwise, this module supports all updates, hotfixes, and service packs for the releases listed below.

AppManager for UNIX and Linux Servers has the following system requirements:

Item	Requirement
AppManager repository, management server, and Control Center Console	8.0.3, 8.2, 9.1, 9.2, 9.5, or later
NetIQ UNIX agent installed on the computers you want to monitor (agents)	7.5 or later



Item	Requirement
One of following operating systems on the computers you want to monitor:	<p data-bbox="870 218 1089 239">One of the following:</p> <ul style="list-style-type: none"> <li data-bbox="894 275 1442 331">◆ CentOS on x86_32 or x86_64 (32-bit agent): 4, 5, 6, and 7</li> <li data-bbox="894 348 1442 405">◆ CentOS on x86_64 (64-bit kernel, 64-bit agent): 4, 5, 6, and 7</li> <li data-bbox="894 422 1442 478">◆ CentOS on Itanium (64-bit kernel, 64-bit agent): 4, 5, and 6</li> <li data-bbox="894 495 1442 552">◆ IBM AIX on IBM Power (32-bit kernel): 5.3, 6, and 7.1</li> <li data-bbox="894 569 1442 625">◆ IBM AIX on IBM Power (64-bit kernel, 32-bit agent): 5.3, 6, and 7.1</li> <li data-bbox="894 642 1442 699">◆ HP-UX on PA-RISC (64-bit kernel): 11.1x, 11iv2, and 11iv3</li> <li data-bbox="894 716 1442 772">◆ HP-UX on Itanium (64-bit kernel, 64-bit agent): 11iv2 and 11iv3</li> <li data-bbox="894 789 1442 846">◆ Oracle Linux on x86_32 or PowerPC (32-bit agent): 4, 5, and 6</li> <li data-bbox="894 863 1442 919">◆ Oracle Linux on x86_64 or PowerPC (64-bit kernel, 64-bit agent): 4, 5, 6, and 7</li> <li data-bbox="894 936 1442 993">◆ Oracle Linux on Itanium (64-bit kernel, 64-bit agent): 4, 5, and 6</li> <li data-bbox="894 1010 1442 1066">◆ Oracle Solaris on SPARC (64-bit kernel): 9, 10, and 11</li> <li data-bbox="894 1083 1442 1140">◆ Oracle Solaris on x86 (32-bit kernel): 10 and 11</li> <li data-bbox="894 1157 1442 1213">◆ Red Hat Advanced Server on x86_32, x86_64, or PowerPC (32-bit agent): 4, 5, 6, and 7</li> <li data-bbox="894 1230 1442 1287">◆ Red Hat Advanced Server on x86_64 or PowerPC (64-bit kernel, 32-bit agent): 4, 5, 6, and 7</li> <li data-bbox="894 1304 1442 1360">◆ Red Hat Advanced Server on Itanium (64-bit kernel, 64-bit agent): 4, 5, and 6</li> <li data-bbox="894 1377 1442 1434">◆ SUSE Linux Enterprise Server on x86, x86_64, or PowerPC (32-bit agent): 9, 10, 11, 12, and 15</li> <li data-bbox="894 1451 1442 1507">◆ SUSE Linux Enterprise Server on x86_64 or PowerPC (64-bit kernel, 32-bit agent): 9, 10, 11, 12, and 15</li> <li data-bbox="894 1524 1442 1581">◆ Ubuntu Linux: Ubuntu 16.04.2 LTS and Ubuntu 18.04 LTS</li> </ul>
Operating system components installed on any agent computer where you want to monitor hardware	<p data-bbox="870 1623 1422 1644">One of the following operating system components:</p> <ul style="list-style-type: none"> <li data-bbox="894 1677 1442 1766">◆ To monitor Dell equipment: all OMSA components. You install these components using the <code>srvadmin-all</code> meta package.</li> <li data-bbox="894 1782 1442 1887">◆ To monitor HP equipment: the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux.</li> </ul>

Item	Requirement
Microsoft SQL Server Native Client 11.0	11.3.6538.0 or later
(for TLS 1.2 support)	<b>NOTE:</b> The SQL Server Native client can be installed from this <a href="#">Microsoft download link</a> .

For more information, see the *AppManager for UNIX and Linux Servers Management Guide* on the [AppManager Modules](#) page.

## 2.2 Installing and Upgrading UNIX Agent Manager

NetIQ UNIX Agent Manager is a console that you can use to manage all UNIX agent components across your enterprise. You can use UNIX Agent Manager to install the UNIX agent to several computers at the same time and see the computers that NetIQ Change Guardian, NetIQ Secure Configuration Manager, NetIQ Sentinel, and NetIQ Security Manager products monitor.

After you have installed UNIX Agent Manager, you can set up users and assign access to them. For more information about managing UNIX Agent Manager users, see [Section 3.6, “Managing Users in UNIX Agent Manager,”](#) on page 40.

### 2.2.1 Installing UNIX Agent Manager on a Microsoft Windows Computer

Complete the following steps to install the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Windows computer.

**To install UNIX Agent Manager on a Windows computer:**

- 1 Run `UAMInstaller.MSI` in the root folder of the installation kit, and begin responding to the questions in the wizard.
- 2 When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you select that option, UNIX Agent Manager cannot communicate with agents that do not have the same restriction. For more information about FIPS and the other security level options, see [Section 3.2, “Understanding Communication Security Levels,”](#) on page 32.
- 3 Complete the automatic installer wizard. The wizard guides you through the Trial Software License Agreement and installs the UNIX Agent Manager to the folder that you specify.
- 4 Start the UNIX Agent Manager server.
- 5 Type and confirm a password for the UNIX Agent Manager server to use with the admin user account.

To change the administrative password for the UNIX Agent Manager server, start the server using the old password, then in the **Manage Server** window, click **Reset Admin Password**.

### 2.2.2 Installing UNIX Agent Manager on a UNIX or Linux Computer

Complete the following steps to install the UNIX Agent Manager server, the UNIX Agent Manager console, or both on a Red Hat or SUSE computer.

### To install the UNIX Agent Manager on a UNIX or Linux computer:

- 1 Change directories to where you copied the installation package for UNIX Agent Manager.
- 2 Uncompress the appropriate `.tar.gz` file for your platform.
- 3 (Conditional) If you need to restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms, run the `enablefips.sh` script. If you run that script, UNIX Agent Manager cannot communicate with agents that do not have the same restriction. For more information about FIPS and the other security level options, see [Section 3.2, “Understanding Communication Security Levels,”](#) on page 32.
- 4 Start the UNIX Agent Manager server by running the `runserver.sh` script.
- 5 Type and confirm a password that you want the UNIX Agent Manager server to use for the admin user account.
- 6 Start the UNIX Agent Manager console by running the `run.sh` script.

## 2.3 Installing and Upgrading the UNIX Agent and Module

To use AppManager for UNIX, you must:

- ♦ Install the UNIX agent on all the computers you want to manage. Install the agent to a folder, not to the root directory.
- ♦ If you install the agent to a computer that you will manage using AppManager for Oracle RDBMS on UNIX or Linux Servers, ensure that the account you use to install the agent has access to the Oracle Home directory.
- ♦ Install the patch to the agent computers that provides the new monitoring features, install UNIX Agent 8.1.0.11 (this is a hotfix) or UNIX Agent 8.1.0.1 with patch 8.1.0.9 or UNIX Agent 8.0 with patch 8.0.0.12, or UNIX Agent 7.5 with patch 7.5.0.14.
- ♦ Install the Knowledge Scripts by running the module installer `.msi` on all AppManager repositories that store data for this module.
- ♦ Install the Help files by running the module installer `.msi` on all AppManager Control Center and Operator Console computers you will use with this module.

### 2.3.1 Deploying the UNIX Agent Components Using UNIX Agent Manager

Remotely installing the AppManager for UNIX to your agent computers provides a convenient and uniform method for deploying one or more UNIX agents. You can use the Deployment wizard provided in the UNIX Agent Manager for remote deployment, unless one of the following conditions exist:

- ♦ Your site standards prohibit your access to root passwords.
- ♦ Your site standards require a specific software distribution mechanism.
- ♦ Your site standards prohibit software distribution mechanisms.
- ♦ You installed UNIX Agent Manager using the options to restrict all communication to FIPS certified encryption algorithms.

For information about installing UNIX Agent Manager, see [Section 2.2, “Installing and Upgrading UNIX Agent Manager,”](#) on page 18.

### To remotely deploy UNIX agent components:

- 1 In the **File** menu of UNIX Agent Manager, click **Remote Deployment**.
- 2 Click the **Add Host** button and fill in the fields as prompted.
- 3 When you are given the option of setting the security level, NetIQ Corporation recommends that you choose Security Level 1 or 2. For more information about security level options, see [Section 3.2, “Understanding Communication Security Levels,” on page 32](#).
- 4 When you are given the option of communication security settings, do not restrict communication to only Federal Information Processing Standard (FIPS) encrypted algorithms unless you are certain that your environment requires that restriction. If you select that option, UNIX Agent Manager cannot communicate with agents that do not have the same restriction. For more information about FIPS and the other security level options, see [Section 3.2, “Understanding Communication Security Levels,” on page 32](#).
- 5 When you are given the option to specify the restart method, NetIQ Corporation recommends that you accept the default, **rclink**. For more information about restart methods, see [Section 3.3.4, “Restart Methods,” on page 35](#).
- 6 When you are given the option of including additional startup options, you can select from the list of options described in the section [Section 3.3.3, “Script Options,” on page 35](#).
- 7 Proceed through the wizard to complete the agent installation.

## 2.3.2 Upgrading UNIX Agent Using UNIX Agent Manager

UNIX Agent Manager provides a utility to upgrade existing agents. You cannot use this feature if your UNIX Agent Manager restricts communication to FIPS certified encryption algorithms.

### To upgrade UNIX agents using UNIX Agent Manager

- 1 Ensure the computer that you want to upgrade is registered in UNIX Agent Manager. You can do this by either importing an existing list that contains the computer using **Manage Hosts > Import/Export Host Lists**, or by adding the computer using **Manage Hosts > Add Host**.
- 2 Highlight the computer you want to upgrade, and select **Manage Hosts > Upgrade Hosts**. The left pane displays any options you need to select for your agent.
- 3 Scroll to the bottom of the panel and click the **Start Upgrade** button.

## 2.3.3 Installing Locally on a UNIX or Linux Computer

The following procedure guides you through logging on to an agent computer and locally installing all required components on the agent computer.

### To install an agent on the local computer:

- 1 Log on to an agent computer using an account with super user privileges.
- 2 Change directories to product installation package, and then enter the following command to start the install script:  

```
/bin/sh ./install.sh
```
- 3 Proceed through the prompts.
- 4 When you are given the option to specify the restart method, NetIQ Corporation recommends that you accept the default, **rclink**. For more information about restart methods, see [Section 3.3.4, “Restart Methods,” on page 35](#).

- 5 When you are given the option to configure the agent for use with other products, only select the option if you run NetIQ Secure Configuration Manager, NetIQ Change Guardian, or NetIQ Security Manager to monitor the computer. If you do not use those products, type `n` instead of accepting the default response of `y` for those questions.
- 6 When you are given the option of setting the security level, NetIQ recommends that you choose Security Level 1 or 2. For more information about security level options, see [Section 3.2, “Understanding Communication Security Levels,”](#) on page 32.
- 7 When you are given the option of including additional startup options, you can select from the list of options described in the section [Section 3.3.3, “Script Options,”](#) on page 35.
- 8 When you finish the installation process, AppManager starts the daemons.

## 2.3.4 Silently Installing on the Agent Computer

Performing a silent installation allows you to install the UNIX agent without interactively running the installation script. Silent installation uses an installation file that records the information required for completing the installation. Each line in the file is a *name=value* pair that provides the required information, for example, `HOME=/usr/netiq`.

If you use the deployment wizard to perform a local installation on one computer, the wizard lets you create a silent installation file based on your choices. A sample installation file, `SampleSilentInstallation.cfg`, is located on your UNIX agent download package.

The following parameters are available for silent installation for the NetIQ UNIX Agent working with AppManager:

Parameter	Description
<code>CREATE_TARGET_DIR</code>	Specifies whether you want the install program to create the target installation directory if it does not already exist. Valid entries are <code>y</code> and <code>n</code> . The default is <code>y</code> .
<code>CONTINUE_WITHOUT_PATCHES</code>	Specifies whether the install program stops or continues when the operating system is not a supported version. Valid entries are <code>y</code> and <code>n</code> .
<code>IQCONNECT_PORT</code>	Specifies the port that the UNIX agent uses to listen for communications from UNIX Agent Manager. The default is 2620.
<code>IQ_STARTUP</code>	Specifies restart method for the uagent process. This process is used by the UNIX agent for the AppManager, Security Manager, and Secure Configuration Manager products. For information about the options, see <a href="#">Section 3.3, “Starting and Stopping the UNIX Agent,”</a> on page 32. Valid entries are <code>relink</code> and <code>inittab</code> . The default is <code>relink</code> .
<code>USE_FIPS_COMMON</code>	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only FIPS certified encryption algorithms. Only use this option if your environment requires this restriction. Valid entries are 0, meaning that communication is not restricted, and 1, meaning that communication is restricted.
<code>INSTALL_AM</code>	Specifies whether the UNIX agent works with AppManager. Valid entries are <code>y</code> and <code>n</code> .
<code>OWNER</code>	Username that runs the UNIX agent. The default is <code>root</code> .
<code>GROUP</code>	User group of the account that runs the UNIX agent. The default is the primary group of the user to which <code>OWNER</code> is set.

Parameter	Description
AM_LANG	Specifies the locale in which the UNIX agent runs. The default is the locale of the user who executes the installation script. This parameter is available for UNIX agent 8.0 and above.
AM_ORACLE_ENABLED	Specifies whether the UNIX agent works with AppManager for Oracle. Valid entries are <i>y</i> and <i>n</i> .
AM_STARTUP	The restart method for the <i>nqmagt</i> and agent processes. These processes are specific to AppManager. Valid options are <i>rclink</i> and <i>inittab</i> . For information about the options, see <a href="#">Section 3.3.4, "Restart Methods,"</a> on page 35.
ADDITIONAL_STARTUP_OPTIONS	Any additional startup parameters you want the agent to use when it is restarted. For a list of options, see <a href="#">Section 3.3.3, "Script Options,"</a> on page 35.
INHERIT_AM	<p>For upgrade only. Specifies whether you want to use the previous AppManager-specific configuration information. If you set this parameter to <i>y</i>, you do not need to specify many of the other parameters, such as parameters related to the management server, because the values are inherited from your current configuration.</p> <p>If you set this parameter to <i>n</i>, any running jobs and their current configuration settings are <b>not</b> migrated, and the UNIX agent installation is treated as a new installation. All running jobs no longer run. You must configure and start new jobs.</p>
KEEP_OLD_AM_DIR	For upgrade only. Specifies whether you want to keep the directory from the previous installation that contains AppManager-specific information. Valid entries are <i>y</i> and <i>n</i> .
PREVIOUS_AM_HOME_MOVED	For upgrade only. Specifies where you want to move the directory used by the previous installation to keep AppManager-specific information.
INHERIT_AM_DIR	<p>For upgrade only. Specifies whether you want to use the previous directory that contained AppManager-specific information. If you set this parameter to <i>y</i>, you do not need to specify many of the other parameters, such as parameters related to the management server, because the values are inherited from your current configuration.</p> <p>If you set this parameter to <i>n</i>, any running jobs and their current configuration settings are <b>not</b> migrated, and the UNIX agent installation is treated as a new installation. All running jobs no longer run. You must configure and start new jobs.</p>
AM_MACHINENAME	Name of the UNIX computer to be displayed in the Operator Console TreeView. The name should be the full hostname for the computer and must be a name or address the management server can resolve for discovery to succeed.
SKIP_DISCOVERY	Specifies whether you want to install and start the agent without running discovery. Valid entries are <i>y</i> and <i>n</i> .
AM_PRIMARY_MS_ADDRESS	Name or IP address of the primary management server. If you are upgrading and have set <i>INHERIT_AM_DIR</i> to <i>y</i> , you can leave this setting blank to use the address from the previous installation. For example: <i>tc09k05</i> .

Parameter	Description
AM_PRIMARY_MS_PORT	Port on which the AppManager primary management server listens for the UNIX agent. The suggested port is 9001. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation.
AM_PRIMARY_MS_SEC	Security level for the primary management server. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. For example, 2.
AM_PRIMARY_MS_KEY	Location of the public encryption key file for the primary management server. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. For example, <code>/home/smba/keystore/key_1.key</code> .
AM_SECONDARY_MS_ADDRESS	Name or IP address of the secondary management server. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. For example, <code>10.26.7.184</code> .
AM_SECONDARY_MS_PORT	Port on which the secondary management server listens for the UNIX agent. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. The suggested port is 9001.
AM_SECONDARY_MS_SEC	Security level for the secondary management server. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. For example, 1.
AM_SECONDARY_MS_KEY	Location of the public encryption key file for the secondary management server. If you are upgrading and have set <code>INHERIT_AM_DIR</code> to <code>y</code> , you can leave this setting blank to use the address from the previous installation. For example <code>/home/smba/keystore/key_1.key</code> .
USE_FIPS_AM	Specifies whether the UNIX agent communicates with UNIX Agent Manager using only FIPS certified encryption algorithms. Only use this option if your environment requires this restriction. Valid entries are 0, meaning that communication is not restricted, and 1, meaning that communication is restricted.
KEEP_OLD_AGENT_DIR	Specifies whether to keep the previous installation directory when you are upgrading from version 7.5 of the UNIX agent. Valid entries are <code>y</code> and <code>n</code> .
OLD_INSTALL_DIR_MOVED	Specifies the directory where you want the installation program to move the previous installation directory.

After you have created the installation file, run the silent installation command. For example:

```
./install.sh Target_Directory -s SilentConfigurationFile.cfg
```

where `Target_Directory` is the directory you want to install to, and `SilentConfigurationFile` is the file name you used to specify the installation options. You can also use the default configuration file, `SampleSilentInstallation.cfg`.

The script then extracts information from the installation file and installs the agent based on the values you have specified.

---

**NOTE:** You must specify the installation filename as an absolute path. By default, `SampleSilentInstallation.cfg` is located in the UNIX agent install directory.

---

## 2.3.5 Installing the Module on AppManager Repository and Console Computers

Access the `AM70-UNIX-7.x.x.x.msi` module installer from the `AM70_UNIX_7.x` self-extracting installation package on the [AppManager Module Upgrades & Trials](#) page.

You can install the Knowledge Scripts into local or remote AppManager repositories (QDBs). Install these components only once per QDB.

The module installer now installs Knowledge Scripts for each module directly into the QDB instead of installing the scripts in the `\AppManager\qdb\kp` folder as in previous releases of AppManager.

### To install the module on the QDB and AppManager console computers:

- 1 On the QDB computer, double-click the module installer `.msi` file.
- 2 Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.
- 3 Specify the SQL Server name of the server hosting the QDB and the case-sensitive QDB name.
- 4 (Conditional) If you use Control Center 7.x, run the module installer for each QDB attached to Control Center.
- 5 (Conditional) If you use Control Center 8.x, run the module installer only for the primary QDB, and Control Center automatically replicates this module to secondary QDBs.
- 6 Run the module installer on all console computers to install the Help and console extensions.
- 7 (Optional) If you have not discovered UNIX and Linux computers, run the `Discovery_UNIX` Knowledge Script on all agent computers. For more information, see [Section 2.5, “Discovering UNIX and Linux Computers,”](#) on page 25.
- 8 To get the updates provided in this release, upgrade any running Knowledge Script jobs. For more information, see [Section 2.6, “Upgrading Knowledge Script Jobs,”](#) on page 26.

## 2.4 Applying Patches

NetIQ provides patches to the UNIX agent in a zipped file known as a p-ball for agent components and in a zipped file for UNIX Agent Manager.

Patches to UNIX Agent Manager are applied to the UNIX Agent Manager server that automatically applies any required changes to the consoles using that server. To install patches to UNIX Agent Manager, right-click the UNIX Agent Manager server icon in the task bar.

### To upgrade the agent computer using the UNIX Agent Manager:

- 1 Click **Patch > Patch Manager**.
- 2 Click **Load Patch** to add the patch you want to apply to the list of available patches.
- 3 Select the computers where you want to apply the patch.
- 4 Select the patches that you want to apply.



- 5 Click **Start Install**. The time required to update your agents depends on factors such as the number of agents to update, distance from the UNIX Agent Manager server, network connectivity, and bandwidth. This process can take up to 20 minutes per agent.
- 6 Click **Back** to close the Patch Manager.

## 2.5 Discovering UNIX and Linux Computers

Use the `Discovery_UNIX` and the `Discovery_HardwareUNIX` Knowledge Scripts to discover configuration and resource information for many types of UNIX and Linux operating environments and servers.

---

**NOTE:** Discovery of floppy disk drives and ROM Drivers (sd) are not supported.

---

The UNIX agent 8.0 or later supports delta discovery for all UNIX and Linux discovery Knowledge Scripts. Delta discoveries are more efficient and require fewer system and network resources to perform since they only send information about changes to the QDB. This is the default setting for any new discovery job you run. However, the first time you run a delta discovery job it will perform a full discovery since there is no previous full discovery to compare against. Any subsequent jobs will perform a delta discovery.

For more information about delta discovery, see the *AppManager Control Center User Guide* on the [AppManager](#) page.

By default, these scripts run once for each computer.

### 2.5.1 Discovery\_UNIX Values

Set the **Values** tab parameters as needed.

Description	How to Set It
Raise event if discovery succeeds? (y/n)	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to y to raise an event when the job succeeds. The default is n.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to reflect the importance when the job succeeds. The default is 25.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to reflect the importance when the job fails. The default is 5.
Event severity when discovery partially succeeds	Set the event severity level, from 1 to 40, to reflect the importance when the job is partially completed. This type of event usually indicates the operating environment on the target computer is not supported or not recognized. The default is 15.
Ignore partial discovery event for network interfaces? (y/n)	Set this parameter to y if you want discovery to avoid partial discovery events related to network interfaces. The default is n.
Discover printers?	Set this parameter to y if you want discovery to include printer resources. By default, printers are discovered.
Discover ZFS pool datasets?	Set this parameter to y if you want discovery to include ZFS pool datasets. The default is n.

Description	How to Set It
Event severity for internal failure	Set the event severity level, from 1 to 40, to reflect the importance when the job fails. The default is 5
Enable debugging?	Set to y to enable debugging. The default is n.

## 2.5.2 Discovery\_HardwareUNIX Values

The Discovery\_HardwareUNIX Knowledge Script discovers hardware resources for Dell and HP computers running a Linux operating system. For more information about the hardware Knowledge Scripts, see [Chapter 5, “HardwareUNIX Knowledge Scripts,” on page 151](#).

Set the **Values** tab parameters as needed.

Description	How to Set It
<b>Discovery Settings</b>	
<b>Event Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager cannot retrieve information from the hardware. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance when AppManager cannot retrieve metrics. The default is 5.
<b>Raise event when discovery succeeds?</b>	By default, this Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to yes to raise an event when the job succeeds. The default is unselected.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance when the job completes successfully. The default is 25.
<b>Raise event when discovery partially succeeds?</b>	Select <b>Yes</b> to raise an event if discovery cannot complete. This type of event usually indicates the operating environment on the target computer is not supported or not recognized. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to reflect the importance when the job cannot complete. The default is 15.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.

## 2.6 Upgrading Knowledge Script Jobs

This release of AppManager for UNIX contains updated Knowledge Scripts. You can push the changes for updated scripts to running Knowledge Script jobs in one of the following ways:

- ◆ Use the AMAdmin\_UpgradeJobs Knowledge Script.
- ◆ Use the Properties Propagation feature.

## 2.6.1 Running AMAdmin\_UpgradeJobs

The AMAdmin\_UpgradeJobs Knowledge Script can push changes to running Knowledge Script jobs. Your AppManager repository (QDB) must be at version 7.0 or later. In addition, the repository computer must have hotfix 72040 installed or the most recent AppManager repository hotfix. To download the hotfix, see the [AppManager Suite Hotfixes](#) page.

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job. For more information, see the Help for the AMAdmin\_UpgradeJobs Knowledge Script.

## 2.6.2 Propagating Knowledge Script Changes

You can propagate script changes to jobs that are running and to Knowledge Script Groups, including recommended Knowledge Script Groups and renamed Knowledge Scripts.

Before propagating script changes, verify that the script parameters are set to your specifications. Customized script parameters might have reverted to default parameters during the installation of the module. New parameters might need to be set appropriately for your environment or application.

You can choose to propagate only properties (specified in the Schedule and Values tabs), only the script (which is the logic of the Knowledge Script), or both. Unless you know specifically that changes affect only the script logic, you should propagate both properties and the script.

For more information about propagating Knowledge Script changes, see the “Running Monitoring Jobs” chapter of the *Operator Console User Guide for AppManager*.

### Propagating Changes to Ad Hoc Jobs

You can propagate the properties and the logic (script) of a Knowledge Script to ad hoc jobs started by that Knowledge Script. Corresponding jobs are stopped and restarted with the Knowledge Script changes.

#### To propagate changes to ad hoc Knowledge Script jobs:

- 1 In the Knowledge Script view, select the Knowledge Script for which you want to propagate changes.
- 2 Right-click the script and select **Properties propagation > Ad Hoc Jobs**.
- 3 Select the components of the Knowledge Script that you want to propagate to associated ad hoc jobs:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, such as schedule, monitoring values, actions, and advanced options.

## Propagating Changes to Knowledge Script Groups

You can propagate the properties and logic (script) of a Knowledge Script to corresponding Knowledge Script Group members.

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see [“Propagating Changes to Ad Hoc Jobs” on page 27](#).

### To propagate Knowledge Script changes to Knowledge Script Groups:

- 1 In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
- 2 Right-click the Knowledge Script Group and select **Properties propagation > Ad Hoc Jobs**.
- 3 (Conditional) If you want to exclude a Knowledge Script member from properties propagation, deselect that member from the list in the Properties Propagation dialog box.
- 4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

Select	To propagate
Script	The logic of the Knowledge Script.
Properties	Values from the Knowledge Script Schedule and Values tabs, including the schedule, actions, and Advanced properties.

- 5 Click **OK**. Any monitoring jobs started by a Knowledge Script Group member are restarted with the job properties of the Knowledge Script Group member.

## 2.7 Uninstalling UNIX Agents and UNIX Agent Manager

You can uninstall the AppManager for UNIX agent components and UNIX Agent Manager.

### 2.7.1 Uninstalling the UNIX Agent

You can use UNIX Agent Manager to uninstall agents from remote computers, or you can uninstall them locally. When you uninstall the agent, all agent components, including the ones for other products, are uninstalled.

---

**NOTE:** You do not need to uninstall agents with a lower version number before upgrading agents. Use this procedure only if you want to completely remove agents from remote computers. For more information about upgrading agents, see [Section 3.5, “Saving UNIX Agent Information to a File,” on page 39](#).

---

To uninstall the agent locally, change to the installation directory, then run the following command:

```
./uninstall.sh
```

You can also uninstall using the console. This option allows you to uninstall from many computers at once. To uninstall an agent in UNIX Agent Manager, select the computers where you want to uninstall the agent, click **Manage Hosts > Uninstall Agent**.

## 2.7.2 Uninstalling UNIX Agent Manager

To uninstall the UNIX Agent Manager on Windows computers, use the **Add/Remove Programs** Control Panel to remove the **UNIX Agent Manager** program, then delete the UNIX Agent Manager folder.

To uninstall the UNIX Agent Manager on a Linux computer, change directories to the UNIX Agent Manager installation directory, and then enter `rm -rf VSAU`.



# 3 Working with AppManager for UNIX

Use AppManager to monitor UNIX and Linux computers the same way you monitor your Windows-based systems and applications. This chapter provides information that is unique to AppManager for UNIX. For complete information about working with AppManager and performing common AppManager tasks, such as starting jobs, defining monitoring policies, responding to events, setting up corrective actions, and creating charts and reports, see the AppManager documentation.

## 3.1 Management Sites

A **management site** always consists of one AppManager repository and at least one AppManager management server. A management site might have multiple management servers to distribute processing and communication for managed clients, but each management site has exactly one repository, and each management server communicates with only one repository.

In each management site, you can designate a primary and backup management server for each managed client computer by running the `AMAdminUNIX_SetPrimaryMS` Knowledge Script.

After you designate a primary management server, the agents communicate only with that management server. If communication with the primary management server is interrupted and you have identified a secondary management server, communication is automatically transferred to the secondary management server. When communication with the primary management server is interrupted and then restored, the agent resumes communication with that server. If you have not specified a secondary management server, data and events are stored locally on the managed client until communication is restored.

Explicitly designating a primary and secondary management server is the way most organizations handle failover support and control which management servers communicate with which agents.

You should always designate both management servers for UNIX and Linux computers. For more information about designating a primary and secondary management server for load-balancing and failover support, see the *Administrator Guide for NetIQ AppManager*.

### 3.1.1 Managing a UNIX Client Computer from Multiple AppManager Sites

The UNIX agent automatically restricts its management server communication to the management servers you specified during installation or the management servers that you designated using the `AMAdminUNIX_SetPrimaryMS` Knowledge Script, meaning the last management site added. Always run the `SetPrimaryMS` Knowledge Script after agent installation to properly designate primary and secondary management servers, or to add other management servers from additional management sites.

If you restart the agent using the `-c` option (cold start), the agent maintains only the primary and secondary management servers that you designated when you last ran the `AMAdmin_SetPrimaryMS` Knowledge Script. After you cold start, you need to re-designate the primary and secondary management servers from the other site.

If your site uses secure communication to communicate with UNIX agents, you can share the repository encryption key information with the additional repository using the `nqKeyGenUNIX.exe` utility and configure the additional repository to use the same security level for UNIX agent communications. Alternatively, you can create a separate encryption key for the additional repository if you use authentication.

### 3.1.2 Organizing Computers in Groups and Views

In the Control Center Console, you can include both UNIX and Windows-based computers in a management group. However, in most cases, organizing UNIX and Windows computers in different server groups or views simplifies the maintenance of monitoring policies and Knowledge Script groups.

## 3.2 Understanding Communication Security Levels

You must choose the level of security for communication between the NetIQ components that is appropriate for your environment. If your policies allow, use the same security level for AppManager for UNIX that you use throughout your AppManager environment. The options available are:

- ◆ Unencrypted messages (no security): no extra measures are taken to secure agent-to-management server communications. This option is only available for use with NetIQ AppManager Operator Console. All data sent between the management server and the agent is transmitted without encryption, and the agent does not authenticate the identity of the management server. The lowest security setting for agent communications is entirely appropriate in many environments. Cleartext communications facilitate troubleshooting and are suitable for a closed network environment. However, many organizations require greater security to ensure data privacy and integrity and to help prevent potential attacks from unauthorized, external sources.
- ◆ Encrypted communication only (Security Level 1): a basic level of security. All data transmitted between the server and the agent is encrypted and decrypted using a session key generated dynamically when the server is started.
- ◆ Authentication and encrypted communications (Security Level 2): a high level of security. The agent uses a predefined key to authenticate the identity of the management server before sending encrypted data. The key information is stored and a portion of the key is made available for the agent computers to use.

## 3.3 Starting and Stopping the UNIX Agent

When you install the UNIX agent on your computer, the agent starts automatically. The UNIX agent installation adds the UNIX agent to the server startup profile to be automatically started or stopped when you restart or shut down the UNIX system. You can also start or stop the UNIX agent using the UNIX Agent Manager console or the UNIX agent startup script, `nqmdaemon`. If you start the agent from UNIX Agent Manager, you can enter additional startup options.

You can manually start the process at any time by running the `nqmdaemon start` command. The path for running this command can vary, depending on the UNIX platform and information you entered during installation. The complete path for the current platform is always displayed at the end of the UNIX agent installation. For example, on Solaris, the command typically looks like this:

```
/etc/init.d/nqmdaemon start
```



---

**NOTE:** To start the UNIX agent, log in as the user you specified during installation before issuing the `ngmdaemon start` command.

---

To start or stop `ngmdaemon`, the UNIX agent user account must have root access by either running as the root account or using a command such as `uroot` or `sudo`. Depending on your environment, you might need to specify the path to the directory where the command resides. For example, if the `uroot` command is installed in the location `/usr/netiq/vsau/bin`:

```
/usr/netiq/vsau/bin/uroot /etc/init.d/ngmdaemon start
```

### 3.3.1 Command Line Options

Use the following commands to start or stop the UNIX agent from a command line.

Option	Description
<code>cold</code>	Also called cold start. Starts the UNIX agent using the default settings. Pending jobs do not run, but the agent can connect to the management server. This options removes job information from the configuration file.
<code>discover</code>	Runs the Discovery_UNIX Knowledge Script to discover configuration and resource information.
<code>frozen</code>	Also called frozen start. Starts the UNIX agent without any settings. This options deletes the existing <code>NqmCfg.xml</code> configuration file. Pending jobs do not run immediately, and the agent cannot connect to the management server right after starting. However, the connection is restored after a few minutes, and pending jobs are restarted at that time. Use the option only with the assistance of NetIQ Technical Support.
<code>restart</code>	Stops then starts the UNIX agent using the settings in the configuration file.
<code>start</code>	Starts the UNIX agent. If you do not include an argument, the agent starts normally using the settings in the configuration file.
<code>stop</code>	Stops the UNIX agent. The UNIX agent preserves information about any running jobs, but does not actively stop jobs.

### 3.3.2 Automatic Startup and Shutdown Scripts

The UNIX agent provides a set of scripts or commands that facilitate automatic startup and shutdown when the computer is rebooted. These commands vary depending on the operating system of the computer on which they are run. The following table lists the location of these automatic startup and shutdown scripts for some of the key platforms where you run the UNIX agent:

UNIX Operating System	Location and Commands
<b>Startup Commands</b>	
Solaris	<code>/etc/rc3.d/S91ngmdaemon</code>
AIX	<code>/etc/rc.d/rc2.d/S99ngmademon</code>
HP-UX	<code>/sbin/rc3.d/S991ngmdaemon</code>

UNIX Operating System	Location and Commands
Red Hat Linux Enterprise Server 4	<pre>chkconfig --list   grep nqm</pre> <p>Use this command to ensure the rc2, rc3, rc4, and rc5 are on and the S95nqmdaemon is present in each of the following directories:</p> <pre>/etc/rc5.d</pre> <pre>/etc/rc4.d</pre> <pre>/etc/rc3.d</pre> <pre>/etc/rc2.d</pre>
Red Hat Linux Advanced Server 4 (Itanium)	<p>The location and commands are the same as Red Hat Linux Enterprise Server 4 except you must verify whether the S95nqmdaemon is present in each of the following directories:</p> <pre>/etc/rc.d/rc5.d/</pre> <pre>/etc/rc.d/rc4.d/</pre> <pre>/etc/rc.d/rc3.d/</pre> <pre>/etc/rc.d/rc2.d/</pre>
<b>Shutdown Commands</b>	
Solaris	<pre>/etc/rc0.d/K09nqmdaemon</pre>
AIX	<pre>/etc/rc.d/rc2.d/K05nqmdaemon</pre>
HP-UX	<pre>/sbin/rc0.d/K009nqmdaemon</pre>
Red Hat Linux Enterprise Server 4	<pre>chkconfig --list   grep nqm</pre> <p>Use this command to ensure the rc2, rc3, rc4, and rc5 are on and the K08nqmdaemon is present in each of the following directories:</p> <pre>/etc/rc5.d</pre> <pre>/etc/rc4.d</pre> <pre>/etc/rc3.d</pre> <pre>/etc/rc2.d</pre>
Red Hat Linux Advanced Server 4 (Itanium)	<p>The location and commands are the same as Red Hat Linux Enterprise Server 4 except you must verify whether the K05nqmdaemon is present in each of the following directories:</p> <pre>/etc/rc.d/rc1.d/</pre> <pre>/etc/rc.d/rc0.d/</pre> <pre>/etc/rc.d/rc6.d/</pre>
<p><b>NOTE:</b> Startup and shutdown scripts for the Linux operating system are generated automatically. Therefore, the daemon name might not always be S14nqmdaemon and K05nqmdaemon.</p>	

### 3.3.3 Script Options

If you are starting the agent from UNIX Agent Manager, using the manual installation, or using the silent installation script, you can enter the following additional start up options.

Option	Description
-a <i>PortNumber</i>	Sets the default port for communication with all management servers. The suggested port is 9001.
-C	Also called cold start. Starts the UNIX agent using the default settings. Pending jobs do not run, but the agent can connect to the management server. You cannot use this option with any other option.
-d <i>AgentLogDirectory</i>	<p>Sets the directory where the UNIX agent stores log information. Log files in this directory include a timestamp as part of the filename, which is <code>NqmAgt.log</code> or <code>NqmAgt_#.log</code>, depending on how many logs are configured to be kept. For example, a log file named <code>NqmAgt20120412180531.log</code> indicates that the file was created on April 12, 2012, 18:05:31 hrs. The most recently created log file is linked to <code>NqmAgt.log</code>. The default log directory is <code>\$NQMAGT_HOME/log</code>.</p> <p>If you are running the UNIX agent as a non-root user, ensure that the account has permission to read the log directory. If the user running the agent cannot read the log directory, then the UNIX agent cannot start.</p>
-F	Also called frozen start. Starts the UNIX agent without any default settings. Pending jobs do not run, and the agent cannot connect to the management server. You cannot use this option with any other option. Use the option only with the assistance of NetIQ Technical Support.
-H <AgentIPAddress>	Sets an IP address for the UNIX agent. The agent listens on the specified IP address instead of any IP address associated with the agent computer. Use this option to bind the UNIX agent to specific address if your UNIX computer has multiple network interface cards (NICs) with unique IP addresses.

### 3.3.4 Restart Methods

NetIQ recommends that you accept the default, `rclink`. However, the following start methods are available:.

Option	Description
<code>rclink</code>	Starts the agent daemons immediately after the deployment process and adds a startup script to the <code>/etc/rc.d</code> directory. This startup script starts the agent daemons after each reboot when the master <code>rc</code> script runs. This is the default method, and should be used in nearly all environments.
<code>inittab</code>	Starts the agent daemons immediately after the deployment process and adds an entry to the <code>/etc/inittab</code> file. This <code>inittab</code> file entry starts the agent daemons at the default run level after each reboot.

## 3.4 Changing Options for the Agent Computer and the Management Server

After installation, you can change several options for the AppManager for UNIX components on the agent computer and the management server.

---

**NOTE:** If you use the `AMAdminUNIX_SetPrimaryMS Knowledge Script` to set a primary and secondary management server, this information is added to the `NqmComms.xml` file underneath `$AM_HOME/netiq/AM/data/Config_X`, where `X` is an integer.

---

### 3.4.1 Changing the Account the UNIX Agent Uses

When you install the UNIX agent, you identify a user account for the UNIX agent to use. This account effectively owns all of the AppManager files on the computer and handles your monitoring jobs. Depending on the permissions associated with the account, there might be a few limitations on the Knowledge Script jobs you can run. Most Knowledge Script functionality is enabled by the `sudoers` configuration file that extends non-root account access, but in rare cases, the root user or an admin group account might be able to access certain statistics that are not available to a normal user account.

You can change the account you use to run the UNIX agent using UNIX Agent Manager. Select the computer you want and click **Configure > AppManager Options > Configure AM**, then change the account in the **Owner** field.

### 3.4.2 Changing the Listening Port on the Management Server

By default, the computer you designate as a management server for UNIX listens on port number 9001. You have an opportunity to change that port number automatically, during agent installation. However, you can also change it manually after the agent has been installed.

**To change the port number where the management server listens:**

- 1 Click **Start > Run**, then type `regedt32.exe` to start the Registry Editor on the management server computer.
- 2 Open the `HKLM\Software\NetIQ\AppManager\4.0\NetIQms` registry key.
- 3 Click the **UNIX Port** value entry, then click **Edit > DWORD**.
- 4 Select the **Decimal** option to display the current value in decimal format.
- 5 Enter the new port number to use.
- 6 Click **OK**.
- 7 Restart the computer for this change to take effect.

After you change the registry entry for the Windows computer where the management server is installed, you also need to update the UNIX agent with this information. To do this, you need to edit the UNIX agent's communications file, `NqmComms.xml`.

### 3.4.3 Changing the Management Server Hostname or Port Number

You can use UNIX Agent Manager to change the management server that a UNIX agent communicates with or the port number the management server listens on. Using UNIX Agent Manager, select the computer you want and click **Configure > AppManager Options > Configure AM**, then change the port in the Server Management area.

You can also use the `AMAdminUNIX_SetPrimaryMS` Knowledge Script to change the management server that a UNIX agent communicates with or the port number the management server listens on. This Knowledge Script allows you to specify a primary management server or a secondary management server by hostname and change the port number the management server listens on.

### 3.4.4 Changing the Agent Heartbeat Interval

The heartbeat interval controls how frequently the UNIX agent communicates with the management server. In most environments, you do not need to modify the heartbeat interval. However, if you need to modify the heartbeat interval, modify the `<HEARTBEAT>`, `<SCHEDULE>`, and `<INTERVAL>` tags in the `uaconf.xml` configuration file in `$AM_HOME/etc`.

```
<HEARTBEAT>
    <SCHEDULE>
        <INTERVAL>30</INTERVAL>
    </SCHEDULE>
</HEARTBEAT>
```

Set the interval to the number of seconds between agent heartbeat signals. Changing the UNIX agent heartbeat interval might require you to also adjust the UNIX Machine Check and UNIX Machine Timeout intervals on the management server. For example, if you set a longer heartbeat interval to conserve network bandwidth, you should lengthen the UNIX Machine Check and UNIX Machine Timeout intervals to prevent the UNIX agent from appearing to be unavailable between heartbeat signals. For information about changing the intervals on the management server, see the *Administrator Guide for NetIQ AppManager*.

### 3.4.5 Changing the Management Server Trace Logging Level

By default, the management server records information about its operations in a log file on the computer designated as the management server. The log file, `ms.log`, is located in the `NetIQ\Temp\NetIQ_debug\computer` directory, where `NetIQ` is the AppManager installation path

and *computer* is the name of the computer where the management server is installed. The directory for the log file is specified in the `HKEY_LOCAL_MACHINE\Software\NetIQ\Generic\Tracing\TraceLogPath` registry key.

Typically, the information in the log is not detailed. However, you can change the amount of information recorded in the log file by modifying a registry key.

**To change the level of logging for the management server:**

- 1 In the Registry Editor on the computer you are using as the management server., find the `HKEY_LOCAL_MACHINE\Software\NetIQ\NetIQms\Tracing` registry key. This key contains several entries for tracing management server activity. By default, all trace logs are enabled and set to record error and warning messages (values set to 1). Two of the entries, `TraceSockets` and `TraceXml`, trace communication between the management server and NetIQ UNIX agents.

Registry Entry	Purpose
TraceSockets	Tracing of communication activity between the management server and AppManager UNIX agents.
TraceXml	Tracing of all the XML messages transferred to and from the UNIX agents.

- 2 Click the **Trace** value entry that you want to change, then click **Edit > DWORD**.
- 3 Select the **Decimal** option to display the current value in decimal format.
- 4 Set the logging level to one of the following values:

Logging Level	Description
0	Disables trace logging for the selected type of activity.
1	Minimal tracing. Errors and warnings are logged, but there are no informational messages.
2	Minimal tracing with only limited informational messages.
3	Medium level of tracing with more informative messages, including tracing of the communication with the UNIX agent. This is the default.
4	More verbose informative messages.
5	Most verbose tracing.

- 5 Click **OK**.

The change does not require you to restart the computer or the `NetIQms` service.

Each line in the log file includes a time stamp in UTC format, a message type indicator, and the message body. For example:

```
987220342: info 1: computer name = MERCURY
987220342: info 1: host name = MERCURY
987220342: info 1: ip = 10.5.102.152
987220342: info 2: SocketServerThread, 2920
987220342: info 2: UnixAgentsThread, 3052
987220342: info 2: QUnixaConfigureThread, 2620
```

## 3.4.6 Checking the Status of UNIX Servers

Two registry keys control how the management server determines the status of the NetIQ UNIX agents. The registry keys are under the `HKEY_LOCAL_MACHINE\Software\NetIQ\AppManager\4.0\NetIQms\Config` registry key on the management server computer.

- 1 Click the value entry for the queue you want to modify, then click **Edit > DWORD**.

Registry Key Entry	Description
UNIX Machine Check Interval	<p>Set the interval, in seconds, to control how often the management server checks the time of the last heartbeat signal from each of its UNIX agents. This registry key is used in conjunction with the UNIX Machine Timeout value to determine whether a UNIX server is available.</p> <p>If the management server has not received a heartbeat signal in the period specified as the UNIX Machine Timeout value, the UNIX agent is deemed unavailable. The default is 300 seconds.</p>
UNIX Machine Timeout	<p>Set the interval, in seconds, that identifies a UNIX agent as unavailable. If the UNIX agent does not send a heartbeat signal in this period of time, it is deemed unavailable. The default is 1200 seconds.</p>

- 2 Select the **Decimal** option to display the current value in decimal format.
- 3 Set the key value as appropriate for your environment.
- 4 Click **OK**.

This change requires you to restart the `NetIQms` service to take effect. To restart the `NetIQms` service, use the Services Control Panel.

## 3.5 Saving UNIX Agent Information to a File

The UNIX Agent Manager server stores the information about the UNIX agents you monitor. However, storing the information to a separate file can be useful for backups or for copying the server to another computer. To store your UNIX agent list and configuration information in a file outside the UNIX Agent Manager server click **Manage Hosts > Export/Import Host Lists** in UNIX Agent Manager.

If you are upgrading from previous version of UNIX Agent Manager to the latest version, you should save your configuration information before you upgrade so that you can import it after you upgrade. You can export your UNIX agent information from the existing UNIX Agent Manager, then import the information into the latest UNIX Agent Manager.

---

**NOTE:** The latest version of UNIX Agent Manager is 7.4.0.2

---

**To export the host information from UNIX Agent Manager:**

- 1 In the left pane of UNIX Agent Manager, click **Agent Manager**.
- 2 Click **Hosts > Edit Hosts**.
- 3 Select all of the hosts in the Current Hosts list.
- 4 Click **Export Selected**.

## 3.6 Managing Users in UNIX Agent Manager

UNIX Agent Manager allows administrators to control user access to features and computers. To log into any UNIX Agent Manager server, an administrator on that server must create the user account in the UNIX Agent Manager Administrator Console, which is part of the UNIX Agent Manager console.

You can grant different permissions to each user account that allows access to only the features required by that user's role. Permission sets allow you to simplify this process. Permission sets define product, computer, and feature access. Once you create a permission set, you can assign it to multiple user accounts with the same role.

For example, you can create a permission set that grants access to all AppManager functionality separate from Secure Configuration Manager functionality. You can then assign this permission set to all computers running AppManager. When you grant a new AppManager user access to a console, simply assign the user to the AppManager permission set to grant them access to the applicable features and computers.

To assign permissions, log into a UNIX Agent Manager console as an administrator and click **Access Control > Admin Console**. From there, add the users that need access to that UNIX Agent Manager server, then assign the appropriate permissions.

### 3.6.1 Using LDAP or Microsoft Active Directory Credentials

UNIX Agent Manager version 7.3 or later can access the information you have already set up in your LDAP or Microsoft Active Directory server to allow users to log into the UNIX Agent Manager server. This functionality is not available if you restricted UNIX Agent Manager to only use Federal Information Processing Standard (FIPS) encrypted algorithms.

To configure UNIX Agent Manager server to use LDAP or Active Directory credentials:

1. Ensure you have the following information:
  - ◆ The domain and computer address, such as `ldap://houston.itservice.production:389`, of the LDAP or Active Directory server
  - ◆ The location of the user entries in the structure of the LDAP or Active Directory server
  - ◆ The attribute that identifies the login name for each user
  - ◆ An account that UNIX Agent Manager server can use to access the LDAP or Active Directory server
2. Log into a UNIX Agent Manager console as an administrator, and open the **Manage Server** window.
3. Click the **LDAP** or **AD** tab, then the **Add** button.
4. Enter the name of the domain that contains the LDAP or AD server. Users must also enter this domain name when they log into UNIX Agent Manager.
5. Select the domain and provide the information as requested on the window using the following guidelines:
  - ◆ In **Server Address**, enter LDAP or Active Directory server computer name and port. For example, `ldap://houston.itservice.production:389`
  - ◆ In **User's Parent DN**, enter the path to the node that contains the usernames you want to use. For example, `ou=AMAdmins,dc=netiq,dn=com`



- ♦ In **Username Attribute**, enter the attribute you want UNIX Agent Manager to use to identify the user. This attribute will be used as a consistent identifier even if the user name changes. The default and only attribute supported by UNIX Agent Manager 7.2 is `uid`
  - ♦ (Conditional) If you use simple authentication for specific users, in **Username**, enter the path to the user name. For example, `ou=Operator,dc=netiq,dc=com`
6. Click **Save**.
  7. Have the users log into UNIX Agent Manager using their LDAP or Active Directory credentials. The user list will not contain the username until the user logs into UNIX Agent Manager for the first time.

## 3.6.2 SSL Communication with the LDAP or Active Directory Server

The UNIX Agent Manager server can communicate with the LDAP or Active Directory server using Secure Sockets Layer (SSL). If you choose to have UNIX Agent Manager server communicate with the server using SSL, you must obtain and manage the required certificates. UNIX Agent Manager requires certificates that are base-64 encoded.

For example, to get a certificate from an OpenLDAP server, run the following command from the `/etc/openldap/certs` directory on the computer that is running the `slapd` daemon:

```
certutil -L -a -n "OpenLDAP Server" -d `pwd` > servername.pem
```

The command creates a `servername.pem` file that you can import into UNIX Agent Manager using the Manage Server window where you identify your LDAP server.



# 4 UNIX Knowledge Scripts

AppManager for UNIX provides the following Knowledge Scripts for monitoring UNIX and Linux computers.

From the Knowledge Script view of console, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help** or **F1**.

Knowledge Script	What It Does
<a href="#">AIXLparUtil</a>	Monitors CPU utilization for Logical Partitions (LPAR) on AIX.
<a href="#">ApplicationProcessMonitor</a>	Monitors the status of processes of an application.
<a href="#">AsciiLog</a>	Monitors an ASCII text file for specific strings and messages logged.
<a href="#">CpuByProcess</a>	Monitors CPU usage for each process and the total CPU usage for all processes.
<a href="#">CpuLoaded</a>	Monitors CPU usage.
<a href="#">CpuResources</a>	Monitors CPU consumption for users, the number of active processes, the number of threads, the number of context switches, and the number of interrupts per second.
<a href="#">CpuUtil</a>	Monitors CPU utilization and queue length.
<a href="#">DNSConnectivity</a>	Checks a DNS client's list of DNS servers to verify each DNS server is reachable and responding to client look-up requests.
<a href="#">DNSHealth</a>	Checks memory and CPU usage for the DNS process and performs a basic <code>nslookup</code> test.
<a href="#">DNSReplication</a>	Monitors replication between two name servers in a specified domain.
<a href="#">DynamicFileSystemSpace</a>	Monitors used space and free space on only non-excluded mounted file systems and, optionally, checks for incremental increases in used space.
<a href="#">ExecUtil</a>	Runs a UNIX or Linux command and, optionally generates events based on the program's output or collects data from the output that can be used to generate graphs.
<a href="#">FailedLogon</a>	Monitors failed logon and failed <code>su</code> attempts.
<a href="#">FileSystemSpace</a>	Monitors used space and free space on mounted file systems and, optionally, checks for incremental increases in used space.
<a href="#">FileSystemSpaceLC</a>	Uses a configuration file to monitor used space on mounted file systems and, optionally, checks for incremental increases in used space.
<a href="#">FindFiles</a>	Monitors the number of files that match a set of criteria.
<a href="#">GeneralCounter</a>	Monitors any user-specified system performance data.
<a href="#">HTTPHealth</a>	Sends a status request to a Web server's HTTP port to check server operation.

<b>Knowledge Script</b>	<b>What It Does</b>
LargeDir	Checks the disk space used by the directories you specify and the number of files under those directories.
LogicalDiskBusy	Monitors logical disk operation time and the maximum queue length.
LogicalDiskIO	Monitors logical disk IO activity, including disk transfers, reads, and writes per second.
LogicalDiskIO26	Monitors transfers, block reads and block writes per second on a logical disk on Linux 2.6 kernel and above. Raises an event if any threshold is exceeded.
LogicalDiskUtilization	Monitors the utilization and I/O request queue for logical disk devices.
MemByProcess	Monitors the individual memory usage for each specified process and total memory usage for all specified processes.
MemShortage	Monitors the physical memory for a system.
MemUtil	Monitors physical memory, virtual memory, and paging files.
NetInterfacesCollision	Monitors network interface collision.
NetInterfacesConnectivity	Monitors the physical connection between network interface adapters and the network.
NetInterfacesDown	Checks the status of network interfaces.
NetInterfacesErrors	Monitors the percentage of input and output errors for network interfaces.
NetInterfacesIO	Monitors the input, output, and throughput of the network traffic on network interface cards.
OpenFiles	Monitors the number of files that are opened by a process in a system
PagingHigh	Monitors UNIX paging activity.
PhysicalDiskBusy	Monitors physical disk activity and response time.
PhysicalDiskIO	Monitors physical disk reads and writes in KB per second.
PhysicalDiskStats	Monitors physical disk operation time and response time.
PingMachine	Checks server availability by running a Ping test and returning response time.
PortHealth	Checks whether system ports are working properly.
PrinterQueue	Monitors the printer queue length and the memory size of the documents in the queue.
PrivilegedProcs	Monitors the number of system processes with an effective user ID (euid) of <code>root</code> .
ProcessDown	Determines whether specified processes are currently running.
Processes	Monitors the number of processes currently running on a system.
ProcessUp	Checks whether a specified process is running.

<b>Knowledge Script</b>	<b>What It Does</b>
<a href="#">RemoteProcessDown</a>	Monitors applications on remote UNIX computers using a proxy UNIX agent.
<a href="#">Report_CPULoad</a>	Generates a detailed report about CPU usage and queue length.
<a href="#">Report_DiskUsageSummary</a>	Generates a summary report about the percentage of disk space used and the amount of free space.
<a href="#">Report_MemoryUtilization</a>	Generates a detailed report about the use of physical and virtual memory, and paging files.
<a href="#">Report_NetInterfacesIO</a>	Generates a report about the use of bandwidth on network interface cards.
<a href="#">Report_SystemUpTime</a>	Generates a report detailing the uptime and downtime (by percentage) of monitored computers.
<a href="#">Report_TopMemoryProcs</a>	Generates a report about the total memory used by all processes and the processes that consume the most memory resources.
<a href="#">RunAwayProcs</a>	Detects runaway processes by sampling CPU usage and terminates processes.
<a href="#">RunCommand</a>	Runs a non-interactive UNIX command.
<a href="#">SmartCPULoad</a>	Monitors CPU utilization of Linux/UNIX machines.
<a href="#">SmartMemoryStats</a>	Monitors the use of physical memory of the system.
<a href="#">SmartPhysicalDiskStats</a>	Monitors physical activity and response time.
<a href="#">SwapLow</a>	Monitors the availability of swap areas.
<a href="#">Syslog</a>	Monitors the <code>syslog</code> file for the search strings you specify.
<a href="#">SystemUpTime</a>	Tracks the number of hours a computer has been operational since it was last rebooted.
<a href="#">TopCpuProcs</a>	Monitors total CPU used by all processes and reports processes that consume the most CPU resources.
<a href="#">TopMemoryProcs</a>	Monitors the total memory used by all processes and reports processes that consume the most memory.
<a href="#">UserSessions</a>	Monitors the number of accounts logged into a computer.
<a href="#">WAMAgentConfiguration</a>	Knowledge Script to configure WAM Client to connect to the WAM server.
<a href="#">ZFSDataset</a>	Monitors the usage of a ZFS dataset.
<a href="#">ZFSPoolHealth</a>	Monitors ZFS Pool Health
<a href="#">ZFSPoolSnapshot</a>	Monitors snapshot usage of the pool.
<a href="#">ZFSPoolStats</a>	Monitors ZFS pool and IO statistics.
<a href="#">ZombieProcs</a>	Monitors the number of zombie processes.

# 4.1 Creating Filters with Regular Expressions

The [AsciiLog](#), [RemoteProcessDown](#), [NT\\_UnixRemoteProcessDown](#), and [Syslog](#) Knowledge Scripts enable you to use regular expressions to define include and exclude filters for pattern-matching against the text being evaluated. Where available, include and exclude filters can be used independently or together to give you a great deal of control in looking for and filtering text files. You can also use the regular expression modifiers to further refine your filtering.

For example, if your **include filter** contains `replic.*` and you specify the modifier `i` to make the search case insensitive, the regular expression contains the wildcard `.` and repeat `*` special characters, indicating you want to find strings that start with `replic` followed by any string of characters. Messages containing either `replication` or `replicated` are matched.

The format is the same for the exclude filter. For example, to find log entries that do not start with the string `success`, the exclude filter might be:

```
^success.*
```

If you are only searching for included strings, you can leave the exclude filter blank. If you want to retrieve all messages in the log in a given interval, you can specify `.*` for the include filter and leave the exclude filter blank.

## 4.1.1 Special Characters for Regular Expressions

The following special characters can be used in regular expressions:

Character	Purpose
.	Wildcard for any one character
*	Repeat zero or more occurrences
^	Beginning of the line
\\$	End of the line
\	Escape the next meta-character
	Alternate matches
[ ]	Any character in the class set. You can specify individual characters or ranges
( )	Grouping characters. For example, you can specify <code>(a b c)</code> to indicate a match with <code>a</code> , or <code>b</code> , or <code>c</code>
+	Quantifier indicating one or more occurrences
?	Quantifier indicating zero or one occurrence
{ <i>n</i> }	Quantifier indicating exactly <i>n</i> occurrence
\w	A word character (alphanumeric plus <code>_</code> )
\s	A white-space character
\d	A digit character

If you use any of these special characters in a literal string, you must “escape” it with a single backslash (\) character. For example, if you run the [AsciiLog](#) Knowledge Script, which scans an ASCII text file for specific strings and messages, and you want to search the log for the string **www.netiq.com**, the string you specify in the Knowledge Script parameter is `www\.netiq\.com`

## 4.1.2 Modifiers for Regular Expressions

In addition to the special characters you can use to create the regular expression, you can also use modifiers to change how pattern-matching is handled. Valid modifiers include:

Modifier	Description
c	Complements the search list
g	Matches globally as many times as possible
i	Makes the search case insensitive
m	Treats the string as multiple lines
o	Interpolates variables only once
s	Treats the regular expression string as a single long line
x	Allows for regular expression extensions

## 4.2 AIXLparUtil

Use this Knowledge Script to monitor Logical Partitions (LPAR) utilization on AIX computers. LPAR utilization is measured in percentage. This Knowledge Script collects utilization data based on the following parameters:

- ◆ Percentage of partition utilized in user mode
- ◆ Percentage of partition utilized in system kernel mode
- ◆ Percentage of partition utilized for I/O operations
- ◆ Percentage of partition in idle mode
- ◆ Number of physical processors consumed
- ◆ Entitled capacity consumed
- ◆ Logical processor utilization

You can set thresholds for each of these parameters. If the partition utilization exceeds any threshold, an event is generated.

### 4.2.1 Resource Object

CPU icon on AIX

### 4.2.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.2.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Number of seconds between samples	Enter the data collection interval, from 2 to 30, in seconds for the <code>lparstat</code> utility. The default value is 5 seconds.
Number of times <code>lparstat</code> should iterate before reporting an average value	Enter the iteration count, from 1 to 100, for the <code>lparstat</code> utility. The default value is 3 iterations.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Data Collection Options</b>	
Collect data for %User CPU state?	Select <b>Yes</b> to collect data for the percentage of CPU used in user mode. The default is unselected, the data is not collected.
Collect data for %System CPU state?	Select <b>Yes</b> to collect data for the percentage of CPU used in kernel/system mode. The default is unselected, the data is not collected.
Collect data for %Wait CPU state?	Select <b>Yes</b> to collect data for the percentage of CPU used in I/O mode. The default is unselected, the data is not collected.
Collect data for %Idle CPU state?	Select <b>Yes</b> to collect data for the percentage of CPU in the idle mode. The default is unselected, the data is not collected.
Collect data for total CPU utilization?	Select <b>Yes</b> to collect data for the total percentage of CPU used. This includes utilization data when the CPU is in user and kernel/system modes. The default is Yes.
Collect data for number of physical processors consumed?	Select <b>Yes</b> to collect data for the number of physical processors consumed by the CPU. The default is Yes.
Collect data for %Entitled capacity consumed?	Select <b>Yes</b> to collect data for the total percentage of entitled capacity used. The default is Yes.
Collect data for %Logical processors utilization?	Select <b>Yes</b> to collect data for the total percentage of logical processor used. The default is Yes.
<b>Thresholds and Eventing</b>	
Threshold -- Maximum %User CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in user mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %System CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in the kernel/system mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.



Description	How to Set It
Threshold -- Maximum %Wait CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in the I/O wait mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Idle CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU in the idle mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 10%.
Threshold -- Maximum total CPU utilization	Enter the threshold value, from 1 to 100, for the maximum percentage of total CPU utilization (in user and kernel/system modes). AppManager raises an event if the CPU utilization exceeds this threshold. The default is 90%.
Threshold -- Maximum number of physical processors consumed. -1 disables	Enter the threshold value, from 1 to 100, for the maximum number of physical processors consumed. AppManager raises an event if the number exceeds this threshold. Enter -1 to disable the threshold. The default is -1.
Threshold -- Maximum %Entitled capacity consumed. -1 disables	Enter the threshold value, from 1 to 1000, for the maximum percentage of entitled capacity utilization. AppManager raises an event if the capacity exceeds this threshold. Enter -1 to disable the threshold. The default is -1.
Threshold -- Maximum %Logical processors utilization. -1 disables	Enter the threshold value, from 1 to 1000, for the maximum percentage of logical processor utilization. AppManager raises an event if the processor utilization exceeds this threshold. Enter -1 to disable the threshold. The default is -1.

## 4.3 ApplicationProcessMonitor

Use this Knowledge Script to monitor the number of application processes for a particular application.

An application can include multiple application processes. Each application process in turn can have more than one process instance. If the total number of process instances for any of the application processes detected falls below the threshold count you set, AppManager raises an event.

The threshold parameter allows you to set a separate threshold for multiple monitored processes. First, supply a list of processes to monitor for the `Process names` parameter. Separate the process names in the list with commas and no spaces. Then supply a comma-separated list of threshold values that correspond to the processes and are listed in the same order.

You also have the option to restart any process that appears to be down. Anytime the number of process instances for a process reaches 0, this Knowledge Script can invoke a restart command that you supply (see the `Command to restart processes when process count crosses minimum threshold` parameter, below). You can enable events to notify you if the attempt to restart a process with a process count of 0 has succeeded or failed. These events are raised by the output term corresponding to success in your command script. You need to supply this output term for the `Word(s) in restart command output that indicate success` parameter.

If you enable data collection, this Knowledge Script returns the current process instance count for all the processes in the monitored application(s).

### 4.3.1 Resource Object

UNIX CPU folder

## 4.3.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

## 4.3.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Application to monitor	Supply the name of the application whose processes you want to monitor. The default is <code>My Application</code> .
<b>Process Monitoring</b>	
Process names	Specify the names of processes to monitor, separate the names of multiple processes with commas and no spaces.
Threshold -- Minimum number of processes	<p>Specify the minimum number of process instances that must be running for each monitored process to prevent an event from being raised.</p> <p>Separate multiple threshold values with commas and no spaces. To ensure that the proper threshold is applied to the intended process, list thresholds in the same order as you listed processes for the <code>Process names</code> threshold.</p>
Threshold -- Maximum number of processes	<p>Specify the maximum number of process instances that must be running for each monitored process to prevent an event from being raised. If an application is running more than this number of process instances, an event is raised.</p> <p>Separate multiple threshold values with commas and no spaces. To ensure that the proper threshold is applied to the intended process, list thresholds in the same order as you listed processes for the <code>Process names</code> threshold.</p>
Command to restart processes when process count crosses minimum Threshold	Specify a command to use to restart any process whose process count is higher than the threshold. Separate multiple commands with commas and no spaces. Leave this parameter blank if you do not want to restart processes automatically.
Word(s) in restart command output that indicate success	<p>Specify a list of the words to be returned by the scripts you supplied to indicate that the scripts succeeded in restarting a process. The presence of these words raises the success event in AppManager.</p> <p>Use a vertical bar character (<code> </code>) to separate multiple words, and use a comma to separate the word groups for each process. The default is:</p> <pre>started success succeed</pre>
<b>Event Notification</b>	
Raise event if number of processes falls below threshold?	Select <b>Yes</b> to raise an event if the process instance count for any monitored process falls below a threshold you set. The default is <b>Yes</b> .
Event severity when number of processes falls below threshold	Set the event severity level, from 10 to 19, to indicate the importance of the event. The default is 10.

Description	How to Set It
Event severity when attempt to restart process fails	Set the event severity level, from 1 to 9, to indicate the importance of the event. The default is 5.
Event severity when attempt to restart process succeeds	Specify the event severity level, from 20 to 40, to indicate the importance of the event. The values you enter for the <code>Word(s)</code> in <code>restart</code> command output that indicate success parameter raises this event. The default is 25.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Data Collection</b>	
Collect data for number of processes?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the number of process instances detected for each monitored process. The default is Yes.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.4 AsciiLog

Use this Knowledge Script to monitor an ASCII text file for specific strings and messages logged since the last monitoring interval. This Knowledge Script allows you to specify the file name, and a regular expression to identify the string to look for or to exclude. The script scans the ASCII file and reports the matching entries found since the last monitoring period. The script checks for changes to the text file that match the expression you enter; it does not re-scan the entire file at each interval unless it determines that the entire file is new (either because the new file size is smaller or because the cyclic redundancy check indicates there is a new file).

This Knowledge Script reads the entire file to find matching strings the first time it executes. The AsciiLog Knowledge Script tracks the last item read in the file persistently. If the Knowledge Script restarts, it is treated as the first iteration. Because the file it is monitoring has already been read before, the first iteration (that is, after restart), starts reading the file from where the marker stopped before it restarted.

You can configure the script to ignore any ASCII log entries that were generated while the computer was in maintenance mode.

You can also configure the script to perform a cyclic redundancy check (CRC) on the file for the purpose of determining when a file has been replaced rather than appended. If the original file has been replaced by a file of the same size or by a larger file, the CRC exposes that change and cause the script to parse the entire new file.

If the file is recreated between intervals and the file size is smaller than the previous version of the file, the script treats it as a new file and searches it from the beginning.

The script raises an event if the number of lines matching your search criteria exceeds the threshold you set, or if the file is missing.

Scanning a large log, bigger than 1 GB for example, might use more operating system resources than you want this script to use. If that happens, reduce the size of the log.

---

**NOTE:** To specify the include and exclude patterns, you need to be familiar with Perl regular expressions. Some information is available in the topic [Section 4.1, “Creating Filters with Regular Expressions,”](#) on page 46.

---

You can use this script to monitor any text file the UNIX agent has permission to read. If the UNIX agent runs under a specific user name rather than `root`, ensure that user account has read permission for the files you want to monitor.

## 4.4.1 Resource Object

UNIX computer icon

## 4.4.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.4.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <b>y</b> to raise events for the ASCII log. The default is <b>y</b> .
Event if log missing? (y/n)	Set to <b>y</b> to raise an event if the log is missing. The default is <b>y</b> .
Event if log file list changed? (y/n)	Select <b>y</b> to raise an event if the number of log files changes, for example, if a new file is added. The default is <b>y</b> .
Create event for each matching line? (y/n)	Select <b>y</b> to raise a new event for each line that meets the event criteria. The default is <b>n</b> , no event is created.
Do you want to limit the number of matching lines returned? (y/n)	Select <b>y</b> to limit the number of lines from the log file matching the search criteria that is returned from a single job iteration. The default is <b>no</b> .  If you are expecting numerous matches, enable this limit. Console performance might be adversely affected by jobs that return a very large number of matches Use the <code>Maximum number of matching lines to return</code> parameter to specify a limit.
Maximum number of matching lines to return	Enter the maximum number of lines, from 0 to 9999, from the log file matching the search criteria to be returned from a single job iteration.  This limit avoids a degradation in performance in cases where many lines match the search criteria. To set a limit here, you must enable the <code>Do you want to limit the number of matching lines returned?</code> parameter. The default is 500 lines.
Parse the log file the first time? (y/n)	Select <b>y</b> to parse the file for the strings you have identified the first time the script runs. Subsequent iterations of the script measure any differences between this version of the file and any subsequent versions.  If you select <b>n</b> , the first iteration of the script reads the file and inserts a marker at the end. Subsequent iterations of the script then measure differences in the script from this point forward. The default is <b>n</b> .

Description	How to Set It
Create events for lines generated during maintenance mode? (y/n)	<p>Select <b>y</b> to have AppManager report events for ASCII log entries that were created when the computer was in maintenance mode.</p> <p>If you select <b>n</b>, AppManager ignores all ASCII log entries created while the computer is in maintenance mode. The default is <b>y</b>.</p>
Collect data? (y/n)	<p>Select <b>y</b> to collect data. The script returns the number of lines containing matching strings. The default is no data is collected.</p>
File names to parse (full path, UNIX-like shell pattern matching notation and comma-separated)	<p>Enter the full path to the file you want to monitor or a regular expression representing the file. You can enter multiple files, comma separated without spaces. An event is created when the file is not found, and when files matching the description are added or deleted since the previous job. For example:</p> <pre data-bbox="708 625 1263 653">/tmp/applog.log, /\var\log\netlog[0-9]/</pre> <p>The UNIX agent must run as an account that has permission to read the file. If you restrict read access on files, you might need to change the account the UNIX agent uses. The default is <code>/etc/hosts</code>.</p>
Maximum number of log files to parse (value 0 equals infinite)	<p>Enter the maximum number of log files, from 0 to 100, that you want to monitor. This limit avoids a degradation in performance in environments with numerous large log files. Enter 0 if you want all log files monitored. The default is 0, all log files are monitored.</p>
Regular expression specifying the include filter	<p>Enter a regular expression in Perl, to identify the pattern you want to look for in the text file being monitored. Strings matching the include filter pattern are returned. The default expression, <code>.+</code>, matches all strings.</p>
Optional file with regular expressions specifying the include filter	<p>If you do not want to enter a regular expression in the <code>Regular expression specifying the include filter</code> parameter, specify the full path to a file containing the regular expression specifying the include filter.</p>
Modifier for the regular expression include filter	<p>Enter any modifier you want to use to change the behavior of the regular expression. For example, specifying <code>i</code> for this parameter makes the include filter case-insensitive. For more information about writing Perl regular expressions, see <a href="#">Section 4.1, "Creating Filters with Regular Expressions,"</a> on page 46.</p>
Regular expression specifying the exclude filter	<p>Enter a regular expression, in Perl, to identify the pattern you want to exclude from matching in the text file being monitored. Strings with the exclude filter pattern are not returned. Separate multiple commands with commas and no spaces.</p> <p>For information about writing Perl regular expressions, see <a href="#">Section 4.1, "Creating Filters with Regular Expressions,"</a> on page 46.</p>
Optional file with regular expressions specifying the exclude filter	<p>If you do not want to enter a regular expression in the <code>Regular expression specifying the exclude filter</code> parameter, specify the full path to a file containing the regular expression specifying the exclude filter.</p>
Modifier for the regular expression exclude filter	<p>Enter any modifier you want to use to change the behavior of the regular expression. For example, specifying <code>i</code> for this parameter makes the exclude filter case-insensitive.</p> <p>For information about writing Perl regular expressions, see <a href="#">Section 4.1, "Creating Filters with Regular Expressions,"</a> on page 46.</p>

Description	How to Set It
Threshold for matching lines	Enter the number of times, from 0 to 99999, to detect a line that matches the search criteria before raising an event. The default is 0, which is the first instance that exceeds the threshold and raises an event.
Avoid file permission check on monitored log file?	Select to <b>Yes</b> to avoid a file permission check on the monitored log file. The default is unselected.
Validate previously scanned lines with CRC? (y/n)	Select <b>y</b> to perform a cyclic redundancy check on the log file. The default is n.
Maximum number of log files to keep	Enter the maximum number of log files, from 0 to 9999, to create when the Knowledge Script logs ASCII entries. The default is 10.
Event severity level for threshold crossing	Set the event severity level, from 1 to 40, for crossing the specified threshold. The default is 5.
Event severity level for all other errors	Set the event severity level, from 1 to 40, when an error occurs. The default is 10.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging?	Set to <b>y</b> to enable debugging. The default is n.

## 4.5 CpuByProcess

Use this Knowledge Script to monitor whether specific processes have exceeded CPU thresholds. The Knowledge Script monitors CPU usage for each named process, as well as the total CPU usage for all named processes.

To determine CPU usage, the Knowledge Script checks the percentage of processor time that the threads for each process used to execute instructions. If a process is not found, the Knowledge Script raises an event and the event detail message indicates which process was not found.

### 4.5.1 Resource Object

UNIX CPU folder

### 4.5.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.5.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Comma-separated list of process names or regular expressions	Enter one or more process names or regular expressions, separated by commas and no spaces. For example: <code>qttest.d</code> . The default is <code>proc1,proc2</code> .

Description	How to Set It
<b>Event Settings</b>	
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Create event for each specified process?	Select <b>Yes</b> to create events for each specified process. The default is Yes.
Create event for the sum of all processes?	Select <b>Yes</b> to create events for the sum of all processes. The default is Yes.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold Settings</b>	
Maximum CPU usage (%) for each specified process	Specify a percentage for the maximum CPU usage percentage for each process. The default is 60 percent.
Maximum CPU usage (%) for all specified processes together	Specify a maximum CPU usage threshold percentage for all specified processes you are monitoring. The default is 95.
<b>Collect Data Settings</b>	
Collect data...	Select <b>Yes</b> to collect data for charts, graphs, and reports for: <ul style="list-style-type: none"> <li>◆ for each specified process?</li> <li>◆ on the sum of all processes</li> </ul> The default is unselected.
Enable debugging?	Select <b>Yes</b> . The default is unselected.
<b>NOTE:</b> This Knowledge Script does not detect invalid process names. If you enter an invalid process name, the Knowledge Script assumes that the process is not running, and reports zero as the CPU result.	

## 4.6 CpuLoaded

Use this Knowledge Script to monitor average CPU usage and average queue length to determine whether the CPU is overloaded. You can monitor the average usage on each processor or the average usage across all processors in a computer. If both the CPU usage and CPU queue length thresholds are exceeded, the CPU is overloaded and AppManager raises an event.

On some systems the CPU queue length does not rise easily and you might want to ignore the queue length. If you do not want to monitor the CPU queue length, set `Maximum number of processes in the queue threshold` to -1.

### 4.6.1 Resource Objects

CPU folder or any individual CPU icon (for multiprocessor systems).

## 4.6.2 Default Schedule

The default interval for this script is **Every 15 minutes**.

## 4.6.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if CPU usage and queue are over thresholds? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. When set to <code>y</code> , this script returns the average CPU utilization percentage (%) and the average CPU run queue length. The default is <code>n</code> .  <b>TIP:</b> If you only want to collect run queue length data, use the <code>UNIX_GeneralCounter Knowledge Script</code> .
Monitor overall CPU load? (y/n)	Set to <code>y</code> to monitor the average load across all processors in a computer. If you are collecting data, setting this option to <code>y</code> creates a single data stream for all processors.  Set to <code>n</code> to monitor the average load for each processor separately. If you are collecting data, setting this option to <code>n</code> creates a separate data stream for each processor.  The default is <code>y</code> .  <b>NOTE:</b> For a single CPU system, monitoring all CPUs produces the same results as monitoring an individual CPU.
Maximum CPU usage (%) threshold	Specify the maximum CPU utilization (user plus kernel). The default is 90%.
Maximum number of processes in the queue threshold	Specify the maximum number of processes in the queue length threshold. CPU queue length indicates how many processes are ready to run. The default is 2.  <b>TIP:</b> If you do not want to monitor the CPU queue length, set the threshold to -1.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.6.4 Example of How this Script Is Used

This script monitors both the percentage of CPU used and processor queue length because, by itself, high CPU usage might not indicate a problem. Instead, you need to consider several factors, including:

- ♦ Queue length (Load average)



- ♦ How you are using the computers monitored
- ♦ Your overall strategy for the environment

For example, if you have a **transactional** environment on a computer consistently using 90% of the CPU, the computer is full. However, if the queue length remains low and stable (for example, never more than 2 processes waiting), it might indicate the computer is sized perfectly for maximum efficiency. If the queue length increases and you have processes waiting, it is likely to be a problem you need to address.

In a **batch** environment, consider setting the thresholds differently; for example, during down times when batch jobs are not running you might want an event if CPU usage is over 50% and any process is waiting (queue length at 0) to ensure the computer has enough CPU headroom when the batch jobs are running.

Other factors to consider are long-range plans, such as the number of users you expect to support, for how long, and how much room for growth you need. For example, you might want to set the CPU usage lower to give you an early warning that you need to off-load some processing or order new systems.

## 4.6.5 Selecting Overall or Individual CPU Load

Monitoring load for each CPU individually provides more specific information about what is happening on a system. For example, if you monitor average load and see CPU usage is 100%, it does not tell you as much about the resource usage as seeing that CPU 0 is running at 90% and CPU 1 is running at 10%.

## 4.6.6 Handling Spikes

Because CPU and queue length are often subject to temporary spikes, you should set a short interval, such as every 3 to 5 minutes, but raise an event only after thresholds are exceeded in 3 consecutive periods.

## 4.6.7 Collecting Data

This Knowledge Script is typically used to raise events, but if you collect data, you can use the information to identify usage trends. For example, seeing the CPU usage growing steadily can help you plan for growth. If you want to do this type of analysis, consider running a second job at a less frequent interval.

You can configure this Knowledge Script to collect data on the average CPU utilization percentage (%) and the average CPU run queue length. You can collect data for the average usage on each processor or the average usage across all processors in a computer.

## 4.6.8 Working with Multi-Processor Systems

On a multi-processor system, the total CPU utilization is the average percentage of time that all the processors on the system are busy executing non-idle threads. For example:

- ♦ if all processors are always busy, this is 100%.
- ♦ if all processors are 50% busy, this is 50%.
- ♦ if 25% of the processors are busy and all processors use a single queue in which threads wait for a processor cycle, this is 25%.

## 4.7 CpuResources

Use this Knowledge Script to monitor CPU resource consumption for users. This Knowledge Script also monitors the number of active processes, the number of threads, the number of context switches per second, and the number of interrupts per second. If any metric exceeds one of the thresholds you set, AppManager raises an event.

### 4.7.1 Resource Object

CPU folder

### 4.7.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.7.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event settings</b>	
Event if user CPU time (%) exceeds threshold?	Select <b>Yes</b> to raise an event if user CPU time usage exceeds the threshold in the interval. The default is Yes.
Event severity when user CPU time exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the user CPU time exceeds the threshold. The default is 5.
Event if number of processes exceeds threshold?	Select <b>Yes</b> to raise an event if the number of processes exceeds the threshold in the interval. The default is Yes.
Event severity when number of processes exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the number of processes exceeds the threshold. The default is 5.
Event if number of threads exceeds threshold?	Select <b>Yes</b> to raise an event if the number of threads exceeds the threshold in the interval. The default is Yes.
Event severity when number of threads exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the number of threads exceeds the threshold. The default is 5.
Event if context switch rate exceeds threshold?	Select <b>Yes</b> to raise an event if the context switches per second exceeds the threshold in the interval. The default is Yes.
Event severity when context switch rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the number of context switches per second exceeds the threshold. The default is 5.
Event if interrupt rate exceeds threshold?	Select <b>Yes</b> to raise an event if the number of interrupts per second exceeds the threshold in the interval. The default is Yes.
Event severity when interrupt rate exceeds threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the number of interrupts per second exceeds the threshold. The default is 5.

Description	How to Set It
Event severity for miscellaneous runtime errors	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when a runtime error occurs. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold settings</b>	
Threshold -- Maximum CPU usage (%) for user time	Enter a threshold for the maximum CPU usage percentage in user mode. The default is 80%.
Threshold -- Maximum number of processes	Enter a threshold for the maximum number of processes that can be running simultaneously. The default is 100 processes.
Threshold -- Maximum number of threads	Enter a threshold for the maximum number of threads that can be running simultaneously. The default is 400 threads.
Threshold -- Maximum context switch rate	Enter a threshold for the maximum number of context switches per second. The default is 100 switches per second.
Threshold -- Maximum interrupt rate	Enter a threshold for the maximum number of interrupts per second. The default is 500 interrupts per second.
<b>Collect data settings</b>	
Collect data for user CPU time?	Select <b>Yes</b> to collect the percentage of user CPU time usage during the interval so that the data can be used for graphs and reports. By default, data is not collected.
Collect data for number of processes?	Select <b>Yes</b> to return the number of active processes for the interval so that the data can be used for graphs and reports. By default, data is not collected.
Collect data for number of threads?	Select <b>Yes</b> to return the number of threads for the interval so that the data can be used for graphs and reports. By default, data is not collected.
Collect data for context switches per second?	Select <b>Yes</b> to return the number of context switches per second so that the data can be used for graphs and reports. By default, data is not collected.
Collect data for interrupts per second?	Select <b>Yes</b> to return the number of interrupts per second so that the data can be used for graphs and reports. By default, data is not collected.

## 4.8 CpuUtil

Use this Knowledge Script to monitor CPU utilization and queue length. CPU utilization is measured in percentage. This Knowledge Script collects utilization data based on the following parameters:

- ◆ User: Percentage of CPU utilized in user mode
- ◆ System: Percentage of CPU utilized in kernel mode
- ◆ Wait: Percentage of CPU utilized for I/O operations
- ◆ Idle: Percentage of CPU in idle mode

You can set thresholds for each of these parameters. If the CPU utilization exceeds any threshold, an event is generated.

If you are using Logical Partitions (LPAR) on AIX, use the [AIXLparUtil](#) Knowledge Script.

## 4.8.1 Resource Object

CPU icon

## 4.8.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.8.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Monitor overall CPU load? (y/n)	Set to <code>y</code> to monitor the total load on the CPU. If you set the value to <code>n</code> , only individual CPUs are monitored. By default, CPU load is monitored. The default is <code>y</code> .
Number of seconds between samples	Enter the data collection interval (in seconds), from 2 to 30, for the <code>sar</code> utility. The default is 5 seconds.
Number of times <code>sar</code> should iterate before reporting an average value	Enter the iteration count, from 1 to 100, for the <code>sar</code> utility. The default is 1 iteration.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
<b>Data Collection Options</b>	
Collect data for %User CPU state? (y/n)	Set to <code>y</code> to collect data for the percentage of CPU utilized in user mode. The default is <code>n</code> .
Collect data for %System CPU state? (y/n)	Set to <code>y</code> to collect data for the percentage of CPU utilized in kernel/system mode. The default is <code>n</code> .
Collect data for %Wait CPU state? (y/n)	Set to <code>y</code> to collect data for the percentage of CPU utilized in I/O mode. The default is <code>n</code> .
Collect data for %Idle CPU state? (y/n)	Set to <code>y</code> to collect data for the percentage of CPU in the idle mode. The default is <code>n</code> .
Collect data for Total CPU utilization? (y/n)	Set to <code>y</code> to collect data for the total percentage of CPU utilized. This includes utilization data when the CPU is in user and kernel/system modes. The default is <code>y</code> .
Collect data on CPU Queue Length? (y/n)	Set to <code>y</code> to collect data for the number of processes in the CPU run queue. The default is <code>n</code> .
<b>Thresholds and Eventing</b>	
Event if CPU usage exceeds thresholds? (y/n)	Set to <code>y</code> to raise an event when the CPU usage exceeds the thresholds you have specified. The default is <code>y</code> .
Threshold -- Maximum %User CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in user mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.

Description	How to Set It
Threshold -- Maximum %System CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in the kernel/system mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Wait CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU utilization in the I/O wait mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 90%.
Threshold -- Maximum %Idle CPU state. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of CPU in the idle mode. AppManager raises an event if the CPU utilization exceeds this threshold. Enter -1 to disable the threshold. The default is 10%.
Threshold -- Maximum Total CPU utilization. -1 disables	Enter the threshold value, from 1 to 100, for the maximum percentage of total CPU utilization (in user and kernel/system modes). AppManager raises an event if the CPU utilization exceeds this threshold. The default is 90%.
Threshold -- Maximum number of processes in the queue.	Enter the maximum number of processes that should be allowed to be queued. If the number of processes in queue exceeds the threshold, AppManager raises an event. The default is 10.
Event if queue length is over threshold? (y/n)	Set to <i>y</i> to raise an event when the queue length exceeds the threshold you have specified. The default is <i>n</i> .
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.9 DNSConnectivity

Use this Knowledge Script to check a DNS client's list of name servers. The Knowledge Script identifies the servers to check by scanning the `/etc/resolv.conf` file, then verifies that each server is reachable with a `ping` command and responds to an `nslookup` request. You should run this Knowledge Script on one or more DNS clients to ensure your DNS servers are available and responding to address (`nslookup`) requests. If any server listed in `/etc/resolv.conf` fails to reply to the `ping` command or the `nslookup` request, AppManager raises an event.

You can only use this Knowledge Script on computers that are running a DNS server.

---

**NOTE:** If your firewall configuration is set to disable the `ping` command, you should disable the Attempt to ping servers parameter to avoid unwanted events.

---

### 4.9.1 Resource Object

Network folder

### 4.9.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.9.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Attempt to ping servers? (y/n)	Set to <code>y</code> to monitor the availability of DNS servers by sending a <code>ping</code> command.  Set to <code>n</code> if you do not want to verify the server availability using a <code>ping</code> command. For example, if your organization or firewall configuration is set to disable the <code>ping</code> command, you should set this option to <code>n</code> to avoid unwanted events.  The default is <code>y</code> .
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.10 DNSHealth

Use this Knowledge Script to check the health of the DNS server by monitoring memory and CPU usage for the DNS process and attempting a basic address look-up (`nslookup`) request. With this Knowledge Script, you can set separate thresholds for the maximum percentage of CPU and memory the DNS process should be using.

This script raises an event if:

- CPU used by the DNS process exceeds the threshold
- Memory used by the DNS process exceeds the threshold
- The DNS process fails to respond to the look-up request

Because temporary spikes or increases in memory or CPU consumption are typically of less concern than look-up failures, the default event severity level signalling that the memory or CPU threshold has been crossed is a Warning event. For look-up failures, the default severity level indicates that the failure is a Severe event.

You can only use this Knowledge Script on computers that are running a DNS server.

### 4.10.1 Resource Object

Network folder

### 4.10.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.10.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if CPU usage is over threshold? (y/n)	Set to <code>y</code> to raise events for CPU usage over the threshold in the interval. The default is <code>y</code> .
Event if memory usage is over threshold? (y/n)	Set to <code>y</code> to raise events for memory usage over the threshold in the interval. The default is <code>y</code> .
Event if bind not running or nslookup fails? (y/n)	Set to <code>y</code> to raise events when the DNS process is down or the look-up request fails in the interval. The default is <code>y</code> .
Collect CPU usage data? (y/n)	Set to <code>y</code> to collect CPU data for charts and reports. If set to <code>y</code> , the script returns the average percentage of CPU used. The default is <code>n</code> .
Collect memory usage data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the average percentage of memory the DNS process used. The default is <code>n</code> .
Maximum CPU usage (%) threshold	Enter a threshold for maximum percentage of CPU the DNS process should be allowed to use before raising an event. The default is 90% of available CPU.
Maximum memory usage (%) threshold	Enter a threshold for maximum percentage of memory the DNS process should be allowed to use before raising an event. The default is 50% of available memory.
Site name to look for using nslookup	Enter the name of the site you want the DNS server to look for using <code>nslookup</code> .
Event severity when CPU usage (%) over the threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the percent of CPU usage crosses the threshold. The default is 15.
Event severity when memory usage (%) over the threshold	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the percent of memory usage crosses the threshold. The default is 15.
Event severity when DNS is down or nslookup fails	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the DNS is down or when <code>nslookup</code> fails. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.11 DNSReplication

Use this Knowledge Script to monitor replication between primary and backup DNS nameservers. This Knowledge Script queries the Start of Authority (SOA) records for the DNS server on the local computer where you run the job and the remote DNS server you specify to determine the serial number that's currently in the SOA record for each server. This serial number is incremented when there are changes to the DNS zone. If the serial numbers are the same, there is full replication of the

primary DNS server's address list. By default, if the serial numbers are not exactly the same in the SOA records (that is, the maximum serial number difference threshold is set to zero), AppManager raises an event.

Although full replication is desirable in most cases, you can specify a threshold for the serial number difference that you deem acceptable for your organization. For example, you might find it acceptable for the serial numbers on backup DNS servers to be out of sync periodically and so might want to adjust the maximum serial number difference threshold to a higher value to allow for this. If the difference between the serial number on the computer where you run the job and the remote DNS server you specify exceeds the acceptable threshold, AppManager raises an event.

You can only use this Knowledge Script on computers that are running a DNS server.

---

**NOTE:** Both the DNS server where you run the job and the DNS server you specify in this Knowledge Script should be nameservers responsible for the domain you specify in this Knowledge Script.

---

## 4.11.1 Resource Object

Network folder

## 4.11.2 Default Schedule

The default interval for this script is **Every hour**.

## 4.11.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <i>y</i> to raise events if the difference between the serial numbers in the SOA records is over the threshold. The default is <i>y</i> .
Collect data? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns the SOA serial number difference between the servers. The default is <i>n</i> .
Maximum serial number difference	Enter a threshold for the maximum difference between SOA serial numbers. The default is 0 (identical serial numbers).
Remote DNS server to compare local SOA records against	Enter the name of the DNS server you want to compare SOA records against. The computer you specify should be a backup or secondary DNS server in the same domain as the DNS server where you drop the Knowledge Script job. The default is <code>ns1.netiq.com</code> .
Domain name	Enter the name of the domain the local and remote DNS nameservers are responsible for serving. The default is <code>netiq.com</code> .
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity is 25, indicating this is an "informational" event that does not require immediate attention. If DNS replication is critical in your environment, you might want to set the event severity higher, for example 1-10, for greater visibility.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.



Description	How to Set It
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.12 DynamicFileSystemSpace

Use this Knowledge Script to monitor the used space and free space on various types of mounted file systems, including NFS mounted file systems, that are often unmounted then mounted again. You can also check for incremental increases in used space beyond the specified threshold. For example, you can configure this Knowledge Script to **Create a new event for incremental increases** and set the **Threshold for incremental increases** to 5% to create an event when used space exceeds 80%, and create a new event when used space exceeds 85%, 90%, and 95%.

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly raises an event.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script.

---

### 4.12.1 Resource Object

Logical disk or disks

### 4.12.2 Default Schedule

The default interval for this script is **Every hour**.

### 4.12.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Notification</b>	
Raise event if threshold exceeded?	Select <code>y</code> to raise an event if the amount of file system space used or free exceeds the capacity threshold you specify. The default is <code>y</code> .
Threshold -- Maximum used space	Type a threshold for the maximum amount of used space (total capacity). If you use this parameter, select the units you want to use. The default is 80.
Threshold -- Minimum free space	Type a threshold for the minimum amount of free space available (total capacity) for use. If you use this parameter, select the units you want to use. The default is -1, meaning no minimum.
Units	Select the unit of measure you want to use to determine the threshold for the used space and free space parameters. Available units are percentage, kilobytes, and megabytes. The default is <code>%</code> .
<b>Incremental Event Notification</b>	

Description	How to Set It
Raise new event for incremental increases?	Specify whether you want to continue to raise events if the amount of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is n.
Threshold -- Incremental increases	Type the amount that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 5.
<b>Data Collection</b>	
Collect data for used and available space?	Specify whether you want to collect data for charts, graphs, and reports. When set to y, this script returns the percentage of used file system space, the amount of available file system space, the used space, and free space. The default is n.
Event severity when used space exceeds threshold	Specify the event severity level, from 1 through 40, to indicate the importance of the event. The default is 5.
Filesystem types to exclude	Specify the types of file systems you do not want to monitor. To determine the type of your mounted file system, use the <code>df</code> command with the <code>-T</code> option. Separate the file system types by a comma without a space. The default is:  <code>subfs,usbfs,proc,iso9660,fd,ctfs,mntfs,objfs,devfs</code>
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Skip events if the filesystem is read-only or in the exclude list? (y/n)	Select <b>Yes</b> to skip events if the file system is read-only or in the exclude list. The default is unselected.
Enable debugging? (y/n)	Set to y to enable debugging. The default is n.

## 4.13 ExecUtil

Use this Knowledge Script to run non-interactive programs from the command line interface on the agent computer and report output of the program. You can use this script to report events based on the output of the program, and you can also use this script to retrieve numeric data points from the program output so you can create charts and graphs of that data.

This script also allows you to run the program in trial mode so you can ensure the parameters are set the way you want before you schedule jobs. If you run the script in trial mode, AppManager generates an event that provide useful information, such as the output of the script or command, in the event details. Trial mode reports the output of the program, but does not evaluate the output. In trial mode, you can verify that you have properly set parameters for the command, the command arguments, environment settings, and data collection without generating extraneous events.

This script does not support running interactive scripts, such as scripts using the `\cat` command, and does not support incoming data streams during data extraction, for example, STDIN, Terminal, or TTY.

In order for AppManager to properly interpret the output from your script or executable, the output must be in UNIX plain text.

### 4.13.1 Resource Object

UNIX computer icon

## 4.13.2 Default Schedule

The default interval for this script is **Run Once**.

## 4.13.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
UNIX executable or script name	Specify the command or script name to run on the UNIX or Linux command line. This is the command or script that AppManager will execute on the operating system, not a descriptive name.
Executable or script arguments	Specify the arguments for the command in the format that the command requires.
Application name	Required field. Specify the name you want AppManager to use to identify the program that runs on the UNIX or Linux command line.
<b>Modify environment variable settings?</b>	Select <b>Yes</b> to temporarily add, change a value for, or ignore environment variables when the command or script runs. The default is unselected.
Environment variables to set (comma separated, Eg. VAR1=VAL1,VAR2=VAL2)	Specify the new environment variables you want to set or the existing environment variables you want to override during the execution of the command or script. Separate the variables with a comma, but no spaces. AppManager does not permanently change the variables that you list in this parameter.
Environment variables to unset (comma separated, Eg. VAR1,VAR2)	Specify the environment variables to ignore during the execution of the command or script. Separate the variables with a comma, but no spaces. AppManager does not permanently remove the variables that you list in this parameter.
Inherit environmental settings for data extraction command?	Select <b>Yes</b> if you want AppManager to use the same environment variable parameter settings to retrieve data from the output of the program as AppManager used to run the program. The default is unselected.
Trial mode? (reports output without validating)	Select <b>Yes</b> if you want AppManager to run the program and report the output of the program, but not compare the output to the criteria you have set for events. Use this parameter to ensure that you have properly configured the parameters in this Knowledge Script to generate the events and data that you want. The default is Yes.
<b>Event Settings</b>	
<b>Raise event with the standard output?</b>	Select <b>Yes</b> if you want AppManager to report an event if the program generates any output. The details of the event contain the output of the program. When you run in Trial Mode, this parameter is ignored. The default is unselected.
Event severity	Specify the event severity level, from 1 through 40, to indicate the importance of the event generated for standard output. The default is 25.
<b>Raise event if execution generates no output?</b>	Select <b>Yes</b> to raise an event if the program does not generate any results. This parameter will create an event if the program fails to execute. When you run in Trial Mode, this parameter is ignored. The default is Yes.

Description	How to Set It
Event severity	Specify the event severity level, from 1 through 40, to indicate the importance of the event generated if the program does not create output. The default is 5.
<b>Raise event if output contains specific strings?</b>	Select <b>Yes</b> to raise an event if the program generates output that matches a specified character string. Specify the criteria using the <b>String list</b> parameter. If you enter multiple character strings, a separate event is raised for each string that matches the output. When you run in Trial Mode, this parameter is ignored. The default is unselected.
String list (comma-separated)	Specify one or more set of UNIX plain text characters to compare to the output of the program. Do not use special characters or rich text. Separate the strings with commas and no spaces. For example, <code>Incomplete,Data out of bounds,7,error9</code>
Match case?	Select <b>Yes</b> if you want to distinguish between uppercase and lowercase. The default is unselected.
Event severity	Specify the event severity level, from 1 through 40, to indicate the importance of the event generated when the output matches a specified character string. The default is 5.
<b>Raise event if output doesn't contain specific strings?</b>	Select <b>Yes</b> if you want to raise an event if the program generates output that does not include a specified character string. Specify the criteria using the <b>String list</b> parameter. If you enter multiple character strings, a separate event is raised for each string that is not included in the output. When you run in Trial Mode, this parameter is ignored. The default is unselected.
String list (comma separated)	Select <b>Yes</b> to specify one or more sets of characters to compare to the output of the program. Separate the strings with commas and no spaces. For example, <code>No data available,Data written to file,InfoMessage2</code>
Match case?	Select <b>Yes</b> to specify whether you want to distinguish between uppercase and lowercase. The default is unselected.
Event severity	Specify the event severity level, from 1 through 40, to indicate the importance of the event generated when the output does not include a specified character string. The default is 5.
<b>Raise event if extracted numeric data exceed thresholds?</b>	Select <b>Yes</b> to raise an event if data over a specified threshold is extracted from the program using the <b>Data Collection</b> parameters. Specify the numeric threshold using the <b>Thresholds for extracted data</b> parameter. When you run in Trial Mode, this parameter is ignored. The default is unselected.
Event severity	Specify the event severity level, from 1 through 40, to indicate the importance of the event generated when the data extracted exceeds the threshold. The default is 5.
Event severity for internal failure	Specify the event severity level, from 1 though 40, to indicate the importance of an event generated for internal failures. The default is 5.
<b>Data Collection</b>	
<b>Collect numeric data?</b>	Select <b>Yes</b> if you want AppManager to extract numeric data from the program output that can be used to create charts and graphs or generate events if the number is greater than or less than specified thresholds. You can extract more than one number to use for graphing or to generate events, but the data must be numeric so AppManager can perform the necessary calculations. You can extract negative numbers and decimals, but not numbers that are in scientific notation. The default is unselected.

Description	How to Set It
Data extraction method? (awk/perl/custom)	Specify how you want AppManager to get numeric data from the output generated by the command or application you specified in the General Settings parameters. If you use awk command or perl command, ensure that the account running the agent can access the utilities. The default is <code>custom</code> command.
Data extraction arguments or expression	Specify the command or expression to extract the numeric data from the program output.
Labels to use for extracted data (comma separated)	Specify the name for AppManager to use to identify the extracted numeric data. If you have multiple numbers, separate the labels for each with a comma and no spaces.
Thresholds for extracted data (comma separated, Eg. MAX1:MIN1,MAX2:MIN2)	Type a set of maximum and minimum thresholds for the extracted data. Separate the maximum and minimum with a colon and no spaces. For example, if you want AppManager to generate an event when the numeric data goes above 75 or below 50, enter <code>75:50</code> . If you have multiple numbers, separate the thresholds for each number with a comma and no spaces. For example, <code>75:50,8600:-2486</code> .
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.14 FailedLogon

Use this Knowledge Script to monitor the number of failed log-on and switch-user-to-root (`su`) attempts since the last interval. The result is always zero for the first interval so that the Knowledge Script can establish a baseline for subsequent checks. A higher than average number of failed logon or `su` attempts might indicate an attempt to break in to the server or that password guessing programs are being used to try to crack the security on the server.

If the number of failed logon or switch user attempts exceeds the threshold you set, AppManager raises an event.

To run this Knowledge Script as a non-root user on a CentOS computer:

- 1 Log in using the root account.
- 2 Run the command `chmod +w /etc/uroot.cfg`.
- 3 In the uroot configuration file, using for example, `vi /etc/uroot.cfg`, add `/bin/grep` to the end.
- 4 Save the uroot configuration file.
- 5 Run the command `chmod -w /etc/uroot.cfg`.

### 4.14.1 Resource Object

UNIX computer icon

### 4.14.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.14.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event for failed login? (y/n)	Set to <code>y</code> to raise an event if the number of failed user login attempts exceeds the threshold in the interval. On Solaris, a failed log-on attempt is only registered after five consecutive failures. The default is <code>y</code> .
Event for failed su? (y/n)	Set to <code>y</code> to raise an event if the number of failed su attempts exceeds the threshold in the interval. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the number of failed login attempts for the interval. The default is <code>n</code> .
System log file (leave blank for default)	<p>Type the full path to the location of the log file that records failed attempts to use the <code>login</code> command. For more information about how to register logins and record failed attempts to a log file, see your operating system documentation. If you leave this parameter blank, the script checks for the log file in the following default locations:</p> <ul style="list-style-type: none"><li>◆ On Sun Solaris, the default location is <code>/var/adm/loginlog</code></li><li>◆ On HP-UX 11.1 and earlier, the default location is <code>/var/adm/btmp</code></li><li>◆ On HP-UX 11.2 and later, the default location is <code>/var/adm/btmps</code></li><li>◆ On IBM AIX, the default location is <code>/etc/security/failedlogin</code></li><li>◆ On Linux, the default location is <code>/var/log/messages</code></li></ul> <p><b>NOTE:</b> On IBM AIX computers, if you configured syslog to log failed login attempts in a file other than the default file, ensure the non-default log file is available by performing the following steps:</p> <ol style="list-style-type: none"><li>1. Create the log file where you want to log failed login attempts. For example, <code>/var/adm/messages</code>. For more information, see your IBM AIX documentation.</li><li>2. Specify the full path to the log file in the <code>syslog.conf</code> system file.</li><li>3. Restart <code>syslog</code> for the changes to take effect.</li></ol>
System su log file (leave blank for default)	Type the full path to the location of the su log file that records failed attempts to use the <code>su login</code> command. For more information about how to register logins and record failed attempts to a log file, see your operating system documentation.
Maximum number of failed login attempts	<p>Enter a threshold for the number of failed login attempts. The default is 1 failed attempt.</p> <p><b>TIP:</b> If you find you are generating too many events from users entering passwords incorrectly, you can determine a typical log on failure pattern (for example 5 per 24 hours) using the Collect data option, then set this parameter based on the typical pattern.</p>
Maximum number of failed su attempts	Enter a threshold for the number of failed <code>su</code> attempts. The default is 1 failed attempt.
Event severity level for failed login	Set the event severity level, from 1 to 40, to indicate the importance of the of a failed login. The default is 8.
Event severity level for failed su	Set the event severity level, from 1 to 40, to indicate the importance of a failed su event. The default is 8.

Description	How to Set It
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.15 FileSystemSpace

Use this Knowledge Script to monitor the used space and free space on mounted file systems and optionally, check for incremental increases in used space beyond the specified threshold.

For example, you can configure this Knowledge Script to **Create a new event for incremental increases** and set the **Threshold for incremental increases** to 5% to create an event when used space exceeds 80%, and create a new event when used space exceeds 85%, 90%, and 95%.

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly raises an event.

If you want to prevent monitoring of some types of file systems, use the [DynamicFileSystemSpace](#) Knowledge Script.

### 4.15.1 Resource Objects

Any logical disk or disks.

### 4.15.2 Default Schedule

The default interval for this script is **Every hour**.

### 4.15.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Notification</b>	
Raise event if threshold exceeded?	Select <b>Yes</b> to raise an event if the amount of file system space used or free exceeds the capacity threshold you specify. The default is Yes.
Threshold -- Maximum used space	Set the threshold for the maximum amount of used space (total capacity). The default is 80.  <b>NOTE:</b> If you use this parameter, also select the units you want to use.
Threshold -- Minimum free space	Set a threshold for the minimum amount of free space available (total capacity) for use. The default is -1, meaning no minimum.  <b>NOTE:</b> If you use this parameter, also select the units you want to use.

Description	How to Set It
Units	Select the unit of measure you want to use to determine the threshold for the used space and free space parameters. Available units are percentage, kilobytes, and megabytes. The default is %.
<b>Incremental Event Notification</b>	
Raise new event for incremental increases?	Select <b>Yes</b> to continue to raise events if the amount of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is unselected.
Threshold -- Incremental increases	Set the amount that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 5.
<b>Data Collection</b>	
Collect data for used and available space?	Select <b>Yes</b> to collect data for charts, graphs, and reports. When selected, this script returns the amount of used file system space, the amount of available file system space, the used space, and free space. The default is unselected.
Event severity when used space exceeds threshold	Specify the event severity level, from 1 through 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.16 FileSystemSpaceLC

This Knowledge Script uses a configuration file on the managed client computer to monitor the percentage of used space on mounted file systems as reported by the system `df` command and optionally, check for incremental increases in used space beyond the specified threshold. Using the configuration file, you can specify a different threshold for each file system and therefore receive event information for each (for example, when `/usr` is at 95% and `/bin` is at 80%).

When checking for incremental increases, a single event is created if the specified threshold is met; event collapsing is not applicable. If you want to monitor incremental increases in used space, do NOT enable the event option on the **Advanced** Knowledge Script Properties tab to **Generate a new event when original event condition no longer exists**. If you enable this option, the Knowledge Script incorrectly creates an event.

---

**NOTE:** You can set thresholds for file systems not in the configuration file but found as the result of a `df` command. You can enable events and data collection for these file systems. You can also use this Knowledge Script to dynamically monitor file systems without re-running discovery.

---

### 4.16.1 Resource Object

Any logical disk folder

### 4.16.2 Default Schedule

The default interval for this script is **Every hour**.



## 4.16.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Default Event Thresholds for Mounted File Systems</b>	
<b>Event Notification</b>	
Raise event if threshold exceeded for a mounted file system?	Select <b>Yes</b> to raise an event if the percentage of file system space used exceeds the default used threshold you specify for mounted file systems. The default is unselected.
Threshold -- Maximum used space	Set a threshold for the maximum percentage of file system space available (total capacity) that should be in use by mounted file systems. The default is 80.
<b>Incremental Event Notification</b>	
Raise new event for incremental increases?	Select <b>Yes</b> to continue to raise events if the percentage of file system space used exceeds the capacity threshold you specify and continues to increase since the previous event. The default is unselected.
Threshold -- Incremental increases	Type the percentage that must be exceeded before another event is raised while the initial threshold remains exceeded. The default is 5.
Event severity when used space exceeds threshold	Specify the event severity level, from 0 through 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Monitoring</b>	
File system types to exclude	Specify the types of systems you do not want to monitor, separated by commas with no space. The default is <code>subfs,usbfs,proc,iso9660,fd</code> .
Monitor mounted NFS shares?	Select <b>Yes</b> to monitor mounted Network File Systems. The default is unselected.
Override file system configuration values (optional)	Type the file system configuration values to override. This allows you to enter the values in the user interface. The default is blank.  Use the following format (semi-colon, separated) for the configuration values:  <code>"doevent?,dodata?,threshold,mountpoint,machinename" y,n,80,/usr;n,y,80,/var,&lt;machinename&gt;</code>  Entering the machine name is optional.
Override configuration file (full path) (optional)	Type the full path to the logical configuration file you created. The default is blank.  Use the following format for the configuration file; enter one line per entry:  <code>"doevent?,dodata?,threshold,mountpoint " y,n,80,/usr n,y,75,/var y,y,90,/tmp</code>
<b>Default Data Collection Options for Mounted File Systems</b>	

Description	How to Set It
Collect data for space usage on all mounted file systems?	Select <b>Yes</b> to collect data for charts, graphs, and reports for mounted file systems. When selected, this script returns the percentage of used file system space, the percentage of available file system space, the used space (MB), and free space (MB). The default is unselected.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.17 FindFiles

Use this Knowledge Script to monitor the number of files that match a set of criteria. This Knowledge Script raises an event if the number of matching files crosses the threshold you specify.

This Knowledge Script is supported on: [Linux].

### 4.17.1 Resource Object

UNIX Machine folder

### 4.17.2 Default Schedule

The default interval for this script is **Once Every 24 Hours**.

### 4.17.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Root folder to begin the search	Enter the root folder path from where you want to begin the search, The default is <code>/usr</code> .
File name(s) can use * or ? wildcards	Enter the file name that you want to search. You can use the wild card characters * or ? when entering the file name.
Search subfolders?	Select <b>Yes</b> to include sub-folders in the search. The default is unselected.
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the FindFiles job fails. The default is 5.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to retrieve the metrics. The default is 5.
<b>Event Settings</b>	

Description	How to Set It
<b>Raise event if file count threshold is exceeded?</b>	Select <b>Yes</b> to raise an event if the file count threshold is exceeded. The default is Yes.
File count threshold	Enter the file count threshold value with a maximum value of 99999. The default is 500.
Severity - Exceeded threshold	Set the severity level, from 1 to 40, to indicate the importance of an event when the number of files matched exceeds the threshold. The default is 15.
<b>File Filters</b>	
<b>Date Modified Filter</b>	
Apply date modified filter?	Select <b>Yes</b> to apply a date filter to the file. The default is unselected.
Begin date (ddmmyyhhmm)	Enter the begin date for the date modified filter. The default is blank.
End date (ddmmyyhhmm)	Enter the end date for the date modified filter. The default is blank.
<b>File Size Filter</b>	
Apply file size filter?	Select <b>Yes</b> to apply the file size filter. The default is unselected.
File size	Enter the file size to apply to the filter. The default is 2.
File size scale	Set the file size scales to one of the following: <ul style="list-style-type: none"> <li>◆ bytes</li> <li>◆ kilobytes</li> <li>◆ megabytes</li> <li>◆ gigabytes</li> <li>◆ terabytes</li> </ul> The default is megabytes.
File size operator	Select file size operator. Options include: <ul style="list-style-type: none"> <li>◆ less than</li> <li>◆ greater than</li> <li>◆ equal to</li> </ul> The default is greater than.
<b>Raise event if Folder size of matching files exceeds the threshold.</b>	Select <b>Yes</b> to raise an event. The default is unselected
Severity - Exceeded threshold	Set the severity level, from 1 to 40, to indicate the importance of an event in which the folder size of the matched files exceeds the threshold. The default is 15.
Folder size threshold	Enter the folder size threshold level. The default is 10.

Description	How to Set It
Folder size scale	Set the folder size scale to one of the following: <ul style="list-style-type: none"> <li>◆ kilobytes</li> <li>◆ megabytes</li> <li>◆ gigabytes</li> <li>◆ terabytes</li> </ul>
Folder size operator	Select folder size operator. Options include: <ul style="list-style-type: none"> <li>◆ less than</li> <li>◆ greater than</li> <li>◆ equal to</li> </ul> <p>The default is greater than.</p>
<b>Raise event if a folder cannot be accessed?</b>	Select <b>Yes</b> to raise an event if a folder cannot be accessed. The default is unselected.
Severity - Folder not accessible	Set the severity level, from 1 to 40, to indicate the importance of an event in which the folder is not accessible. The default is 25.
Maximum number of entries per event report	Enter the maximum number of entries per event report, with a maximum to 4000. The default is 1000.
<b>Data Collection</b>	
Collect file count data?	Select <b>Yes</b> to collect data for charts, graphs, and reports for file count data. When selected, this script returns the number of files matched. The default is unselected.
Collect folder size data?	Select <b>Yes</b> to collect data for charts, graphs, and reports for folder size data. When selected, this script returns the folder size of the matched files. The default is unselected.

## 4.18 GeneralCounter

Use this Knowledge Script to monitor system performance. This script maps elements of UNIX performance data using a format similar to Windows Performance Monitor counters. It uses the Object, Counter, and Instance model, and identifies which of those UNIX “counters” you want to monitor. Information for the objects and counters you specify is returned to the management server. The performance data is then stored in the AppManager repository and available for reporting in AppManager charts and reports.

There are several base objects, such as:

- ◆ UX Disk
- ◆ UX Virtual Memory
- ◆ UX Processor
- ◆ UX Block IO
- ◆ UX Networking
- ◆ UX Paging
- ◆ UX Swapping

Each object has multiple counters and can have multiple instances. You can set both high (Over) and low (Under) thresholds for the counter you are monitoring, and can set up the script to raise an event if the value of the counter you select is greater than the **Maximum threshold** value, or is less than the **Minimum threshold** value. You can also specify a consecutive number of times that the over or under threshold value must be crossed before an event is raised.

---

**NOTE:** AppManager raises an event only if the counter value is greater than the specified Maximum threshold value or is less than the specified Minimum threshold value. If a counter does not exist on the managed client, the Knowledge Script terminates with an error.

---

For more information about objects and their counters, see [Chapter 7, “Counter Reference,” on page 195](#).

## 4.18.1 Resource Object

UNIX computer icon

## 4.18.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

## 4.18.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for current counter value? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns the current value of the specified counter. The default is <i>n</i> .
Raise event if maximum threshold is exceeded? (y/n)	Set to <i>y</i> to raise an event if the counter value is greater than the value specified in as the <b>Maximum threshold</b> parameter. The default is <i>y</i> .
Threshold -- Maximum counter value	Enter a greater-than threshold for the counter value. If the counter you are monitoring exceeds this value, AppManager raises an event if the <b>Raise event if maximum threshold is exceeded?</b> parameter is enabled. The default is 500.  <b>TIP:</b> Keep in mind that the units this value represents (for example, a number, percentage, or rate) depend on the specific counter you are monitoring.
Raise event if minimum threshold is not met? (y/n)	Set to <i>y</i> to raise an event if the counter value is less than the value specified in the <b>Minimum threshold</b> parameter. The default is <i>y</i> .
Threshold -- Minimum counter value	Enter a lower-limit threshold for the counter value. If the counter you are monitoring falls below this value, AppManager raises an event if the <b>Raise event when minimum threshold not met?</b> parameter is enabled. The units this value represents depend on the specific counter you are monitoring. The default is 20.

Description	How to Set It
Counter to monitor	<p>Type the object, counter, and instance(s) to monitor.</p> <p>Use the format <i>object counter instance</i>. For example:</p> <pre>UX Processor %System Time _Total</pre> <p>The names are case-sensitive and the delimiter ( ) is required. You can enter up to 5 counters, separated by commas and no spaces.</p> <p>Some counters require you to specify an instance name as well as the object and counter. In most cases, if a counter requires an instance name, you can specify the specific instance, for example, a specific CPU or device name, or <code>_Total</code> for all instances.</p> <p>Alternatively, you can leave the instance blank to indicate <code>_Total</code> instances. For example:</p> <pre>UX Block IO Reads/s ,UX Block IO Writes/s </pre> <p>If instances are not applicable for a counter, you can leave the instance blank. For example:</p> <pre>UX Swapping Swap in KBytes/s </pre>
Consecutive times threshold exceeded	Enter the number of consecutive times, from 0 to 99, the maximum or minimum threshold should be exceeded before an event is raised. The default is 1 time.
Event severity when maximum threshold exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event when the maximum threshold is crossed. The default is 5.
Event severity when minimum threshold not met	Set the event severity level, from 1 to 40, to indicate the importance of the event when the minimum threshold is crossed. The default is 8.
Event severity when no counter/instance found	Set the event severity level, from 1 to 40, to indicate the importance of the event when AppManager cannot find a counter or instance. The default is 15.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.18.4 Examples of How this Script Is Used

Use this Knowledge Script to yield performance information for the counters you are interested in monitoring. It is particularly useful for monitoring system statistics not already covered with other Knowledge Scripts and customizing the monitoring of your UNIX servers. With AppManager, you can use the counter data to start corrective actions when thresholds are crossed, generate more complex and sophisticated graphs, and provide historical information for reporting, trend analysis, and capacity planning.

When specifying counters, use the format *object|counter|instance*. For example:

```
UX Processor|%System Time|_Total
```

Object and counter names are case-sensitive and the delimiter (|) is required. For more information about counters, see [Chapter 7, “Counter Reference,” on page 195](#).

## 4.19 HTTPHealth

Use this Knowledge Script to check the operation of an HTTP server. This Knowledge Script connects to the Web servers you specify and sends a status request. If the Web server does not respond to the request, AppManager raises an event.

### 4.19.1 Resource Object

UNIX computer icon

### 4.19.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.19.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <i>y</i> to raise events. The default is <i>y</i> .
Collect data? (y/n)	Set to <i>y</i> to collect data for charts and reports. The default is <i>n</i> .
Web server address list (separated by commas and no spaces)	<p>Enter a list of Web server addresses, separated by commas, that you want to check. You can specify the address by hostname, IP address, or fully qualified domain name.</p> <p>For example:</p> <pre>netiq.com:80,192.168.1.123:8080,google.com</pre> <p>Using this example, the Knowledge Script uses port 80 for the server netiq.com and port 8080 for server 192.168.1.123. If no port is specified in the URL, then the default is 80. In the above example as no ports are specified for the server URL google.com, the Knowledge Script will take it as 80.</p> <p>The default is <code>www.netiq.com</code>.</p>
Return code list (separated by commas and no spaces)	Enter a list of return codes, separated by commas, to check. Use this parameter to specify any server address that is not in standard URL format. You must have a value in this parameter to use this script. The default is 400.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.20 LargeDir

Use this Knowledge Script to monitor the directories you specify. The Knowledge Script checks the disk space used by the directories you specify and the number of files under those directories. You can set this Knowledge Script to check directories recursively or to only check in the directories you specify, and to raise an event when disk usage is over the threshold you set or when the number of files in a directory is over the threshold you set.

### 4.20.1 Resource Object

UNIX computer icon

### 4.20.2 Default Schedule

The default interval for this script is **Every hour**.

### 4.20.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if the disk space usage is over the threshold? (y/n)	Set to <i>y</i> to raise an event if the disk space used by any monitored directory exceeds the disk space threshold. The default is <i>y</i> .
Collect data on disk space usage? (y/n)	Set to <i>y</i> to collect data for charts and reports. The default is <i>n</i> .
Maximum disk space used threshold (in KB)	Type the maximum amount of disk space, in KB, that should be used for the directory. The default is 1000.
Event if the number of files is over the threshold? (y/n)	Set to <i>y</i> to raise an event if the number of files in any monitored directory exceeds the file threshold you set. The default is <i>y</i> .
Collect data on the number of files? (y/n)	Set to <i>y</i> to collect data for charts and reports. The default is <i>n</i> .
Maximum number of files threshold	Type the maximum number of files that should be contained in the directory. The default is 1000.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.
Include sub-directories recursively (y/n)?	Set to <i>y</i> to include disk usage and file information for all sub-directories recursively. The default is <i>y</i> .
List of directories to search (separated by commas)	Type the directory path you want to monitor. You can specify multiple directories, separated by commas. For example: <code>/usr/home,/usr/mail</code> . The default is <code>/tmp</code> .
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .



## 4.21 LogicalDiskBusy

Use this Knowledge Script to monitor the logical disk activity on one or multiple disks. You can use this Knowledge Script to set a threshold for maximum disk operation time and the maximum queue length. This Knowledge Script raises an event if either the disk operation time or the queue length exceeds the threshold. This Knowledge Script only provides logical disk metrics that are provided by the operating system kernel.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script.

---

Do not use this Knowledge Script to monitor queue length for a logical volume on VERITAS or AIX.

On Linux operating systems, this Knowledge Script:

- ◆ Requires the optional sysstat package to be installed
- ◆ Does not monitor file-based file systems

### 4.21.1 Resource Objects

Any logical disk or disks on Solaris, Linux, or AIX.

### 4.21.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.21.3 Setting Parameter Values

Set the following parameters as needed:

---

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data for disk operation time and queue length? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the percentage of logical disk and waiting queue in use. The default is <code>n</code> .
Threshold -- Maximum disk operation time	Specify maximum amount of time a disk operation should take before an event is raised. The default is 200 milliseconds.
Threshold -- Maximum I/O queue length	Specify the maximum number of processes that should be in the I/O queue at any time. The default is 1.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

---

## 4.22 LogicalDiskIO

Use this Knowledge Script to monitor the logical disk input/output (I/O) activity. This Knowledge Script monitors the number of logical disk transfers, logical disk reads, and logical disk writes per second. You can set a threshold for each metric. If logical disk I/O exceeds any of the thresholds you set, AppManager raises an event.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script.

---

### 4.22.1 Resource Objects

Any logical disk or disks

### 4.22.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.22.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to <i>y</i> to raise events. The default is <i>y</i> .
Collect data for transfers per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of transfers per second for each logical disk. The default is <i>n</i> .
Collect data for reads per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of reads per second for each logical disk. The default is <i>n</i> .
Collect data for writes per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of writes per second for each logical disk. The default is <i>n</i> .
Threshold -- Maximum transfers per second	Specify the maximum number of transfers per second that can occur before an event is raised. The default is 80.
Threshold -- Maximum reads per second	Specify the maximum number of reads per second that can occur before an event is raised. The default is 50.
Threshold -- Maximum writes per second	Specify the maximum number of writes per second that can occur before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.23 LogicalDiskIO26

### 4.23.1 Resource Object

Any logical disk or disks for kernel version 2.6 or higher.

### 4.23.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.23.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to <i>y</i> to raise events. The default is <i>y</i> .
Collect data for transfers per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of transfers per second for each logical disk. The default is <i>n</i> .
Collect data for reads per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of reads per second for each logical disk. The default is <i>n</i> .
Collect data for writes per second? (y/n)	Set to <i>y</i> to collect data for graphs and reports. If enabled, returns the number of writes per second for each logical disk. The default is <i>n</i> .
Threshold -- Maximum transfers per second	Specify the maximum number of transfers per second that can occur before an event is raised. The default is 80.
Threshold -- Maximum reads per second	Specify the maximum number of reads per second that can occur before an event is raised. The default is 50.
Threshold -- Maximum writes per second	Specify the maximum number of writes per second that can occur before an event is raised. The default is 50.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.24 LogicalDiskUtilization

Use this Knowledge Script to monitor the logical disk activity. This Knowledge Script raises an event if either the percentage of disk utilization or the percentage of time the I/O request queue is not empty exceeds the threshold.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script.

---

Do not use this Knowledge Script to monitor:

- ♦ I/O queue utilization on AIX
- ♦ VERITAS logical volumes
- ♦ File-based file systems on HP-UX

On Linux operating systems, this Knowledge Script:

- ♦ Requires installation of the sysstat package 8.1.8 or higher

## 4.24.1 Resource Objects

Any logical disk or disks on Solaris, Linux, and AIX.

## 4.24.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.24.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if threshold is exceeded? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the percentage of logical disk and waiting queue in use. The default is <code>n</code> .
Threshold -- Maximum disk utilization	Specify a threshold for the maximum percentage of logical disk that should be in use. The default is 95%.
Threshold -- Maximum I/O queue utilization (Solaris only)	Specify a threshold for the maximum percentage of time processes should be waiting in the I/O queue. The default is 50%.
Event severity when threshold is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.25 MemByProcess

Use this Knowledge Script to monitor memory usage for specified processes. The Knowledge Script monitors individual memory use for each specified process, and the total memory use for all specified processes. If a process is not found, the Knowledge Script assumes that the process is not currently running, and reports zero as the memory result.

If the memory use for any monitored process exceeds the threshold you set, AppManager raises an event.

---

**TIP:** This Knowledge Script does not detect invalid process names. If you enter an invalid process name, the Knowledge Script assumes that the process is not running, and reports zero as the result.

---

## 4.25.1 Resource Object

UNIX computer icon

## 4.25.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.25.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Comma-separated list of process names	Enter one or more process names, separated by commas and no spaces. The default is <code>dtlogin</code> .
Create event for each specified process? (y/n)	Set to <code>y</code> to raise events when the memory usage is over the threshold for individual processes. The default is <code>y</code> .
Collect data for each specified process? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the memory usage for each process. The default is <code>n</code> .
Maximum memory usage (KB) for each specified process	Enter a maximum threshold for memory usage for each process. The default is 20000 KB.
Create event for the sum of all specified processes? (y/n)	Set to <code>y</code> to raise events when the combined memory usage for all specified processes is over the threshold. The default is <code>y</code> .
Collect data on the sum of all specified processes? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the combined memory usage for all specified processes. The default is <code>n</code> .
Maximum memory usage (KBs) for all specified processes together	Specify a threshold for combined memory usage for all processes you are monitoring. The default is 32000 KB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.26 MemShortage

Use this Knowledge Script to monitor the physical memory for a system. This Knowledge Script monitors the swapping scan rate to determine if more physical memory might help system performance. Any non-zero scan rate value can indicate that the current amount of physical memory is causing a performance bottleneck. This Knowledge Script raises an event if the memory (in KB) swapped-in and swapped-out crosses the threshold you specify.

---

**NOTE:** For Linux and Solaris versions earlier than 2.8, without the swapping scan rate metric, Update Definition in User Variables. monitors the swapping rate.

---

## 4.26.1 Resource Object

Memory folder

## 4.26.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.26.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if scan rate exceeds threshold? (y/n)	Set to <i>y</i> to raise an event if the scan rate exceeds the threshold. The default is <i>y</i> .
Collect data? (y/n)	Set to <i>y</i> to collect data for charts, graphs, and reports. The default is <i>n</i> .
Maximum scan rate (per second)	Specify the maximum number of pages that should be scanned per second. The default is 0.
Maximum KBytes swapped-in per second threshold	Specify the threshold for the maximum amount of memory (in KB) that should be swapped-in per second, for systems without the swapping scan rate metric. The default is 5.
Maximum KBytes swapped-out per second threshold	Specify the threshold for the maximum amount of memory (in KB) that should be swapped out per second, for systems without the swapping scan rate metric. The default is 5.
Number of consecutive iterations exceeding threshold before sending an event	Type the number of consecutive times either threshold should be crossed before an event is raised. The default is 2.
Event severity level	Specify the event severity level, from 1 through 40, to indicate the importance of the event. The default is 15.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.27 MemUtil

Use this Knowledge Script to monitor physical memory, virtual memory, and swap space (paging files). This Knowledge Script raises an event if any usage level crosses the specified threshold, or if there are any script errors.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script. When calculating ZFS usage, this script handles ZFS with global zone and non-global.

---

## 4.27.1 Resource Objects

Physical memory object, virtual memory object, paging files folder.

## 4.27.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.27.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
<b>HP-UX specific settings</b>	
Include reserved value in calculations?	Select <b>Yes</b> to include reserved swap space in the calculations. If set to Yes, calculations include space reserved for system deactivation and paging processes. This parameter is only available on computers running the HP-UX operating system. The default is Yes.
HPUX: Include memory pseudo-swap values in calculations?	Select <b>Yes</b> to include pseudo-swap space in the calculations. Specify Pseudo-swap space might be up to 3/4 of the available system memory. If set to Yes, calculations include space in the pseudo swap reservation counters. This parameter is only available on computers running the HP-UX operating system. The default is unselected.
<b>LINUX specific setting</b>	
Exclude buffer and cached memory in calculations?	Select <b>Yes</b> to exclude the buffer and cached memory from the physical memory usage calculation. The default is Yes.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Event Settings</b>	
Raise event if physical memory crosses threshold?	Select <b>Yes</b> to raise an event if physical memory crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is unselected.  <b>NOTE:</b> It is normal for UNIX systems to use almost all physical memory.
Raise event if total virtual memory crosses threshold?	Select <b>Yes</b> to raise an event if virtual memory crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is Yes
Raise event if swap space crosses threshold?	Select <b>Yes</b> to raise an event if the paging file use crosses the thresholds you specify for maximum percentage used or minimum MB free. The default is Yes.

Description	How to Set It
Event severity -- physical memory	Set the event severity level, from 1 to 40, to indicate the importance of the event when the maximum physical memory used or minimum physical memory free crosses the threshold. The default is 5.
Event severity -- total virtual memory	Set the event severity level, from 1 to 40, to indicate the importance of the event when the maximum virtual memory used or minimum virtual memory free crosses the threshold. The default is 5.
Event severity -- swap space	Specify the severity level, from 1 to 40, to indicate the importance of the of the event when the maximum swap space used or minimum swap space free crosses the threshold. The default is 5.
Event severity when Knowledge Script error occurs	Set the event severity level, from 1 to 40, to indicate the importance of the event when a Knowledge Script error has occurred. For example, if a Knowledge Script aborts before the job starts or during the job. The default is 10.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold settings</b>	
Threshold -- Maximum physical memory used	Specify the maximum percentage (%) of physical memory that can be in use before an event is raised. It is normal for UNIX systems to use almost all physical memory. The default is 95%.
Threshold -- Minimum physical memory free	Specify the minimum amount (in MB) of physical memory that must be free to prevent an event from being raised. The default is 0 MB.
Threshold -- Maximum total virtual memory used	Specify the maximum total percentage (%) of virtual memory that should be in use. The default is 90%.
Threshold -- Minimum total virtual memory free	Specify the minimum amount (in MB) of virtual memory that should be free. The default is 0.
Threshold -- Maximum swap space used	Specify the maximum percentage (%) of swap space that should be in use. The default is 70%.
Threshold -- Minimum swap space free	Specify the minimum amount (in MB) of swap space that should be free. The default is 0 MB.
<b>Collect data settings</b>	
Collect data for physical memory used?	<p data-bbox="748 1516 1386 1543">Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of physical memory in use.</p> <ul data-bbox="776 1570 1442 1772" style="list-style-type: none"> <li data-bbox="776 1570 1442 1623">◆ total virtual memory free? - returns the total amount (in KB) of virtual free memory.</li> <li data-bbox="776 1650 1442 1703">◆ swap space used? - returns the percentage (%) of the paging file in use.</li> <li data-bbox="776 1730 1442 1782">◆ swap space free? - returns the amount (in KB) of free paging file space</li> </ul> <p data-bbox="748 1797 1019 1824">The default is unselected.</p>



Description	How to Set It
Collect data for physical memory free?	Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of free physical memory (in KB).
Collect data for computational memory in use?	Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of computational memory being used with the legend <code>RealMemUsage %</code> .  <b>NOTE:</b> The <code>computational memory in use</code> setting is only available for AIX computers. Set to unselected for other platforms.
Collect data for total virtual memory used?	Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of total virtual memory in use.
Collect data for total virtual memory free?	Select <b>Yes</b> to collect data for charts and reports to return the free percentage (%) of total virtual memory in use.
Collect data for swap space used?	Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of swap space in use.
Collect data for swap space free?	Select <b>Yes</b> to collect data for charts and reports to return the percentage (%) of free swap space.

## 4.28 NetInterfacesCollision

Use this Knowledge Script to monitor network interface collision. The Knowledge Script checks the percentage of network interface collisions in the interval. If the percentage of network interface collisions exceeds the threshold you set, AppManager raises an event.

On AIX, do not use this Knowledge Script to monitor collisions on an Ethernet device. AIX does not provide collision count information for Ethernet devices. If you monitor an Ethernet device on AIX, this Knowledge Script returns a collision count value 0.

This Knowledge Script runs on the Network Interface object. However, it ignores the loopback device.

On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

### 4.28.1 Resource Objects

Network Interface icon on Solaris, Linux, and HP-UX.

### 4.28.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.28.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if network interface collision exceeds the threshold? (y/n)	Set to <i>y</i> to raise an event if the percentage of network interface collision exceeds the threshold. The default is <i>y</i> .
Collect data? (y/n)	Set to <i>y</i> to collect data for charts and reports. The default is <i>n</i> .
Maximum collision rate (%) threshold	Enter the maximum percentage of network interface collision that should be allowed before raising an event. The default is 80%.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.29 NetInterfacesConnectivity

Use this Knowledge Script to monitor the physical connection between network interface adapters and the network. If the cable for a network interface card is disconnected from the network, AppManager raises an event.

If the computer where you run this Knowledge Script has only one network interface card and that interface card is unplugged, the event cannot be relayed to the AppManager repository until the network interface card is back in service. Therefore, you should only run this script on computers that have more than one network interface card.

On Solaris computers, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

### 4.29.1 Resource Objects

Network Interface icon on Solaris computers (not supported on Linux, HP-UX, or AIX).

### 4.29.2 Default Schedule

The default interval for this script is **Asynchronous**. Once you start the Knowledge Script job, it runs continuously on the monitored system and reports events or data as they occur.

## 4.29.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if network interface card is disconnected? (y/n)	Set to <code>y</code> to raise an event if the cable for a network interface card is unplugged. The default is <code>y</code> .
Event severity when network interface card has lost connectivity	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default severity level is 8.

## 4.29.4 Example of How this Script Is Used

If you run this Knowledge Script on a computer with multiple network interface cards and at least one of them is available and allows the NetIQ UNIX agent to communicate with the management server, an event is raised if any of the network interface cards is disconnected from the network.

---

**NOTE:** This Knowledge Script does not alert you if all network interfaces are disconnected until after network communication is restored. The Knowledge Script job still raises the event, but stores the event in the UNIX agent's local repository until communication with the management server resumes.

---

## 4.30 NetInterfacesDown

Use this Knowledge Script to monitor the up and down status of network interfaces. This Knowledge Script uses the `ifconfig` command to determine if any network interface card (NIC) on a computer with multiple network interfaces is down. If a network interface is detected down, AppManager raises an event.

If the computer where you run this Knowledge Script has only one network interface card and that interface card is down or unplugged, the event cannot be relayed to the QDB until the card is back in service. Therefore, only run this script on computers with multiple network interface cards.

On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the agent to run as root or as a user with root-level authority through the sudo configuration file.

### 4.30.1 Resource Object

Network Interface icon

### 4.30.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.30.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Interfaces to be excluded (comma-separated)	Enter the interfaces you want to exclude from the list of interfaces owned by root. Use a comma with no spaces to separate interface names.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Event detail format	Set the format for the Event detail. <code>HTML Table</code> is the default.
Enable debugging (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .
<b>Event Settings</b>	
<b>Event if network interface is down?</b>	Select <b>Yes</b> to raise an event if a network interface is detected down. The default is <b>Yes</b> .
Consolidate events for all network interfaces?	Select <b>Yes</b> to consolidate events for all network interfaces. The default is unselected.
Raise event for undiscovered network interface	Select <b>Yes</b> to raise an event for undiscovered network interface. The default is unselected.
Add command output in detail event message?	Select <b>Yes</b> to add command output in the detail event message. The default is unselected.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 20.
Consider the status Running as UP? (available on solaris)	Select <b>Yes</b> to consider the status Running as UP? The default is unselected.  This parameter is for Solaris only.
<b>Data Collection</b>	
Collect data?	Select <b>Yes</b> to collect data for charts and reports. If set to <b>Yes</b> , the script returns a value of 100 if the network interface is up and 0 if the network interface is down. The default is unselected.

## 4.30.4 Example of How this Script Is Used

If you run this Knowledge Script on a computer with multiple network interface cards and at least one of them is available and allows the NetIQ UNIX agent to communicate with the management server, an event is raised if any of the network interface cards goes down. In response to the event, you can configure this Knowledge script to run a managed client (MC) action to attempt to bring the NIC back online using the `ifconfig` command and the `Action_UXCommand` Knowledge Script.

You might also want to use this Knowledge Script in conjunction with other Knowledge Scripts, such as [NetInterfacesConnectivity](#) and [PingMachine](#) to fine-tune your troubleshooting.

---

**NOTE:** The NetInterfacesDown Knowledge Script does not alert you if all network interfaces are on computer are down until after network communication is restored. The Knowledge Script job still raises the event, but stores the event in the UNIX agent's local repository until communication with the management server resumes.

---

## 4.31 NetInterfacesErrors

Use this Knowledge Script to monitor the input and output errors for network interfaces. If the number of network interface input errors or output errors exceeds the threshold you set, AppManager raises an event.

This Knowledge Script runs on the Network Interface object. However, the NetInterfacesErrors Knowledge Script ignores the loopback device.

On Solaris, the UNIX agent must run as root or as a user with root-level authority to retrieve counters associated with the UX Networking performance object. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the sudo configuration file.

### 4.31.1 Resource Objects

Network Interface icon.

### 4.31.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.31.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if network interface input errors exceed the threshold? (y/n)	Set to <i>y</i> to raise an event if the percentage of network interface input errors exceeds the threshold. The default is <i>y</i> .
Collect data on input errors? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns the percentage of input errors for the interval. The default is <i>n</i> .
Maximum percentage of input errors (%) threshold	Specify the maximum percentage of network interface input errors that should be allowed before raising an event. The default is 80%.
Event if network interface output errors exceed the threshold? (y/n)	Set to <i>y</i> to raise an event if the percentage of network interface output errors exceeds the threshold. The default is <i>y</i> .
Collect data on output errors? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns the percentage of output errors for the interval. The default is <i>n</i> .
Maximum percentage of output errors (%) threshold	Specify the maximum percentage of network interface output errors that should be allowed before raising an event. The default is 80%.

Description	How to Set It
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default severity level is 15.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.32 NetInterfacesIO

Use this Knowledge Script to monitor the input and output rate for network interfaces in bytes per second. If the rate of network traffic for input, output, or both exceeds the threshold you set, AppManager raises an event. You cannot use this Knowledge Script in Solaris zones that are not global zones.

This Knowledge Script runs on the Network Interface object. However, the NetInterfacesIO Knowledge Script ignores the loopback device.

### 4.32.1 Resource Object

Network Interface icon

### 4.32.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.32.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event?	Select <b>Yes</b> to raise events. The default is Yes.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold settings</b>	
Bytes sent and received per second threshold	Specify a threshold for the maximum number of bytes sent and received per second to monitor the throughput rate for the network interface. The default is 8000000 bytes.
Bytes sent per second threshold	Specify a threshold for the maximum number of bytes sent per second. The default is 8000000 bytes.
Bytes received per second threshold	Specify a threshold for the maximum number of bytes received per second. The default is 8000000 bytes.

Description	How to Set It
Maximum network bandwidth utilization (%) threshold	Specify a threshold for the maximum percent of network bandwidth. The default is 10%.
<b>Collect data settings</b>	
Collect data for throughput per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of bytes sent and received per second for each interface. The default is unselected.
Collect data for bytes sent per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of bytes sent per second for each interface. The default is unselected.
Collect data for bytes received per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of bytes received per second for each interface. The default is unselected.
Collect data for network utilization?	For Solaris computers only. Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of bytes received per second for each interface. The default is unselected.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.33 OpenFiles

Use this Knowledge Script to monitor the number of files that are opened by a process in the system.

This Knowledge Script is supported on: [Linux].

### 4.33.1 Resource Objects

UNIX Machine folder

### 4.33.2 Default Schedule

The default interval for this script is **Once Every Hour**.

### 4.33.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the OpenFiles job fails. The default is 5.
List of processes (comma-separated)	Enter the list of comma-separated process names for which you want to monitor the number of files opened by the processes.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.

Description	How to Set It
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to retrieve the metrics. The default is 5.
<b>Event Settings</b>	
<b>Raise event if open file count exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the open file count threshold is exceeded. The default is Yes.
Threshold --Open file count	Enter the open file count threshold with a maximum value of 99999. The default is 800.
Severity	Set the severity level, from 1 to 40, to indicate the importance of an event when the number of files opened by a process exceeds the threshold. The default is 15.
<b>Data Collection</b>	
Collect data for open file count?	Select <b>Yes</b> to collect data for charts, graphs, and reports for the open file count data. When selected, this script returns the average number of files opened by processes that matched the specified process name. The default is unselected.
<b>NOTE:</b>	
<ul style="list-style-type: none"> <li>◆ The average number of open file counts of a specified process in a data point is 0 (zero) until an event is raised.</li> <li>◆ When an event is raised the data point at that moment contains the average of open file count of the specified processes and details of all the processes that have exceeded the threshold.</li> </ul>	

## 4.34 PagingHigh

Use this Knowledge Script to monitor UNIX paging activity. If the size in KB paged-in or paged-out per second exceeds the threshold you set, AppManager raises an event.

### 4.34.1 Resource Object

UNIX computer on Solaris, Linux, and HP-UX (not supported on AIX).

### 4.34.2 Default Schedule

The default interval for this script is **Every 10 minutes**.



### 4.34.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data on page-in KBytes per second? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the average size in KB paged-in per second. The default is <code>n</code> .
Collect data on page-out KBytes per second? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the average size in KB paged-out per second. The default is <code>n</code> .
Maximum paged-in KBytes per second threshold	Specify a threshold for the maximum size in KB for page-in swaps per second. The default is 200.
Maximum paged-out KBytes per second threshold	Specify a threshold for the maximum size in KB for page-out swaps per second. The default is 200.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.35 PhysicalDiskBusy

Use this Knowledge Script to monitor physical disk activity and average response time. A disk is considered busy if the percentage of time the disk is in operation is high or the average response time is over the threshold. With this Knowledge Script, you can monitor the load for individual disks or the overall load across all physical disks in a computer.

Total disk activity and average response time threshold are reported separately. Each detailed message will contain both values and the value exceeding the threshold will be mentioned.

---

**NOTE:** If the total disk activity or average response time threshold is exceeded, the disk is considered overloaded and AppManager raises an event.

---

### 4.35.1 Resource Objects

Physical disk folder or individual physical disks.

### 4.35.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

## 4.35.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data for physical disk busy? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the percentage of time the disk is busy and the average response time for requests. The default is <code>n</code> .
Collect data for average response time? (y/n) (unavailable on AIX)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the average response time for requests. The default is <code>n</code> .
Event if disk activity and response time over threshold? (y/n)	Set to <code>y</code> to raise events when both the disk activity and average response are over their respective thresholds. The default is <code>y</code> .
Average response time maximum threshold (unavailable on AIX)	Specify a threshold for the maximum response time in milliseconds. The default is 200 milliseconds. Do not use this parameter on computers running an AIX operating system.
Maximum physical disk activity (% busy) threshold	Specify a threshold for the maximum percentage of disk activity before raising an event. The default is 80% busy.
Monitor overall physical disk load? (y/n)	Set to <code>y</code> to monitor the overall disk load (for all physical disks on a system). Set to <code>n</code> to monitor individual disks separately. The default is <code>n</code> .
Event severity level	Specify the event severity level, from 0 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.36 PhysicalDiskIO

Use this Knowledge Script to monitor the physical disk I/O activity in kilobytes per second. The Knowledge Script monitors the size of physical disk reads and physical disk writes per second.

On Solaris, Linux, and AIX AppManager raises an event if the size of disk reads per second, the size of disk writes per second, or the overall throughput per second exceeds the threshold you set.

On HP-UX, this Knowledge Script only monitors overall throughput and raises an event if the total size of reads and writes per second is over the threshold.

---

**NOTE:** Oracle Solaris ZFS and ZFS Storage Pools file system monitoring is not available for this Knowledge Script.

---

### 4.36.1 Resource Object

Physical disk object

## 4.36.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 4.36.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event? (y/n)	Select <b>Yes</b> to raise events. The default is Yes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold settings Collection</b>	
Maximum reads per second (KB) threshold	Specify the threshold for the maximum rate of read operations in KB per second. The default is 50 KB per second.
Maximum writes per second (KB) threshold	Specify the threshold for the maximum rate of write operations in KB per second. The default is 50 KB per second.
Maximum throughput per second (KB) threshold	Specify the threshold for the maximum rate of read and write operations in KB per second. The default is 100 KB per second.
Maximum reads per second threshold	Specify the threshold for the maximum number of read operations per second. The default is 50 operations per second.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
Maximum writes per second threshold	Specify the threshold for the maximum number of write operations per second. The default is 50 operations per second.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
Maximum throughput per second threshold	Specify the threshold for the maximum number of read and write operations per second. The default is 100 operations per second.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
<b>Data Collection</b>	
Collect data for reads per second (KB)?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of disk read operations in KB per second for each disk. The default is unselected.
Collect data for writes per second (KB)?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of disk write operations in KB per second for each disk. The default is unselected.
Collect data for throughput per second(KB)?	Set to <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the rate of disk read and write operations in KB per second for each disk. The default is unselected.

Description	How to Set It
Collect data for reads per second?	Set to <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the number of disk read operations per second for each disk. The default is unselected.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
Collect data for writes per second?	Set to <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the number of disk write operations per second for each disk. The default is unselected.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
Collect data for throughput per second?	Set to <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the number of disk read and write operations per second for each disk. The default is unselected.  <b>NOTE:</b> This parameter is not supported on Solaris 11 or later versions.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.37 PhysicalDiskStats

Use this Knowledge Script to monitor physical disk activity and response time.

### 4.37.1 Resource Object

UNIX computer icon

### 4.37.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

### 4.37.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the UNIX_PhysicalDiskStats job fails. The default is 5.
Enable debugging	Select <b>Yes</b> to enable debugging. The default is unselected.
Event detail format	Set the format for the Event detail. <code>HTML Table</code> is the default.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to reflect the importance of the event if AppManager fails to get metrics. The default is 5.

Description	How to Set It
<b>Event Settings</b>	
<b>Event if average response time of disk operations exceeds threshold? (y/n)</b>	Select <b>Yes</b> to raise an event of the average response time of disk operations exceeds the threshold. The default is Yes.
Threshold - Maximum average response time (unavailable on AIX)	Specify the maximum average response time that can be detected before an event is raised. The default is 200 ms (milliseconds) average response time.
Event severity	Set the event severity level, from 1 to 40, to reflect the importance of the event if AppManager fails to get metrics. The default is 5.
Event if disk activity exceeds threshold? (y/n)	Select <b>Yes</b> to raise an event if the average response time of disk operations exceeds the threshold. The default is unselected.
Event severity	Set the event severity level, from 1 to 40, to reflect the importance of the event if AppManager fails to get metrics. The default is 5.
<b>Collect data settings</b>	
Collect data for average response time of disk operations?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the average response time of the disk operations. The default is unselected.
Collect data for physical disk load?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the physical disk load. If set to Yes, the script returns the physical disk load. The default is unselected.
Collect data for KBs read per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the KBs read per second. The default is unselected.
Collect data for KBs written per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the KBs written per second. If set to Yes, The default is unselected.
Collect data for reads per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the reads per second of the disk operations. The default is unselected.
Collect data for writes per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the writes per second of the disk operations. If set to Yes, the script returns the The default is unselected.
Collect data for throughput per second?	Select <b>Yes</b> to collect data for charts and reports. If set to Yes, the script returns the throughput per second of the disk operations. If set to Yes, the script returns the The default is unselected.

## 4.38 PingMachine

Use this Knowledge Script to check the availability of any computers or other devices that reply to ICMP Echo requests. (The ICMP Echo request is commonly used by the `ping` command on UNIX and Windows computers.) With this Knowledge Script, you can check the up/down status of your managed UNIX computers, Windows computers, and other equipment, such as TCP/IP-based printers.

You can specify computers to ping in two ways: by providing comma-separated lists or by naming files containing comma-separated lists. If a computer does not respond to a ping within the response time threshold, the script raises an event.

There are separate lists for UNIX and Windows computers. This separation allows the script to push raised events to computers listed in your TreeView: to do this, the script needs to know whether an event is destined for a UNIX or Windows computer. When an event is pushed to a computer listed in your TreeView, its icon blinks.

This script can raise an event for a computer that is not listed in your TreeView. When this happens, a server group named AppManager Proxy Events is automatically created in the Master TreeView. From this group, you can view, acknowledge, close, and delete all events on the computer. To discover resources and run monitoring jobs on the computer, you must delete the computer from the AppManager Proxy Events server group, then manually add the computer to the TreeView. If necessary, stop any proxy jobs that are monitoring the remote computer so you can add it to the TreeView.

## 4.38.1 Resource Object

UNIX computer icon

## 4.38.2 Default Schedule

The default interval for this script is **Every two hours**.

## 4.38.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
List of UNIX machines to check (by hostname or IP address)	Enter a list of UNIX computer names, separated by commas, that you want to test communication with. The default is <code>localhost</code> .
List of Windows machines to check (by hostname or IP address)	Enter a list of Windows computer names, separated by commas, that you want to test communication with. The default is blank.
Optional file listing UNIX hosts to ping	Type the full path to the file containing a list of the UNIX computers you want to check. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example, the contents of a file could be:  <code>NYC01, NYC02</code> <code>SALES01, 10.15.221.5, SFO01</code> <code>LABMACH, QATEST</code>  The default is blank.
Optional file listing Windows hosts to ping	Type the full path to the file containing a list of the Windows computers you want to check. The file should contain the hostname or IP address for each computer in one or more lines. Each line can have multiple computer names, separated by commas. For example, the contents of a file could be:  <code>NYC01, NYC02</code> <code>SALES01, 10.15.221.5, SFO01</code> <code>LABMACH, QATEST</code>  The default is blank.

Description	How to Set It
Collect data for response time? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns the time it took the server to respond to the <code>ping</code> command. The default is <i>n</i> .
Collect data for machine up/down? (y/n)	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the script returns: <ul style="list-style-type: none"> <li>◆ 100 -- Computer tested sent a reply indicating a successful connection, or</li> <li>◆ 0 -- There was no reply.</li> </ul> The default is <i>n</i> .
Event if response time exceeds the threshold? (y/n)	Set to <i>y</i> to raise an event if the response time from the computer whose connection you are testing exceeds the threshold you set. The default is <i>y</i> .
Event if the machine is not responding? (y/n)	Set to <i>y</i> to raise an event if the computer whose connection you are testing fails to respond to the Ping test. The default is <i>y</i> .
Maximum response time (ms) threshold	Enter a threshold for the maximum response time in milliseconds for the reply to take. The default is 500 milliseconds.
Event severity level when response time is exceeded	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when the response time threshold is crossed. The default severity is 15.
Event severity level when machine is unreachable	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when AppManager cannot communicate with the computer. The default severity is 5.
Number of times to ping target machine per iteration	Enter the number of times that you want to ping the target computer for each iteration. The default is 1.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.39 PortHealth

Use this Knowledge Script to check whether system ports are working properly. This Knowledge Script raises an event if a port is not operating properly.

There are separate lists for UNIX and Windows computers. This separation allows the script to push raised events to computers listed in your TreeView: to do this, the script needs to know whether an event is destined for a UNIX or Windows computer. When an event is pushed to a computer listed in your TreeView, its icon blinks.

This script can raise an event for a computer that is not listed in your TreeView.

---

**NOTE:** This Knowledge Script raises an event if a port specified for monitoring cannot be reached from the computer where you dropped the Knowledge Script. In addition to the event, the icon for the computer where you dropped the Knowledge Script blinks.

---

## 4.39.1 Resource Object

UNIX computer icon

## 4.39.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.39.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if port cannot be reached? (y/n)	Set to <b>y</b> to raise an event if a specified port is not operating properly. The default is <b>y</b> .
Collect data for port status? (y/n)	Set to <b>y</b> to collect data for graphs and reports. If enabled, returns: <ul style="list-style-type: none"><li>◆ 100 -- the port is operating properly, or</li><li>◆ 0 -- the port is not operating.</li></ul> The default is <b>n</b> .
Windows network addresses in format hostIP:port_number (comma-separated, no spaces)	Type one or more Windows network addresses using the format <i>host_IP:port_number</i> . Separate multiple addresses by commas and no spaces.  The <i>host_IP</i> can be a hostname or an IP address. For example: <code>www.storm.com:8008,21.1.10.1:30</code> . The default is <code>www.netiq.com:80</code> .
UNIX network addresses in format hostIP:port_number (comma-separated, no spaces)	Type one or more UNIX network addresses using the format <i>host_IP:port_number</i> . Separate multiple addresses by commas and no spaces.  The <i>host_IP</i> can be a hostname or an IP address. For example: <code>www.storm.com:8008,21.1.10.1:30</code> .
Event severity when port cannot be reached	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <b>y</b> to enable debugging. The default is <b>n</b> .

## 4.40 PrinterQueue

Use this Knowledge Script to monitor the health of printers. This Knowledge Script checks the number of jobs in printer queue and the size of the printer queue in KB. If either the number of jobs waiting or the queue size exceeds the threshold you set, AppManager raises an event.

**NOTE:** General printer status information, such as when the printer is taken off-line or is low on toner, cannot be detected by this Knowledge Script.



## 4.40.1 Resource Objects

UNIX Printer objects

## 4.40.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.40.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if printer queue exceeds the threshold? (y/n)	Set to <i>y</i> to raise an event if the number of jobs in the printer queue exceeds the threshold. The default is <i>y</i> .
Event if printer queue size (KB) exceeds the threshold? (y/n)	Set to <i>y</i> to raise an event if the size of the printer queue, in KB, exceeds the threshold. The default is <i>y</i> .
Collect printer queue length data?	Set to <i>y</i> to collect data for charts and reports. The default is <i>n</i> . If you collect data, the Knowledge Script reports the number of print jobs in the queue at each interval.
Collect printer queue size data?	Set to <i>y</i> to collect data for charts and reports. If set to <i>y</i> , the Knowledge Script reports the size in KB of the printer queue at each interval. The default is <i>n</i> .
Maximum number of jobs in the printer queue threshold	Enter a threshold for the maximum number of print jobs waiting in the queue. The default is 100 jobs.
Maximum printer queue size (KB) threshold	Enter a threshold for the maximum size of the printer queue in KB. The default is 4000 KB.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.41 PrivilegedProcs

Use this Knowledge Script to monitor the number of system processes with an effective user ID (*eid*) of *root*. You can specify one or more processes to exclude from the list, if needed. If the number of processes running under *root* is over the threshold you set, AppManager raises an event.

### 4.41.1 Resource Object

UNIX CPU folder

### 4.41.2 Default Schedule

The default interval for this script is **Every hour**.

## 4.41.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold? (y/n)	Set to <code>y</code> to raise an event if the number of processes running under the root user exceeds the threshold. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the Knowledge Script reports the number of processes owned by the root user at each interval. The default is <code>n</code> .
Maximum number of processes owned by root threshold	Enter a threshold for the maximum number of processes owned by the root user. The default is 30 processes.
Processes to exclude separated by commas	Enter the processes you want to exclude from the list of processes owned by root. Use a comma with no spaces to separate process names.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.42 ProcessDown

Use this Knowledge Script to determine whether specified processes are currently running. AppManager raises an event if a specified process is not running or if the minimum number of processes are not running.

### 4.42.1 Resource Object

UNIX CPU folder

### 4.42.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.42.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event if the process is not running? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data for processes not running? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns data for each named process. A value of 100 is returned if the process is running; a value of 0 is returned if the process is not running. The default is <code>n</code> .

Description	How to Set It
Processes to monitor (comma-separated)	Enter one or more process names, separated by commas and no spaces. For example:  <code>grep, batch</code>
Minimum number of each process required (comma-separated)	Enter the minimum number of instances that have to go down before you want AppManager to raise an event. If you are monitoring more than one process, list the numbers for each process separated by commas and no spaces. The default is 1. For example, if you do not want to raise an event every time the grep and batch processes goes down, but you do want to raise an event after 10 instances of the process go down, enter:  <code>10, 10</code>
Event severity when process is down	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <b>y</b> to enable debugging. The default is n.

## 4.43 Processes

Use this Knowledge Script to monitor the number of processes. If the total number of processes detected exceeds the threshold you set, AppManager raises an event.

### 4.43.1 Resource Object

UNIX CPU folder

### 4.43.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.43.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold? (y/n)	Set to <b>y</b> to raise events. The default is y.
Collect data? (y/n)	Set to <b>y</b> to collect data for charts and reports. If set to y, the script returns the total number of processes running on the system. The default is n.
Maximum number of processes threshold	Enter a threshold for the maximum number of processes. The default is 100 processes.
Monitor process count for just specified user	Specify a user account if you want to monitor the number of processes started by that user.

Description	How to Set It
Processes to exclude separated by commas	Enter the names of any processes you want to exclude from the list of processes found. Use a comma with no spaces to separate process names.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.44 ProcessUp

Use this Knowledge Script to check whether a specified process is running. If the specified process is running, AppManager raises an event. You also have the option to automatically terminate the process.

This Knowledge Script requires the UNIX agent to run as the root user account.

### 4.44.1 Resource Object

UNIX CPU folder

### 4.44.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.44.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise an event if the process is running? (y/n)	Set to <i>y</i> to raise events. The default is <i>y</i> .
Collect data for processes running? (y/n)	Select <b>Yes</b> to collect data for charts and reports. If set to <i>y</i> , the script returns a value of 100 when the number of running processes exceeds the threshold, or a value of 0 when the number of running process does not exceed the threshold. The default is unselected.
Processes for which to look (comma-separated)	Enter one or more process names, separated by commas and no spaces. For example:  <code>grep, batch</code>
Maximum number of each process required (comma-separated)	Enter the number of instances required to generate an event for each process, separated by commas and no spaces. AppManager reports an event when the number of instances is running for each process. The default is 0,0. For example:  <code>3, 4</code>

Description	How to Set It
Kill the running process? (y/n)	Select <b>Yes</b> to kill the specified processes if they are detected running. The default is unselected.
Event severity level for process running	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when AppManager identifies the specified process as being up. The default is 10.
Event severity level for failed to kill process	Set the event severity level, from 1 to 40, to indicate the importance of the event reported when AppManager identifies the specified process as being up and but the attempt to kill the process failed. The default is 10.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.45 RemoteProcessDown

Use this Knowledge Script to monitor processes on a remote UNIX computer where you have not installed the UNIX agent. This Knowledge Script runs on a proxy UNIX agent and monitors processes on a remote UNIX computer.

When you drag this Knowledge Script to a UNIX computer in the TreeView, the Knowledge Script runs on that computer and tries to communicate with a specified list of remote UNIX computers. This Knowledge Script raises an event if any of the named processes are down or any of the computers you specify cannot be reached from the computer where this Knowledge Script is running.

If a monitored process is found to be down, this Knowledge Script can restart it using a script or command you supply. Be sure to read the help for the **Scripts or commands to restart processes** parameter, below, before proceeding.

This Knowledge Script requires the UNIX agent to run as the root user account.

### 4.45.1 Resource Object

UNIX computer icon (not supported on HP-UX Itanium).

### 4.45.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

If the script used to restart any process found to be down takes a considerable amount of time, events generated by the job are generated more than 10 minutes apart (by default).

### 4.45.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Notification</b>	
Raise event if process is down?	Select <b>Yes</b> to raise an event if the monitored process is found to be down. The default is Yes.

Description	How to Set It
<b>Event severity when process is down</b>	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Raise event if process is running?	Select <b>Yes</b> to raise an event if the monitored process is found to be running. The default is unselected.
Event severity when process is running	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
<b>Remote Host Connection</b>	
Configure access to the remote managed computers by specifying their root password. All of the remote computers must use the same root password. This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.	
Password for root user account	<p>If you want to use Secure Shell (SSH) for the connection to the remote computers, make sure SSH with root authentication is enabled on the remote UNIX computers where you want to install the UNIX agent.</p> <p>For this parameter, you must specify the password for the root user to securely access the remote UNIX computers. This Knowledge Script does not support SSH root authentication with an RSA key.</p>
<b>Connection Transport</b>	<p>Select either SSH/SFTP or Telnet/FTP. The default is Telnet/FTP,</p> <p>This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.</p> <p>If you select the Telnet/FTP option the Telnet prompt on the remote computer must end with a space or one of the following characters: % &gt; # \$</p> <p>This example shows a supported Telnet prompt:</p> <pre>user@hostname&gt;</pre> <p>This example shows an unsupported Telnet prompt:</p> <pre>&lt;user@hostname:/tmp - 2005-Mar-09&gt; -&gt;</pre> <p>In the examples above, the last character in the first line of the 2-line prompt is a line feed character, which is not supported.</p>
Telnet non-root user account	If you selected Telnet to connect to the remote UNIX computers, specify a non-root user account to use for the connection. When connecting to a remote UNIX computer using Telnet and FTP, this Knowledge Script switches from the non-root user to the root user.
Telnet non-root user password	If you selected Telnet as the connection transport medium, specify the password for the non-root user account to connect to the remote UNIX computers.
<b>Proxy Monitoring Configuration</b>	
Full path to configuration file for remote monitoring	<p>Supply a full directory path to an XML file to use for monitoring instructions.</p> <p>The configuration file should specify which processes to monitor on the remote UNIX computer and how to restart them. See <a href="#">Section 4.45.5, "Remote Process Monitoring Using a Configuration File,"</a> on page 112 for more information about the configuration file.</p> <p>The default is <code>/tmp/config.xml</code>.</p>

Description	How to Set It
<b>Proxy Monitoring without Configuration File</b>	
Hostnames or IP addresses where processes are to be monitored (comma-separated)	<p>Enter a list of hostnames or IP addresses of the UNIX computers where processes are to be monitored.</p> <p>Separate multiple hostnames with commas (,) and no spaces.</p> <p>Supply IP addresses in dotted notation, such as 23.45.678.9. Separate multiple IP addresses with commas and no spaces.</p>
Names of processes to monitor (comma-separated)	<p>Supply the names of the UNIX application processes to monitor. Separate multiple process names with commas and no spaces.</p> <p>You can also enter a Perl regular expression here if you want to exclude and include processes on various platforms through the use of one argument. See <a href="#">Section 4.45.4, "Running this Knowledge Script," on page 112</a> for more information.</p>
Scripts or commands to restart processes (comma-separated)	<p>Supply one of the following:</p> <ul style="list-style-type: none"> <li>◆ a list of full directory paths to script files to use to restart any processes that are found to be down, or</li> <li>◆ a list of commands to use to restart these processes.</li> </ul> <p>Use this parameter only when you restart the process when it is down.</p> <p>Specify a list of restart commands or shell scripts that contain the restart commands. Do not execute restart commands in the foreground. When executing a restart command in the foreground, this Knowledge Script cannot run at its next scheduled interval until after all of the restart commands have completed. When specifying:</p> <ul style="list-style-type: none"> <li>◆ A list of commands to run on the remote computer, run each command in the background by appending an ampersand (&amp;) and separate each command with a comma. If this Knowledge Script is configured to use Telnet/FTP, you can restart a process in the background by appending an ampersand (&amp;) to each command. If this Knowledge Script is configured to use SSH/SFTP, you should use a shell script on the remote computer to restart the processes in the background and ensure that <code>stdout</code> and <code>stderr</code> are redirected to a log file. When configured to use SSH/SFTP, this Knowledge Script always executes a command to restart a process in the foreground.</li> <li>◆ A shell script on the remote computer that restarts the processes you want, in the shell script, append an ampersand (&amp;) to each restart command--and ensure that <code>stdout</code> and <code>stderr</code> are redirected to a log file--to restart a process in the background.</li> </ul>
Restart process if down? (y/n for each process, comma-separated)	<p>Provide a list specifying "y" or "n" for each process in the list of processes to monitor. Specify y for a process if you want this Knowledge Script to restart it on the remote computer if it is found to be down. The commands or scripts you specified for the previous parameter are used. Separate each entry in the list with a comma. Do not use spaces.</p>
Enable debugging? (y/n)	<p>Set to <b>y</b> to enable debugging. The default is n.</p>

## 4.45.4 Running this Knowledge Script

This Knowledge Script requires the proxy UNIX agent to run as the root user account.

It can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX computer(s). By default, Telnet is used, but you can select SSH/SFTP from the **Connection Transport** list to use Secure Shell instead. If you choose to use Telnet, you must supply a non-root user account name and password.

---

**NOTE:** Proxy monitoring with this Knowledge Script is possible only if the SSH program is installed on the target computer, or if the Telnet protocol is enabled on it.

A version of this Knowledge Script that runs on a Windows proxy computer to monitor remote UNIX computers is also available. See the `NT_UnixRemoteProcessDown` Knowledge Script.

---

You can use this Knowledge Script to monitor the up and down status of the UNIX agent. To do this, specify `nqmagt` in the list of processes you want to monitor. If the `nqmagt` process is detected down, you can specify a restart command, `/etc/init.d/nqmdaemon start`, to restart the agent.

You can specify the process names to be monitored as a parameter, or you can provide a configuration file in XML format to specify processes to monitor and what steps to take to restart them if they are down. See [Section 4.45.5, “Remote Process Monitoring Using a Configuration File,”](#) on [page 112](#) for more information about the configuration file.

You can also supply a Perl regular expression for the **Names of processes to monitor (comma-separated)** parameter if you want to check for a specific string. For example, you can exclude and include processes on various platforms through the use of one argument. For example, assume that a process is running out of the `/usr`, the `/opt`, or the `/var` directory, but you are not sure where. You can enter `(/usr|/opt)/[processname]` for the **Names of processes to monitor** parameter. The Knowledge Script would monitor the process that is running in `/usr` OR in `/opt` but NOT in `/var`. The topic titled [Section 4.1, “Creating Filters with Regular Expressions,”](#) on [page 46](#) contains more information about regular expressions.

## 4.45.5 Remote Process Monitoring Using a Configuration File

The `RemoteProcessDown` Knowledge Script includes an option to use a configuration file in XML format to supply monitoring instructions to the agent. In such a file, you can supply a list of processes to monitor on a given remote UNIX computer, specify how to restart these processes, and indicate whether to restart these processes.

By default, the Knowledge Script looks for the following configuration file:

```
/tmp/config.xml
```

However, you can supply a different file as the value for the **Full path to configuration file for remote monitoring** parameter.



Following is an example of a valid XML configuration file that instructs the UNIX agent which processes to monitor and what to do if they are not running:

```
<?xml version="1.0" encoding="utf-8" ?>
<SERVERS>
  <SERVER name="uws3">
    <PROCESS name="ngmagt" startupscript="/etc/init.d/ngmdaemon start" restart="y"/>
    <PROCESS name="xntpd" startupscript="/etc/init.d/xntpd start" restart="n"/>
  </SERVER>
  <SERVER name="uws19">
    <PROCESS name="inetd" startupscript="/etc/init.d/inetsvc start" restart="n"/>
    <PROCESS name="init" startupscript="/etc/init.d/init start" restart="n"/>
  </SERVER>
</SERVERS>
```

## 4.46 Report\_CPULoad

Use this Knowledge Script to generate a detailed report about CPU usage. Using this report, you can aggregate the data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the [CpuLoaded](#) Knowledge Script.

### 4.46.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

### 4.46.2 Default Schedule

The default schedule for this script is **Run once**.

### 4.46.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report.
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.

Description	How to Set It
Select the style	<p>Select the style for the first page of your report:</p> <ul style="list-style-type: none"> <li>◆ <b>By computer</b> provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer).</li> <li>◆ <b>By data stream</b> provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the <i>UNIX_CpuResource-All Threads(#)</i> data stream from each computer).</li> <li>◆ <b>By computer and data stream</b> provides links to pages showing a single data stream collected from a computer.</li> <li>◆ <b>All data streams on one page</b> provides all the data streams on a single page.</li> </ul> <p>The default is By computer.</p>
Select time range	<p>Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.</p>
Select peak weekday(s)	<p>Click the <b>Browse [...]</b> button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.</p>
Aggregation by	<p>Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is Hour.</p>
Aggregation interval	<p>Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.</p>
Statistics to show per period	<p>Select a statistical method by which to display data in your report:</p> <ul style="list-style-type: none"> <li>◆ <b>Average</b>. The average value of data points for the aggregation interval (for example, the average value for 1 Hour).</li> <li>◆ <b>Minimum</b>. The minimum value of data points for the aggregation interval.</li> <li>◆ <b>Maximum</b>. The maximum value of data points for the aggregation interval.</li> <li>◆ <b>Count</b>. The number of data points for the aggregation interval.</li> <li>◆ <b>Sum</b>. The total value of data points for the aggregation interval.</li> <li>◆ <b>3Sigma</b>. The average + (3 * standard deviation) and average - (3 * standard deviation).</li> <li>◆ <b>Std</b>. The standard deviation. The measure of how widely values are dispersed from the mean.</li> <li>◆ <b>Box</b>. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval.</li> <li>◆ <b>Open</b>. The first value for the aggregation interval.</li> <li>◆ <b>Close</b>. The last value for the aggregation interval.</li> </ul> <p>The default is Average.</p>
<b>Report settings</b>	<p>Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.</p>

Description	How to Set It
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. By default, the table is included.
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the <b>Browse [...]</b> button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the <b>Browse [...]</b> button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_CPUload.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no.  Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box and select the properties as desired. The default title for your report is UNIX CPU Load.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp includes the date and time the report was generated. The default is no.  Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. The default is <i>y</i> .
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.47 Report\_DiskUsageSummary

Use this Knowledge Script to generate a summary report about the percentage of disk space used and the amount of free space (in MB). Using this report, you can develop a statistical summary of the data you select, for example, the average value of data points over the time period you define for the report.

This report uses data collected by the [FileSystemSpace](#) Knowledge Script.

## 4.47.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

## 4.47.2 Default Schedule

The default schedule for this script is **Run once**.

## 4.47.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report.
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.
Select time range	Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the <b>Browse [...]</b> button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Select the style	Select the style for the first page of your report: <ul style="list-style-type: none"><li>◆ <b>By computer</b> displays one value for each computer you selected.</li><li>◆ <b>By legend</b> displays one value for each different legend (the legend is a truncated form of the data stream legend visible in the Operator Console).</li><li>◆ <b>By computer and legend</b> displays one value for each unique legend from each computer.</li></ul> The default is <code>By computer and legend</code> .
<b>Data settings</b>	Use the following parameters to select the data settings for your report.

Description	How to Set It
Statistics to show	<p>Select a statistical method by which to display data in your report:</p> <ul style="list-style-type: none"> <li>◆ <b>Average.</b> The average value of data points for the time range of the report.</li> <li>◆ <b>Minimum.</b> The minimum value of data points for the time range of the report.</li> <li>◆ <b>Maximum.</b> The maximum value of data points for the time range of the report.</li> <li>◆ <b>Min/Avg/Max.</b> The minimum, average, and maximum values of data points for the time range of the report.</li> <li>◆ <b>Range.</b> The range of values in the data stream (maximum - minimum = range).</li> <li>◆ <b>StandardDeviation.</b> The measure of how widely values are dispersed from the mean.</li> <li>◆ <b>Sum.</b> The total value of data points for the time range of the report.</li> <li>◆ <b>Close.</b> The last value for the time range of the report.</li> <li>◆ <b>Change.</b> The difference between the first and last values for the time range of the report (close - open = change).</li> <li>◆ <b>Count.</b> The number of data points for the time range of the report.</li> </ul>
	The default is <i>Average</i> .
Select sorting or display options	<p>Specify whether you want to sort data in your report or how you want to display the data:</p> <ul style="list-style-type: none"> <li>◆ <b>No sort.</b> Data is not sorted.</li> <li>◆ <b>Sort.</b> Data is sorted by value (lowest to highest from front to back; highest to lowest from left to right).</li> <li>◆ <b>Top %.</b> Chart only the top N % of selected data (sorted by default).</li> <li>◆ <b>Top N.</b> Chart only the top N of selected data (sorted by default).</li> <li>◆ <b>Bottom %.</b> Chart only the bottom N % of data (sorted by default).</li> <li>◆ <b>Bottom N.</b> Chart only the bottom N of selected data (sorted by default).</li> </ul>
	The default is <i>No sort</i> .
Percentage (%) or count for top or bottom of chart	Type a number for either the percent or count defined in <b>Select sorting or display options</b> (for example, Top 10%, or Top 10). The default is 25.
Truncate top or bottom? (yes/no)	Specify whether you want to truncate the top or bottom data in your report. If set to <i>y</i> ., the data table displays only the top or bottom N or % (for example, only the top 10%). If set to <i>no</i> , the table displays all data. The default is <i>n</i> .

Description	How to Set It
Show totals on the table? (yes/no)	<p>Specify whether you want to display additional calculations for each column of numbers in a table. If set to yes, the following values are listed at the end of the table:</p> <ul style="list-style-type: none"> <li>◆ <b>Report Average.</b> An average of all values in a column.</li> <li>◆ <b>Report Minimum.</b> The minimum value in a column.</li> <li>◆ <b>Report Maximum.</b> The maximum value in a column.</li> <li>◆ <b>Report Total:</b> The total of all values in a column.</li> </ul> <p>The default is no.</p>
<b>Report settings</b>	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. The default is <i>y</i> .
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. The default is <i>y</i> .
Select chart style	Click the <b>Browse [...]</b> button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is <i>Bar</i> .
Select output folder	Click the <b>Browse [...]</b> button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is <i>UNIX_LogicalDiskUsageSummary</i> .
Add job ID to output folder name? (yes/no)	<p>Specify whether you want to add the job ID to the report's output folder name. The default is no.</p> <p>Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.</p>
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box and select the properties as desired. The default title for your report is <i>UNIX Logical Disk Usage Summary</i> .
Add time stamp to title? (yes/no)	<p>Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is <i>n</i>.</p> <p>Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.</p>
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. The default is <i>y</i> .
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.

Description	How to Set It
Enable debugging? (y/n)	Set to <b>y</b> to enable debugging. The default is n.

## 4.48 Report\_MemoryUtilization

Use this Knowledge Script to generate a report about the use of physical and virtual memory, and paging files. Using this report, you can aggregate data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the [MemUtil](#) Knowledge Script.

### 4.48.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

### 4.48.2 Default Schedule

The default schedule for this script is **Run once**.

### 4.48.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report.
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	<p>Select the style for the first page of your report:</p> <ul style="list-style-type: none"> <li>◆ <b>By computer</b> provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer)</li> <li>◆ <b>By data stream</b> provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the <i>UNIX_CpuResource-All Threads(#)</i> data stream from each computer)</li> <li>◆ <b>By computer and data stream</b> provides links to pages showing a single data stream collected from a computer</li> <li>◆ <b>All data streams on one page</b> provides all data streams on a single page</li> </ul> <p>The default is By computer.</p>
Select time range	Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the <b>Browse [...]</b> button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.

Description	How to Set It
Aggregation by	Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is Hour.
Aggregation interval	Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.
Statistics to show per period	<p>Select a statistical method by which to display data in your report:</p> <ul style="list-style-type: none"> <li>◆ <b>Average.</b> The average value of data points for the aggregation interval (for example, the average value for 1 Hour).</li> <li>◆ <b>Minimum.</b> The minimum value of data points for the aggregation interval.</li> <li>◆ <b>Maximum.</b> The maximum value of data points for the aggregation interval.</li> <li>◆ <b>Count.</b> The number of data points for the aggregation interval.</li> <li>◆ <b>Sum.</b> The total value of data points for the aggregation interval.</li> <li>◆ <b>3Sigma.</b> The average + (3 * standard deviation) and average - (3 * standard deviation).</li> <li>◆ <b>Std.</b> The standard deviation. The measure of how widely values are dispersed from the mean.</li> <li>◆ <b>Box.</b> Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval.</li> <li>◆ <b>Open.</b> The first value for the aggregation interval.</li> <li>◆ <b>Close.</b> The last value for the aggregation interval.</li> </ul> <p>The default is Average.</p>
<b>Report settings</b>	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. The default is <i>y</i> .
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. The default is <i>y</i> .
Select chart style	Click the <b>Browse [...]</b> button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the <b>Browse [...]</b> button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is UNIX_MemoryUtilization.
Add job ID to output folder name? (yes/no)	<p>Specify whether you want to add the job ID to the report's output folder name. The default is no.</p> <p>Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.</p>
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box and select the properties as desired. The default is UNIX Memory Utilization.



Description	How to Set It
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is <i>n</i> .  Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. The default is <i>y</i> .
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.49 Report\_NetInterfacesIO

Use this Knowledge Script to generate a report about the use of bandwidth on network interface cards. Using this report, you can aggregate data by time period (minute, hour, or day) and calculate statistics for each period (for example, the average value per hour).

This report uses data collected by the [NetInterfacesIO](#) Knowledge Script.

### 4.49.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

### 4.49.2 Default Schedule

The default schedule for this script is **Run once**.

### 4.49.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report.
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.

Description	How to Set It
Select the style	<p>Select the style for the first page of your report:</p> <ul style="list-style-type: none"> <li>◆ <b>By computer</b> provides links to pages showing the data collected from individual computers (each page shows all the data streams collected from a single computer)</li> <li>◆ <b>By data stream</b> provides links to pages showing a side-by-side comparison of values for the same data stream collected from different computers (each page shows, for example, the value of the <i>UNIX_CpuResource-All Threads(#)</i> data stream from each computer)</li> <li>◆ <b>By computer and data stream</b> provides links to pages showing a single data stream collected from a computer</li> <li>◆ <b>All data streams on one page</b> provides all the data streams on a single page</li> </ul> <p>The default is By computer.</p>
Select time range	<p>Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.</p>
Select peak weekday(s)	<p>Click the <b>Browse [...]</b> button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.</p>
Aggregation by	<p>Specify how you want to aggregate the data in your report. You can specify Minute, Hour, or Day. The default is hour.</p>
Aggregation interval	<p>Specify the intervals you want to use to aggregate the data in your report. You can specify 1-5, 7, 8, 10, 12, 14, 15, 24, 28, 30, 60, or 90. The default is 1.</p>
Statistics to show per period	<p>Select a statistical method by which to display data in your report:</p> <ul style="list-style-type: none"> <li>◆ <b>Average</b>. The average value of data points for the aggregation interval (for example, the average value for 1 Hour).</li> <li>◆ <b>Minimum</b>. The minimum value of data points for the aggregation interval.</li> <li>◆ <b>Maximum</b>. The maximum value of data points for the aggregation interval.</li> <li>◆ <b>Count</b>. The number of data points for the aggregation interval.</li> <li>◆ <b>Sum</b>. The total value of data points for the aggregation interval.</li> <li>◆ <b>3Sigma</b>. The average + (3 * standard deviation) and average - (3 * standard deviation).</li> <li>◆ <b>Std</b>. The standard deviation. The measure of how widely values are dispersed from the mean.</li> <li>◆ <b>Box</b>. Lower fence, 25% point, median, 75% point, and upper fence for the aggregation interval.</li> <li>◆ <b>Open</b>. The first value for the aggregation interval.</li> <li>◆ <b>Close</b>. The last value for the aggregation interval.</li> </ul> <p>The default is Average.</p>
<b>Report settings</b>	<p>Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.</p>

Description	How to Set It
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. The default is <i>y</i> .
Include table/chart/both?	Select whether you want to include a table, a chart, or both of data stream values in the report. The default is <i>y</i> .
Select chart style	Click the <b>Browse [...]</b> button to open the Chart Settings dialog box and select the graphic properties for the charts in your report. The default is Bar.
Select output folder	Click the <b>Browse [...]</b> button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default folder prefix is <code>UNIX_NetInterfacesTraffic</code> .
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no.  Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box and select the properties as desired. The default title for your report is Network Interface Card Traffic.
Add time stamp to title? (yes/no)	Specify whether you want to append a time stamp to the title of your report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is no.  Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. By default, events are enabled.
Event severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Event severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Event severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.
Enable debugging? (y/n)	Set to <b>y</b> to enable debugging. The default is <i>n</i> .

## 4.50 Report\_SystemUpTime

Use this UNIX Report Script to generate a report detailing the uptime and downtime of monitored computers. Uptime and downtime are illustrated in hours and minutes, as well as the percentage of the monitoring interval during which a computer is running or not. For example, if during a 24-hour monitoring interval, the computer is running for 18 hours and not running for 6 hours, the uptime and downtimes are represented as:

- ◆ Uptime: 18 hours 0 minutes
- ◆ Downtime: 6 hours 0 minutes

- ◆ Uptime: 75%
- ◆ Downtime: 25%

This report uses data collected by the [SystemUpTime](#) Knowledge Scripts. In order to have accurate data for this report, these Knowledge Scripts should be scheduled to run every 5 minutes.

Uptime and downtime are calculated during scheduled maintenance. Ad hoc maintenance is considered as downtime, and is included in all calculations.

## 4.50.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

## 4.50.2 Default Schedule

The default schedule is **Run once**.

## 4.50.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report.
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.
Select the style	<p>Select the style for the first page of the report:</p> <ul style="list-style-type: none"> <li>◆ <b>By computer and data stream</b> provides links to pages showing a single data stream collected from a computer</li> <li>◆ <b>All data streams on one page</b> generates a report with all data on a single page</li> </ul> <p>The default is By computer and data stream.</p>
Select time range	Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
Select peak weekday(s)	Click the <b>Browse [...]</b> button to start the day wizard. Use the day wizard to select the days of the week to include in your report. The default is seven days: Sunday through Saturday.
Aggregation interval	<p>Select the time period by which the data in your report is aggregated:</p> <ul style="list-style-type: none"> <li>◆ Hourly</li> <li>◆ Daily</li> <li>◆ Weekly</li> </ul> <p>The default is Hourly.</p>
<b>Report settings</b>	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.

Description	How to Set It
Include parameter help card? (y/n)	Set to <code>y</code> to include a card in the report that lists parameter settings for the report script. The default is to include the card.
Include table/chart/both	Select whether you want to include a table, a chart, or both of data stream values in the report. By default, the table is included.
Select chart style	Click the <b>Browse [...]</b> button to open the Chart Settings dialog box. Define the graphic properties of the charts in your report. The default is a line chart.
Select output folder	Click the <b>Browse [...]</b> button to set parameters for the output folder. The default output folder prefix is <code>SystemUpTime</code> .
Add job ID to output folder name? (y/n)	Set to <code>y</code> to append the job ID to the name of the output folder. The default is <code>n</code> .  This is helpful to make the correlation between a specific instance of a Report Script and the corresponding report.
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box. Set the properties parameters as desired. The default report title is <code>SystemUpTime</code> .
Add time stamp to title? (y/n)	Set to <code>y</code> to append a time stamp to the title of the report, making each title unique. The time stamp is made up of the date and time the report was generated. The default is <code>n</code> .  Adding a time stamp is useful in order to run consecutive iterations of the same report without overwriting previous output.
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (y/n)	Set to <code>y</code> to raise an event when the report is successfully generated. The default is <code>y</code> .
Severity level for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Severity level for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Severity level for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.51 Report\_TopMemoryProcs

Use this Knowledge Script to generate a report about the total memory used by all processes and which processes consume the most memory resources.

This report uses data collected by the [TopMemoryProcs](#) Knowledge Script.

### 4.51.1 Resource Objects

Report Agent > AM Repositories > *AppManager repository*.

## 4.51.2 Default Schedule

The default schedule for this script is **Run once**.

## 4.51.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Data source</b>	Use the following parameters to select the data for your report
Select computer(s)	Click the <b>Browse [...]</b> button to start the data wizard. Use the data wizard to select the computers for your report.  <b>NOTE:</b> For this report, select only one View, and up to 15 computers or server groups. The data wizard allows you to select more, but if you do, the Finish button is disabled. This mechanism prevents you from selecting too much data for the report.
Select time range	Click the <b>Browse [...]</b> button to start the time wizard. Use the time wizard to set a specific or sliding time range for data included in your report. The default is 1 day sliding time ending at the current time.
<b>Report settings</b>	Use the following parameters to define the graphical presentation of data, the folder where the report is generated, and properties that identify the report.
Include parameter help card? (yes/no)	Specify whether you want to include a table in the report that lists parameter settings for the report script. The default is <i>y</i> .
Select output folder	Click the <b>Browse [...]</b> button to open the Publishing Options dialog box and select the parameters for your report's output folder. The default prefix for the folder name is UNIX_TopMemoryProcs.
Add job ID to output folder name? (yes/no)	Specify whether you want to add the job ID to the report's output folder name. The default is no.  Add the job ID to the output folder name to help make the correlation between a specific instance of a Report Script and the corresponding report easier.
Select properties	Click the <b>Browse [...]</b> button to open the Report Properties dialog box and select the properties as desired. The default title is UNIX Top Memory Utilization by Process.
<b>Event notification</b>	Use the following parameters to raise events associated with generating the report, and to set severity levels for those events.
Event for report success? (yes/no)	Specify whether you want to raise an event if the report is successfully generated. The default is <i>y</i> .
Severity for report success	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report is successful. The default is 35.
Severity for report with no data	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report has no information in it. The default is 25.
Severity for report failure	Set the event severity level, from 1 to 40, to indicate the importance of the event when the report fails. The default is 5.
Enable debugging? (y/n)	Set to <i>y</i> to enable debugging. The default is <i>n</i> .

## 4.52 RunAwayProcs

Use this Knowledge Script to detect runaway processes on the specified computer by repeatedly sampling CPU usage for processes. If a process exceeds the CPU threshold in the number of consecutive samples taken (one at each interval), AppManager raises an event.

For example, if this Knowledge Script detects that a process has exceeded the CPU threshold for five consecutive monitoring periods, it might indicate that the process is trapped in an infinite loop or has encountered other problems. In addition to generating an event to notify you of the problem, you can optionally kill any detected runaway processes. The detail message shows the list of processes being sampled.

The UNIX agent must run under a root account for this script to kill runaway processes.

### 4.52.1 Resource Object

UNIX computer icon

### 4.52.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.52.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. The default is <code>n</code> .
Maximum CPU usage (%) for runaway processes	Enter a threshold for the maximum percentage of CPU any process should be using when sampled. This percentage is used to determine which processes are runaway processes. The default is 90%.
Number of consecutive samples to take	Enter the number of consecutive samples you want taken before raising an event. The default is 3 samples.
Number of runaway processes to show (0 = all)	Specify the number of processes you want displayed in detail event or data message. Enter 0 if you want all processes displayed. The default is 0 for all processes.
Ignore these comma-separated processes	Enter the names of any processes (separated by commas and no spaces) you want to exclude from sampling.
Never kill these comma-separated processes	Enter the names of any processes (separated by commas and no spaces) that should never be killed.  The default processes are <code>sched</code> , <code>init</code> , <code>pageout</code> , <code>fsflush</code> , <code>inetd</code> , <code>yp</code> , and <code>rpc</code> .
Kill runaway process when detected? (y/n)	Set to <code>y</code> to kill any runaway processes found automatically (with the exception of the processes you have specified should never be killed). The default is <code>n</code> .

Description	How to Set It
Event severity level for runaway process detected	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a runaway process is detected. The default is 5.
Event severity level for killed runaway process	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a runaway process is stopped. The default is 10.
Event severity level for failed to kill runaway process	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when stopping a runaway process fails. The default is 10.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.53 RunCommand

Use this Knowledge Script to run a non-interactive UNIX command. For example, you can use this Knowledge Script to run a batch command that appends a log file or kills a process.

This Knowledge Script raises an event if the results of the command produce output. You can configure this Knowledge Script to not raise an event if the results of the command do not produce any output.

### 4.53.1 Resource Object

UNIX computer icon

### 4.53.2 Default Schedule

By default, this script is only run once per computer.

### 4.53.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event displaying text sent to STDOUT? (y/n)	Specify whether you want to raise an event containing the <code>STDOUT</code> of the executed command. The default is <code>y</code> .
Include <code>STDERR</code> in event text? (y/n)	Specify whether you want to include the <code>STDERR</code> of the command along with the <code>STDOUT</code> in the event text. The default is <code>y</code> .
Raise event if output is empty? (y/n)	Specify whether you want to raise an event if the results of the command do not produce any output. The default is <code>y</code> .
UNIX command with possible arguments	Enter the command to run. Do not enter a command that requires user input. The command you enter should include all necessary arguments and handle any input and output redirection or file management required.  Separate multiple processes with semicolons ( <code>;</code> ) and no spaces.



Description	How to Set It
Event severity level for STDOUT/STDERR event	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 22.

## 4.54 SmartCPUload

Use this Knowledge Script to monitor the CPU load of Linux or UNIX machines. This Knowledge Script uses either the CPU utilization or the queue length or both to determine whether the CPU is overloaded.

If you select the queue length to determine the CPU load, the Knowledge Script raises an event when both the queue length and the CPU utilization exceeds its threshold. The threshold for queue length is calculated as the maximum queue length \* number of CPU cores. For example, if you specify the queue length as 2 and you are using a 2 core machine, then the threshold for queue length becomes 4. In this case, if you specify the threshold for CPU utilization as 80% and select the *Use queue length in determining CPU overload?* parameter, then the Knowledge Script raises an event only when the queue length exceeds 4 and CPU utilization exceeds 80%.

This Knowledge Script is supported on all UNIX platforms.

### 4.54.1 Resource Objects

CPU folder

### 4.54.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.54.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a job fails. The default is 5.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event if AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event that is raised when AppManager fails to get the metrics. The default is 5.
Number of seconds between samples	Specify the number of seconds, 2 to 30, to wait between samples. The default is 5 seconds.

Description	How to Set It
Number of times sar should iterate before reporting an average value	Specify the number of sar iterations, 1 to 100, to report the average value. The default is 1 iterations.
Number of processes to add in detail	Specify the number of processes, 1 to 90, to add in the detail. The default is 5.
Cap processor usage values at 100 percent?	Select <b>Yes</b> to cap the processor usage values at 100 percent. If unselected the processor usage values might exceed 100%. The default is unselected.
<b>Event Settings</b>	
<b>Use queue length in determining CPU overload?</b>	Select <b>Yes</b> to use the queue length to determine CPU overload. The default is Yes.
Threshold -- Maximum queue length	Specify the threshold for the maximum queue length. The default is 2 multiplied by the processor capacity.
<b>Raise event if total CPU utilization exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the total CPU utilization exceeds the threshold. The default is Yes.
Threshold -- Maximum CPU utilization	Specify the threshold for the maximum CPU utilization percentage. The default is 80%.
Severity	Set the event severity level, from 1 to 40, from 1 to 40, to indicate the importance of an event reported when the maximum CPU utilization percentage is detected. The default is 5.
<b>Data Collection</b>	
Collect data for CPU utilization in percent?	Select <b>Yes</b> to collect data for charts and reports for the total CPU utilization percentage. The default is Yes.
Collect data for %User CPU state?	Select <b>Yes</b> to collect data for charts and reports for the total User CPU utilization percentage. The default is unselected.
Collect data for %System CPU state?	Select <b>Yes</b> to collect data for charts and reports for the total System CPU utilization percentage. The default is unselected.
Collect data for %Wait CPU State?	Select <b>Yes</b> to collect data for charts and reports for the total Wait CPU utilization percentage. The default is unselected.
Collect data for RunQueue length	Select <b>Yes</b> to collect data for charts and reports for the RunQueue length. The default is unselected.

## 4.55 SmartMemoryStats

Use this Knowledge Script to monitor the use of physical memory and swap usage of the system. When the usage crosses the threshold, the Knowledge Script raises an event indicating the memory usage with a detailed report of the memory utilization of the top memory intensive processes. The event also details paging scan rate information, KBytes swapped-in and swapped-out, and the page-out rate to determine if physical memory is a bottleneck. By providing all this information within a single event, this Knowledge Script eliminates the need to run multiple memory-related Knowledge

Scripts and correlate the events from all of them to figure out what is going wrong, thereby overcoming problems like unnecessary filling up of database space, event storm, and event correlation.

A UNIX system with ZFS almost always displays all memory as used. The ZFS makes use of all the memory until another process needs it. Therefore, the Knowledge Script excludes ZFS memory usage for physical memory calculation and displays the memory that the processes actually use.

## 4.55.1 Resource Objects

Memory folder

## 4.55.2 Default Schedules

The default interval for this scripts is **Every 5 minutes**.

## 4.55.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a job fails. The default is 5.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Number of top memory intensive processes to display (0 for all)	Set the number of top memory intensive processes to display. To display all top memory intensive processes is set to 0. The default is 5.
Number of seconds between samples	Set the number of seconds, 2-30, between samples. The default is 5.
Number of times "vmstat" command should iterate before reporting an average value.	Set the number of times, 1-100, that the "vmstat" command should iterate before reporting an average value. The default is 3.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an even when AppManager fails to get the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a job fails. The default is 5.
<b>HP-UX specific settings</b>	
Include reserved value in calculations?	Select <b>Yes</b> to include a reserved value in the HP_UX calculations. The default is Yes.
Include memory pseudo-swap values in calculations?	Select <b>Yes</b> to include the memory pseudo-swap values in the HP_UX settings. The default is unselected.
<b>Event Settings</b>	

Description	How to Set It
<b>Raise event if physical memory exceeds threshold?</b>	Select <b>Yes</b> to raise an event if physical memory crosses the threshold you specify for maximum percentage used. The default is selected.  <b>NOTE:</b> It is normal for UNIX systems to use almost all physical memory.
Threshold - Maximum physical memory used	Specify the maximum percentage (%) of physical memory that can be in use before an event is raised. The default is 90%.
<b>Use swap usage in determining memory bottleneck?</b>	Select <b>Yes</b> if you want to use swap usage in conjunction with physical memory usage before raising an event. The default is selected.  <b>NOTE:</b> If this option is selected, an event is raised only if physical and swap usage exceeds their respective specified thresholds.
Threshold	Specify the maximum percentage (%) of swap space that should be in use. The default is 90%.
Severity	Specify the severity level, from 1 to 40, to indicate the importance of the event when the maximum swap space usage crosses the threshold. The default is 5.
<b>Raise event if swap usage exceeds threshold</b>	Select <b>Yes</b> to raise an event if the paging file use crosses the threshold you specify for maximum percentage used. The default is unselected.
Threshold	Specify the maximum percentage (%) of swap space that should be in use. The default is 90%.
Severity	Specify the severity level, from 1 to 40, to indicate the importance of the event when the maximum swap space usage crosses the threshold. The default is 5.
<b>Collect data settings</b>	
Collect data for physical memory used?	Select <b>Yes</b> to collect charts and graphs for physical memory use. The default is unselected.
Collect data for percentage of computation memory in use (AIX only)?	Select <b>Yes</b> to collect charts and graphs for the percentage of computation memory in use for AIX systems. The default is unselected.
Collect data for total virtual memory used?	Select <b>Yes</b> to collect charts and graphs for the total virtual memory used. The default is unselected.
Collect data for swap space used?	Select <b>Yes</b> to collect charts and graphs for the total swap space used. The default is unselected.

## 4.56 SmartPhysicalDiskStats

Use this Knowledge Script to monitor physical disk activity and response time. This Knowledge Script combines a newly introduced parameter CPU 'Wait on IO' with disk load, to measure disk performance. CPU IOWait is the percentage of time the CPU has to wait on disk and if this is consistently high, it indicates that your storage device is too slow to keep up with incoming requests.

AIX only reports on disk load and ignores response time parameter.

### 4.56.1 Resource Objects

Physical disk folder or individual physical disks

## 4.56.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

## 4.56.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a job fails. The default is 5.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Number of seconds between samples	Set the number of seconds, from 1 to 30, between samples. The default is 2.
Number of times sar/iostat should iterate before reporting an average value	Set the number of times, from 1 to 100 that sar/iostat should iterate before reporting an average value. The default is 2.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event reported when a job fails. The default is 5.
<b>Event Settings</b>	
<b>Event if average response time of disk operations exceeds threshold? (y/n)</b>	Select <b>Yes</b> to raise an event if the average response time of the disk operations exceeds the threshold. The default is Yes.
Threshold - Maximum average response time (unavailable on AIX)	Specify the threshold for the maximum average response time that can be detected before an event is raised. The default is 200 ms (milliseconds).
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of the event when the maximum average response time exceeds the threshold you set. The default is 5.
<b>Raise event if disk activity exceeds threshold? (y/n)</b>	Select <b>Yes</b> to raise an event if the disk activity exceeds the threshold. The default is Yes.
<b>Use CPU 'Wait on IO' in determining disk load?</b>	Select <b>Yes</b> to use the CPU "Wait on IO" in determining the disk load. The default is Yes. If this parameter is selected, then even if the threshold for disk activity is reached, the event is not raised until an additional condition of CPU metrics <code>iowait% &gt; system% + user%</code> is met.
Threshold - Maximum disk activity (% busy)	Specify the threshold for the busy percentage (%) of the Maximum disk activity. The default is 80%.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the busy percentage of the maximum disk activity exceeds the threshold you set.

Description	How to Set It
<b>Collect data settings</b>	
Collect data for average response time of disk operations?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns the average response time of disk operations. The default is unselected.
Collect data for disk load?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns the disk load. The default is unselected.
Collect data for KBs read per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns KBs read per second. The default is unselected.
Collect data for KBs written per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns KBs written per second. The default is unselected.
Collect data for throughput in KBs per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns rate of disk read and write operations in KBs per second. The default is unselected.
Collect data for reads per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns reads per second of the disk operations. The default is unselected.
Collect data for writes per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns writes per second of the disk operations. The default is unselected.
Collect data for throughput per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, data collection returns throughput per second of the disk operations. The default is unselected.

## 4.57 SwapLow

Use this Knowledge Script to monitor the swap area (files and/or devices) available. You can monitor the overall percentage of space available across all swap areas, or monitor individual swap areas separately. If the percentage of available swap area is below the threshold you set, AppManager raises an event.

### 4.57.1 Resource Objects

Swap folder or individual swap area objects.

### 4.57.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 4.57.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if under the threshold? (y/n)	Set to <b>y</b> to raise events. The default is <b>y</b> .
Collect data? (y/n)	Set to <b>y</b> to collect data for charts and reports. The default is <b>n</b> .

Description	How to Set It
Minimum swap space available (%) threshold	Enter a threshold for the minimum percentage of swap space that should be available. The default is 3%.
Monitor overall swap space availability? (y/n)	Set to <code>y</code> to monitor all swap areas on a system. Set to <code>n</code> to monitor individual swap areas separately (multiple data streams might be created). The default is <code>n</code> .
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 20.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.58 Syslog

Use this Knowledge Script to monitor the `syslog` file asynchronously for specific messages or search strings. You can enter the search strings to look for using regular expressions and modifiers to define an Include filter and an Exclude filter or you can enter your search criteria in a separate filter file and use this Knowledge Script to specify the location of that file.

You can use the Include filter, the Exclude filter, or both. If you use both filters, messages that contain any included search strings and do not contain any of the excluded search strings are returned.

To specify the include and exclude patterns, you need to be familiar with Perl regular expressions. For more information, see [Section 4.1, “Creating Filters with Regular Expressions,” on page 46](#).

On all platforms, the UNIX agent must run as root or as a user with root-level authority to configure and retrieve information from the `syslog` file. Before running this Knowledge Script, configure the UNIX agent to run as root or as a user that has been given root-level authority using the `sudo` configuration file. SUSE10 no longer supports `syslogd` because it has introduced an upgraded `syslog` named `syslogd-ng`. However, if you need monitoring support for `syslogd`, you must install and configure the earlier, `bsd`-based `syslogd`.

This Knowledge Script creates a synchronized duplicate of the `syslog` file in `$AM_HOME/log/`, and uses the duplicate rather than the UNIX `syslog` file. If this is a security concern, either take measures to protect this file or do not run the script.

### 4.58.1 Resource Object

UNIX computer icon

### 4.58.2 Default Schedule

The default interval for this script is **Asynchronous**. After you start the Knowledge Script job, it runs continuously on the monitored system and reports events or data as they occur.

## 4.58.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Raise event if syslog matches filter?	Select <b>Yes</b> to raise events. The default is <i>y</i> .
Event message to display (clearing this setting will display the matched line)	<p>Type the event message you want to display when messages matching the search criteria are found. If you leave this field blank, the entry in the syslog file that matched your search criteria is displayed as the event message.</p> <p>If you specify a custom event message, you can still view the matching entry from the syslog file by displaying the Properties for the child event and clicking the <b>Message</b> tab.</p> <p>The default event message is <i>Syslog match found</i>.</p>
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. By default, the severity level is 8.
Add filter expression string to event message?	Select <b>Yes</b> for AppManager to add the filter to the details of the event message. The default is <i>Yes</i> .
Remove timestamp string from event message?	Select <b>Yes</b> to remove the timestamp from the event message. The default is unselected, which means that the syslog timestamp is included in the event message.
Remove process id string from event message?	Select <b>Yes</b> if you do not want to include the syslog process identifier in the event message. The default is <i>no</i> , which means that the syslog process ID is included in the event message.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Filter Settings</b>	
<b>Include Filter</b>	
Base regular expression	<p>Enter a regular expression, in Perl, to identify the pattern you want to look for in the monitored text file. The default expression matches all strings.</p> <p>For information about writing Perl regular expressions, see <a href="#">Section 4.1, "Creating Filters with Regular Expressions,"</a> on page 46.</p> <p>Control Center also allows you to override values for parameters. You might want to use that feature instead of, or in conjunction with, this parameter. For more information about setting overrides, see the <i>Control Center User Guide</i>.</p>



Description	How to Set It
Special regular expression	<p>Enter an additional regular expression to look for in specific situations. For example, you can have a base regular expression that you use in jobs that run on all computers, then an additional regular expression that you only use in jobs running on some computers.</p> <p>Control Center also allows you to override values for parameters. You might want to use that feature instead of, or in conjunction with, this parameter. For more information about setting overrides, see the <i>Control Center User Guide</i>.</p>
Modifier for regular expression	You can use optional modifiers to change the behavior of the regular expression. For example, specifying <code>i</code> makes the include filter case-insensitive.
<b>Exclude Filter</b>	
Base regular expression	Enter a regular expression, in Perl, to identify the pattern you want to exclude in the monitored text file. The default is <code>.*</code> .
Special regular expression	Enter an additional regular expression to exclude in specific situations. For example, you can have a base regular expression that you use in jobs that run on all computers, then an additional regular expression that you only use in jobs running on some computers. For information about how to selectively run jobs, see the <i>Control Center User Guide for NetIQ AppManager</i> .
Modifier for regular expression	<p>You can use optional modifiers to change the behavior of the regular expression. For example, specifying <code>i</code> makes the include filter case-insensitive.</p> <p>To use the case-insensitive modifier, enter <code>i</code>.</p>
Optional file containing additional filters	Enter the full path to a file containing any additional filter items you want to match. You can also use this parameter if you only want to specify matching expressions in an external file.
Collect data?	Select <b>Yes</b> to collect data for reports and graphs. If set to <code>y</code> , the script returns the number of messages matching the search criteria. The default is <code>n</code> .
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is <code>n</code> .

## 4.58.4 Example of How this Script Is Used

This Knowledge Script allows you to specify include and exclude expressions as Knowledge Script properties or maintain your search criteria independent of the Knowledge Script parameters in a separate filter file.

In many cases, specifying a filter file provides greater flexibility and makes modifying your search criteria more straightforward because you can add virtually any number of expressions and you do not need to modify the Knowledge Script properties through the Operator Console to pick up your changes.

If you want to use a filter file:

- ◆ Identify the strings that you want to find a match for in the syslog file (the entries you want to include in your results).

- ♦ Create the file with one regular expression string per line to locate matching strings.
- ♦ Make sure the file exists on the target UNIX computer.
- ♦ Enter the absolute path to the file on the local UNIX agent in the **Optional file containing additional filters** parameter and start the job.

## 4.59 SystemUpTime

Use this Knowledge Script to monitor the system up time for a UNIX server. This Knowledge Script tracks the number of hours that the computer has been operational since it was last rebooted. If the computer reboots within the monitoring interval, AppManager raises an event.

Given a threshold of max hours, this Knowledge Script will trigger an event if the uptime of the system exceeds the given threshold in hours. This event will occur once per Knowledge Script restart. If the Knowledge Script is run in intervals, and in an interval this event is triggered once, it will not be triggered in the subsequent iterations.

This Knowledge Script now collects data points for the previous minute, 5 minute and 15 minute load averages, as well as triggering events when the corresponding load averages exceeds the given threshold.

This script allows you to specify whether you want AppManager to raise events for reboots when the computer is in maintenance mode.

### 4.59.1 Resource Object

UNIX computer icon

### 4.59.2 Default Schedule

The default interval for this script is **Every hour**.

### 4.59.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if system rebooted? (y/n)	Set to <i>y</i> to raise events. The default is <i>y</i> .
Threshold for system uptime event in hours (-1 to disable)	Enter a threshold for the system uptime event in hours. To disable this parameter, enter -1.
Threshold for system load average for the last 1 min (-1 to disable)	Enter a threshold for the system load average for the last 1 minute. To disable this parameter, enter -1.
Threshold for system load average for the last 5 min (-1 to disable)	Enter a threshold for the system load average for the last 5 minutes. To disable this parameter, enter -1.
Threshold for system load average for the last 15 min (-1 to disable)	Enter a threshold for the system load average for the last 15 minutes. To disable this parameter, enter -1.

Description	How to Set It
Collect uptime hours data? (y/n)	Set to <code>y</code> to collect data for graphs and reports. If set to <code>y</code> , the script returns the number of hours the system has been up. The default is <code>n</code> .
Collect data for last 1 min load average? (y/n)	Set to <code>y</code> to collect data for graphs and reports. If set to <code>y</code> , the script returns the number of hours the system has been up. The default is <code>n</code> .
Collect data for last 5 mins load average? (y/n)	Set to <code>y</code> to collect data for graphs and reports. If set to <code>y</code> , the script returns the number of hours the system has been up. The default is <code>n</code> .
Collect data for last 15 mins load average? (y/n)	Set to <code>y</code> to collect data for graphs and reports. If set to <code>y</code> , the script returns the number of hours the system has been up. The default is <code>n</code> .
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 8.
Ignore reboots during maintenance mode? (y/n)	Set to <code>y</code> to prevent AppManager from reporting events when the computer reboots while in maintenance mode. The default is <code>n</code> .
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.60 TopCpuProcs

Use this Knowledge Script to monitor the total CPU resources used by all processes and which processes consume the most CPU resources. If the CPU usage for any of the listed processes exceeds the threshold you set, AppManager raises an event.

### 4.60.1 Resource Objects

CPU folder

### 4.60.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.60.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the total CPU usage for the interval and the detail message lists the processes consuming the most CPU resources. The default is <code>n</code> .
Maximum CPU usage (%) for all processes threshold	Enter a threshold for the maximum percentage of CPU resources that should be in use for all processes. The default is 90%.

Description	How to Set It
Number of top processes to display (0 means all)	Specify the number of top processes to display in the detail message (event or data). Enter 0 for all processes to display. The default is 5 processes.  <b>NOTE:</b> Limit the number of processes included in the detail message to the top five to ten processes, rather than reporting on all processes. In most cases, including all processes increases the size of the detail message without providing you with more useful information. Typically, the top few processes are the most significant and the most likely ones you are looking to track down for troubleshooting purposes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

## 4.61 TopMemoryProcs

Use this Knowledge Script to monitor the system memory usage to identify which processes are consuming the most memory. This Knowledge Script raises an event if the virtual or physical memory usage for the system crosses the threshold you specify. The top number of processes that are consuming the most physical memory are reported in the event and data detail messages.

### 4.61.1 Resource Object

Memory folder

### 4.61.2 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 4.61.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General settings</b>	
Number of top processes to display (0 means all)	Enter a number indicating how many top processes you want AppManager to display in the detail message (event or data). Type 0 if you want all processes recorded in the detail message. The default is 5.  <b>NOTE:</b> In most cases, including all processes increases the size of the detail message without providing you with more useful information. Therefore, NetIQ recommends that you limit the number of processes included in the detail message to the top five or ten processes. Typically, the top few processes are the most significant for troubleshooting purposes.  Processes that share memory appear to be using more memory than they actually are.

Description	How to Set It
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event?	Select <b>Yes</b> to raise an event if the memory usage for all processes crosses the threshold you specify. The default is Yes.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
<b>Threshold settings</b>	
Maximum virtual memory used (%) threshold	Type a threshold for the maximum percentage (%) of virtual memory that should be in use. The default is 90%.
Maximum physical memory used (%) threshold	Type a threshold for the maximum percentage (%) of physical memory that should be in use for all processes. Physical memory not being used by processes is often used dynamically by the system as cache. The default is 100%.
<b>HP-UX specific settings</b>	
Include reserved value in calculations?	Select <b>Yes</b> to include reserved swap space in the calculations. If set to Yes, calculations include space reserved system for deactivation and paging processes. This parameter is only available on computers running the HP-UX operating system. The default is Yes.
Include memory pseudo-swap values in calculations?	Select <b>Yes</b> to include pseudo-swap space in the calculations. Pseudo-swap space might be up to 3/4 of the available system memory. If set to Yes, calculations include space in the pseudo swap reservation counters. This parameter is only available on computers running the HP-UX operating system. The default is unselected.
<b>Collect Data settings</b>	
Collect virtual memory data?	Select <b>Yes</b> to collect information on virtual memory usage for charts and reports. If set to y, this script returns the virtual memory usage for the interval and the detail message lists the processes consuming the most memory resources. The default is unselected.
Collect physical memory data?	Select <b>Yes</b> to collect information on physical memory usage for charts and reports. If set to Yes, this script returns the physical memory usage for the interval and the detail message lists the processes consuming the most memory resources. The default is unselected.
Enable debugging? (y/n)	Select <b>Yes</b> to enable debugging. The default is unselected.

## 4.62 UserSessions

Use this Knowledge Script to monitor the number of user accounts logged into a computer. This Knowledge Script raises an event if the number of user sessions crosses the threshold you specify. The top number of user sessions are reported in the event and data detail messages.

### 4.62.1 Resource Object

UNIX computer icon

## 4.62.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

## 4.62.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Collect data on user sessions? (y/n)	Select <b>Yes</b> to collect information for virtual memory usage for charts and reports. If set to Yes, this script returns the number of current user accounts that are logged into the computer. The default is unselected.
<b>Session Event Options</b>	
<b>Raise event if session thresholds exceeds? (y/n)</b>	Select <b>Yes</b> to raise an event if the number of active sessions crosses the threshold you specify. The default is Yes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user sessions exceeds the threshold. The default is 5.
Minimum number of users logged in	Type a threshold for the minimum number of active user sessions. The default is 0.
Maximum number of users logged in	Type a threshold for the maximum number of active user sessions. The default is 8.
<b>User Session Options</b>	
<b>Raise event for restricted Users? (y/n)</b>	Select <b>Yes</b> to raise an event if restricted user accounts log in. The default is Yes.
Event severity level	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of user sessions exceeds the threshold. The default is 40.
Restricted User list (separated by commas and no spaces)	Specify the user accounts that should not log into the computer, separated by commas with no space.
Enable debugging? (y/n)	Set to <b>Yes</b> to enable debugging. The default is unselected.

## 4.63 WAMAgentConfiguration

Use this Knowledge Script to configure WAM client to connect to the WAM server.

### 4.63.1 Resource Object

UNIX computer icon.

### 4.63.2 Default Schedule

By default, this script is only run once for each computer.

## 4.63.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
<b>General Setting</b>	
<b>Do you want to configure the parameter?</b>	Set to <b>Yes</b> to configure the parameter. The default is No.
WAM Server address Hostname/IP	Set the WAM server Hostname or IP address.
WAM Server port	Set the port number of the WAM server.
WAM server application name	Set the name of the application, which the WAM server is running.
Heart Beat interval	Set a Heart Beat interval, at which the script must run. The default value is 30 seconds.
<b>CA Certificates Configuration</b>	
Truststore file location	Set the location of truststore file.
Password for truststore	Set the password for truststore.
<b>Private key Configuration</b>	
KeyStore file location	Set location of Keystore file.
Password for KeyStore	Set password for KeyStore.
Event severity when job fails	Set the event severity level to indicate the importance of the event when job fails.
Enable debugging?	Set to <b>Yes</b> to enable debugging. The default value is No.
<b>Raise event if AppManager fails to get metrics?</b>	Set to <b>Yes</b> to raise an event if AppManager fails to get a metric. The default is Yes.
Event severity	Set the event severity level to indicate the importance of the event.
<b>Event Settings</b>	
<b>Raise event when succeeds?</b>	Set to <b>Yes</b> to raise an event when event setting becomes successful. The default value is No.
Event severity when succeeds	Set the event severity level to indicate the importance of the event.

## 4.64 ZFSDataset

Use this Knowledge Script to monitor individual usage and total usage (including child and snapshot usage) of a dataset.

This Knowledge Script is supported on: [Solaris].

## 4.64.1 Resource Object

Dataset folder icon

## 4.64.2 Default Schedule

The default interval for this script is **Every 5 minutes**

## 4.64.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Pools to be excluded (comma-separated)	Specify the pools to exclude from monitoring. The default is unspecified.
Regular expression specifying datasets include filter	Specify the regular expression to include datasets for monitoring. The default is unspecified.
Regular expression specifying datasets exclude filter	Specify the regular expression to exclude datasets from monitoring. The default is unspecified.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails. The default is 5.
Ignore if the dataset is read-only	Select <b>Yes</b> to ignore if the dataset is read-only. The default is Yes.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event when AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to retrieve the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the individual dataset usage exceeds the threshold. The default is 5.
<b>Event Settings</b>	
<b>Raise an event if total dataset usage including child and snapshot usage exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the dataset usage including child and snapshot exceeds the threshold you specified.
Threshold--usage of dataset	Set the threshold percentage for the dataset usage. The default is 80 percent.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event in which the dataset usage, including child and snapshot usage, exceeds the threshold. The default is 10.
<b>Raise an event if individual dataset usage exceeds threshold?</b>	Select <b>Yes</b> to raise an event if an individual dataset usage exceeds the threshold you specified.



Description	How to Set It
Threshold--usage of dataset	Set the threshold percentage for the dataset usage. The default is 80 percent.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the individual dataset usage exceeds the threshold. The default is 10.
<b>Data Collection</b>	
Collect data for total dataset usage?	Select <b>Yes</b> to collect data for total usage of a dataset. The default is unselected.
Collect data for individual dataset usage?	Select <b>Yes</b> to collect data for individual usage of a dataset. The default is unselected.

## 4.65 ZFSPoolHealth

Use the Knowledge Script to monitor ZFS Pool Health. This Knowledge Script raises an event when pool status is not online or when scrub reports an error.

This Knowledge Script is supported on: [Solaris].

### 4.65.1 Resource Object

StoragePoolZFS icon

### 4.65.2 Default Schedule

The default interval for this script is **Every 15 minutes**

### 4.65.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Pool(s) to exclude (comma-separated)	Specify the pools to exclude from monitoring. The default is unspecified.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails The default is 5.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event if AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to get the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails The default is 5.

Description	How to Set It
Consolidate for all pools?	Select <b>Yes</b> to consolidate all pools. The default is unselected.
<b>Event Settings</b>	
<b>Raise event if pool is unhealthy?</b>	Select <b>Yes</b> to raise an event if a pool is unhealthy. If the Consolidate for all pools? parameter is selected, AppManager raises an event for the consolidated pools. A pool is considered as unhealthy if its status is not "ONLINE" or if it has error(s) reported by scrub. Scrub errors are considered for eventing if the scrub last runtime gets changed and the scrub error is greater than zero. The default is Yes.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the pool is unhealthy. The default is 5.
<b>Data Collection</b>	
Collect data for pool status?	Select <b>Yes</b> to collect chart and graph data for the pool status. The default is Yes.
Collect data for scrub errors?	Select <b>Yes</b> to collect chart and graph data for the scrub errors. The default is unselected.

## 4.66 ZFSPoolSnapshot

Use the Knowledge Script to monitor the total usage of snapshots in the pool. This Knowledge Script raises an event if the total usage of snapshots in a pool crosses the threshold you specify.

The topmost snapshots, based on the usage, are reported in the event message.

This Knowledge Script is supported on: [Solaris]

### 4.66.1 Resource Object

Snapshot icon

### 4.66.2 Default Schedule

The default interval for this script is **Every hour**.

### 4.66.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Pools to be exclude (comma-separated)	Specify the pools to exclude from monitoring. The default is unspecified.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails. The default is 5.

<b>Description</b>	<b>How to Set It</b>
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event if AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to get the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails. The default is 5.
<b>Event Settings</b>	
<b>Raise event if the snapshot usage of the pool exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the snapshots usage of the pool crosses the specified threshold. The default is Yes.
Number of top space consuming snapshots to display	Specify the number of top space consuming snapshots to display. The default is 10.
Threshold -- snapshot usage of pool	Set the threshold percentage for the snapshot usage of the pool. The default is 65%.
Severity	Set the event severity level, from 1 to 40, to reflect the importance of the event that is raised when the threshold for the snapshot usage of pool is exceeded.
<b>Raise event if the number of snapshots cross the threshold?</b>	Select <b>Yes</b> to raise an event if the number of snapshots cross the specified threshold. The default is Yes.
Consolidate snapshot count event for all pools?	Select <b>Yes</b> to consolidate the snapshot count event for all pools. The default is unselected.
Threshold -- snapshot count in pool	Set the threshold for the snapshot count of in the pool. The default is 100.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the snapshot count exceeds the specified number. The default is 10.
<b>Raise event if the snapshots are older than the number of days specified?</b>	Select <b>Yes</b> to raise an event if the snapshots are older than the number of days specified. The default is Yes.
Number of days	Specify the number of days, from 0 to 365, to list snapshots that are older than specified. The default is 90 days.
Severity	Set the event severity level, from 0 to 40, to indicate the importance of an event if the snapshots are older than the specified number of days. The default is 10.
<b>Data Collection</b>	
Collect data for space consumed by snapshots of a pool?	Select <b>Yes</b> to collect to collect data for charts and reports. If enabled, this script returns the space consumed by snapshots of a pool. The default is unselected.
Collect data for number of snapshots created in a pool?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the number of snapshots created in the pool. The default is unselected.

## 4.67 ZFSPoolStats

Use the Knowledge Script to monitor ZFS pool space utilization and IO statistics. This Knowledge Script raises an event if any threshold is exceeded.

This Knowledge Script is supported on: [Solaris].

### 4.67.1 Resource Object

StoragePoolZFS icon

### 4.67.2 Default Schedule

The default interval for this script is **Every 15 minutes**

### 4.67.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>General Settings</b>	
Pool(s) to exclude (comma-separated)	Specify the pools to exclude from monitoring. The default is unspecified.
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails The default is 5.
Event detail format	Select the format in which to view the event detail. The default is HTML Table.
Enable debugging?	Select <b>Yes</b> to enable debugging. The default is unselected.
<b>Raise event if AppManager fails to get metrics?</b>	Select <b>Yes</b> to raise an event if AppManager fails to get the metrics. The default is Yes.
Event severity	Set the event severity level, from 1 to 40, to indicate the importance of an event when the job fails The default is 5.
Consolidate events for all pools?	Select <b>Yes</b> to consolidate events for all pools. The default is unselected.
<b>Event Settings</b>	
<b>Raise event if pool space utilization exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the pool space utilization exceeds the specified threshold. The default is Yes.
Threshold -- Maximum pool space utilization	Set a threshold for the maximum pool space utilization. The default is 80 percent.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event if the pool space utilization exceeds the threshold. The default is 5.
Number of top dataset uses to display (0 for all)	Specify the number of top dataset uses to display. The default is 5.

Description	How to Set It
<b>Raise event if reads per second exceeds threshold?</b>	Select <b>Yes</b> to raise an event when the reads per second exceed the specified threshold. The default is Yes.
Threshold -- Maximum reads per second	Set the threshold for maximum reads per second. The default is 300 reads per second.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event if the pool reads per second exceed the threshold. The default is 5.
<b>Raise event if writes per second exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the number of writes per second exceed the specified threshold. The default is Yes.
Threshold--Maximum writes per second	Set the threshold for maximum writes per second. The default is 300.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of the event if the pool writes per second exceed the threshold. The default is 5.
<b>Raise event if throughput per second exceeds threshold?</b>	Select <b>Yes</b> to raise an event if the throughput per second exceeds the specified threshold.
Threshold--Maximum throughput per second	Set the threshold for the maximum throughput per second. The default is 500.
Severity	Set the event severity level, from 1 to 40, to indicate the importance of an event if the pool throughput per second exceeds the threshold. The default is 5.
<b>Data Collection</b>	
Collect data for pool space utilization?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the pool space utilization data. The default is unselected.
Collect data for reads per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the reads per second. The default is unselected.
Collect data for writes per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the writes per second. The default is unselected.
Collect data for throughput per second?	Select <b>Yes</b> to collect data for charts and reports. If enabled, this script returns the throughput per second. The default is unselected.

## 4.68 ZombieProcs

Use this Knowledge Script to detect the number of zombie, or defunct, processes currently left waiting to be cleaned up. If the number of zombie processes exceeds the threshold you set, AppManager raises an event. A large or increasing number of zombie processes can indicate a program you are running is launching child processes but not properly terminating either the parent or child process, or that you might need to exit a running program to eliminate the zombie processes.

### 4.68.1 Resource Object

CPU folder

### 4.68.2 Default Schedule

The default interval for this script is **Every 15 minutes**.

### 4.68.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Event if over the threshold? (y/n)	Set to <code>y</code> to raise events. The default is <code>y</code> .
Collect data? (y/n)	Set to <code>y</code> to collect data for charts and reports. If set to <code>y</code> , the script returns the number of zombie processes detected for the interval. The default is <code>n</code> .
Maximum number of zombie processes threshold	Enter a threshold for the maximum number of zombie processes waiting in the interval. The default is 10.
Event severity level	Set the event notification level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event in which this job experienced an internal error. The default is 5.
Enable debugging? (y/n)	Set to <code>y</code> to enable debugging. The default is <code>n</code> .

# 5

## HardwareUNIX Knowledge Scripts

AppManager for UNIX provides the following Knowledge Scripts for monitoring AIX and Solaris hardware logs, and Dell and HP hardware running a Linux operating system.

To run these Knowledge Scripts as a non-root user:

- 1 Log in using the `root` account.
- 2 Run the command `chmod +w /etc/uroot.cfg`.
- 3 Add the following commands at the end of the `uroot` configuration file:
  - ♦ `/usr/sbin/hpacucli`
  - ♦ `/sbin/hpasmcli`
  - ♦ `/usr/sbin/dmidecode`
- 4 Save the `uroot` configuration file.
- 5 Run the command `chmod -w /etc/uroot.cfg`.

From the Knowledge Script view of console, you can access more information about any NetIQ-supported Knowledge Script by selecting it and clicking **Help** or **F1**.

Knowledge Script	What It Does
<a href="#">AIXHWLog</a>	Monitors the hardware error log on AIX computers.
<a href="#">Fan</a>	Monitors the fan status on HP and Dell computers.
<a href="#">LogicalDrive</a>	Monitors the operational status of logical drives on HP and Dell computers.
<a href="#">PhysicalDrive</a>	Monitors the operational status of physical drives on HP and Dell computers.
<a href="#">PhysicalMemory</a>	Monitors the operational status of physical memory on HP and Dell computers.
<a href="#">PowerConsumption</a>	Monitors the power consumption on Dell computers.
<a href="#">PowerSupply</a>	Monitors the operational status of power supplies on HP and Dell computers.
<a href="#">SmartArrayController</a>	Monitors the operational status of storage controllers, such as HP Smart Array RAID controllers on computers running Linux.
<a href="#">SolarisHWLog</a>	Monitors hardware logs on Solaris computers.
<a href="#">Temperature</a>	Monitors the hardware temperature on HP and Dell computers.
<a href="#">Voltage</a>	Monitors the voltage probe on Dell computers.

### 5.1 HardwareUNIX Object Properties

The `Discovery_HardwareUNIX` Knowledge Script creates and populates properties for each discovered hardware object. The following topics summarize those object properties.

## 5.1.1 Fan Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each fan object.

Property	Description	Platform
Name	Fan name. To make it unique, the device identifier is appended. For example, BMC_FAN_1A_RPM#0.	Dell, HP
DeviceID	Fan internal device identifier.	Dell, HP
Redundant	If yes, this is a redundant fan rather than a primary fan.	HP
HotPluggable	If yes, this fan is hot-pluggable.	HP
MinWarningThreshold	Fan speed in RPM representing the minimum warning threshold. The value is in RPM, for example, 2175 RPM, or N/A if the hardware does not define a minimum warning threshold.	Dell
MaxWarningThreshold	Fan speed in RPM representing the maximum warning threshold. The value is in RPM, for example, 2200 RPM, or N/A if the hardware does not define a maximum warning threshold.	Dell
MinFailureThreshold	Fan speed in RPM representing the minimum failure threshold. The value is in RPM, for example, 2201 RPM, or N/A if the hardware does not define a minimum failure threshold.	Dell
MaxFailureThreshold	Fan speed in RPM representing the maximum failure threshold. The value is in RPM, for example 2500 RPM, or N/A if the hardware does not define a maximum failure threshold.	Dell

## 5.1.2 LogicalDrive Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each logical drive defined for a storage controller object.

Property	Description
Name	Logical device name.
DeviceID	Logical device internal identifier.
ParentDeviceID	Logical device parent internal identifier.
Size	Logical device storage capacity. For example, 1765 GB.



### 5.1.3 PhysicalDrive Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each physical drive object attached to a storage controller object.

Property	Description
Name	Physical drive name.
Model	Physical drive manufacturer's model name. For example, MAXTOR ATLAS10K5_146SCA.
DeviceID	Physical drive internal device identifier.
Size	Physical drive storage capacity. For example, 136.77GB.
FirmwareRevision	Physical drive firmware revision number. For example, JNZM.
Slot	Physical drive installed slot number.

### 5.1.4 PhysicalMemory Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each physical memory object.

Property	Description	Platform
Name	Physical memory name with an appended index to make it unique. For example, DIMM_A.	Dell, HP
Index	Physical memory index. For Dell computers, this is memory array/index, for example 1/1. For HP computers, this is cartridge/module, for example 0/1.	Dell, HP
Type	Physical memory type. For example, Reserved, Cached, or Fast-paged.	Dell, HP
Size	Physical memory size.	Dell, HP
FormFactor	Physical memory form factor. For example, 9H.	HP
Speed	Physical memory clock cycle frequency. For example, 100 MHz.	HP

### 5.1.5 PowerConsumption Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each power consumption object.

Property	Description
Name	Power consumption device name. This is the system board level.
DeviceID	Power consumption computer or device identifier.

Property	Description
WarningThreshold	Power consumption warning threshold in watts. For example, 917 W
FailureThreshold	Power consumption failure threshold in watts. For example, 977 W.

## 5.1.6 PowerSupply Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each power supply object.

Property	Description
Name	Power supply unit name.
DeviceID	Power supply internal device identifier.

## 5.1.7 SmartArrayController Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each storage controller object.

Property	Description
Name	Storage controller name.
DeviceID	Storage controller internal device identifier.

## 5.1.8 Temperature Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each temperature sensor object.

Property	Description
Name	Temperature sensor name.
SensorID	Temperature sensor internal device identifier.
Threshold(C)	Temperature sensor maximum acceptable temperature value in degrees Celsius.

## 5.1.9 Voltage Properties

The Discovery\_HardwareUNIX Knowledge Script creates and populates the following properties for each voltage probe object.

Property	Description
Name	Voltage probe name appended with the index to make it unique. For example, PROC_1 VCORE#1.

Property	Description
Index	Voltage probe index.
Min Warn Threshold	Voltage probe minimum warning threshold. For example, 2.644 V or N/A if the hardware does not define the minimum warning threshold.
Max Warn Threshold	Voltage probe maximum warning threshold. For example, 2.866 V or N/A if the hardware does not define the maximum warning threshold.
Min Fail Threshold	Voltage probe minimum failure threshold. For example, 2.867 V or N/A if the hardware does not define the minimum failure threshold.
Max Fail Threshold	Voltage probe maximum failure threshold. For example, 2.955 V or N/A if the hardware does not define the maximum failure threshold.

## 5.2 AIXHWLog

Use this Knowledge Script to monitor the hardware error log on computers running the AIX operating system. This script uses the AIX `errpt` command to gather hardware records, parses those records, and raises an event when a record matches the filter and regular expression criteria you specify.

This script is intended to monitor AIX hardware error logs and uses the `errpt -d H` option internally to return only hardware records.

---

**NOTE:** This Knowledge Script is available as soon as you install it. It does not require that you run the Discovery\_HardwareUNIX Knowledge Script to discover resources.

---

### 5.2.1 Filtering

This Knowledge Script provides the following filters through the AIX `errpt` command:

- ◆ An error label filter to return records whose label matches a specified error label
- ◆ A start time filter to return records whose timestamp is on or after the start time
- ◆ An end time filter to return records whose timestamp is on or before the end time

In addition to filters provided through `errpt`, this script provides additional filters on the records `errpt` returns:

- ◆ An *include* filter to return records that match a specified regular expression
- ◆ An *exclude* filter to return records that do not match any specified regular expression

This script filters records returned by `errpt` using the include filter first, discarding those records that do not match the filter. This script filters the remaining records using the exclude filter, discarding those records matched by the filter.

By default, the include filter is set to the regular expression `.+` to include all records returned from `errpt`. An empty include filter discards all records.

By default, the exclude filter is empty. An empty exclude filter does not exclude any records.

As with all include and exclude filter pairs, it is important to recognize and avoid include and exclude combinations that discard all records and prevent this script from raising events for important AIX hardware status changes. In many instances it is sufficient to set one filter or the other, include or exclude, to reduce the number of incoming records to those necessary for your AIX hardware monitoring requirements.

## 5.2.2 Resource Objects

Any computer running AIX

## 5.2.3 Default Schedule

The default interval for this script is **Every 30 minutes**.

## 5.2.4 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Text match filters</b>	
Regular expression specifying the include filter (comma-separated)	Type a list of regular expressions, comma-separated, to match and include when parsing hardware records. The default is <code>.+</code> to include all hardware records received from <code>errpt</code> .  <b>WARNING:</b> Do not clear this parameter. An empty include filter discards all hardware records.  <b>NOTE:</b> All regular expressions are Perl regular expressions. Regular expression matching is case-insensitive.
Regular expression specifying the exclude filter (comma-separated)	Type a list of regular expressions, comma-separated, to match and exclude when parsing hardware records. The default is none, so no records are excluded.  <b>NOTE:</b> All regular expressions are Perl regular expressions. Regular expression matching is case-insensitive.
<b>Label match strings</b>	

Description	How to Set It
Comma separated error labels	<p>Type a list of error labels, comma-separated, to match when parsing hardware records. The default is  <code>PHXENT_DOWN,LVM_IO_FAIL,CPU_FAIL_PREDICTED,DISK_ERR2,IDE_DISK_ERR3,LVM_SA_PVMISS</code></p> <p>This field accepts comma-separated regular expressions. This script expands the expressions to match the list of system labels. This script gets the list of system labels from the command:</p> <pre>errpt -t -d H</pre> <p>For example, if you type <code>disk</code> in this field, this Knowledge Script matches all system labels containing <code>disk</code> as a substring.</p> <p>If none of the label strings in this field matches any system label, this field is treated as empty and the entire <code>errpt</code> output is considered. For example, if you type <code>my_label</code> in this field and no system label matches it, all system labels are valid and nothing is filtered.</p> <p><b>NOTE:</b> Events raised by this script list the expanded labels used to filter the <code>errpt</code> output in the event detailed message.</p>
Treat as exclusion label	<p>Select <b>Yes</b> to treat the comma-separated list of error labels as an exclusion list rather than an inclusion list when parsing hardware records. The default is no.</p>
<b>Time settings</b>	
Start Time (ddmmyyhhmm)	<p>Type the time and date as day, month, year, hour, minute, using the format <code>ddmmyyhhmm</code>, to identify the first timestamp to include when parsing hardware records. There is no default, so <code>errpt</code> parses records posted since:</p> <ul style="list-style-type: none"> <li>◆ this script's start time, if this is the first run</li> <li>◆ this script's last run time, if this is the second or a subsequent run</li> </ul> <p>If Start Time precedes the first timestamp in the log, <code>errpt</code> parses the entire log. If the last timestamp in the log precedes Start Time, <code>errpt</code> only parses hardware records added on or after Start Time.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>◆ This script will not save the current time while it precedes Start Time. The script will run normally, but will not store internal states and will not raise events until Start Time arrives.</li> <li>◆ This parameter uses time format <code>ddmmyyhhmm</code>. The AIX <code>errpt</code> command uses format <code>mmddhhmmyy</code>.</li> </ul>

Description	How to Set It
End Time (ddmmyyhhmm)	<p>Type the time and date as day, month, year, hour, minute, using the format ddmmyyhhmm, to identify the last timestamp to include when parsing hardware records. There is no default, indicating <code>errpt</code> should parse to the end of the log.</p> <p>If End Time precedes the first timestamp in the log, <code>errpt</code> will not parse any entries from the log. If End Time precedes the last timestamp in the log, <code>errpt</code> will only parse hardware records added on or before End Time.</p> <p>When the current time passes End Time, this script raises an information event. This script continues to execute but will not raise any additional events while End Time lies in the past.</p> <p><b>NOTE:</b> This field uses time format ddmmyyhhmm. The AIX <code>errpt</code> command uses format mmddhhmmyy.</p>
Override scan from beginning of the log?	<p>Select to <b>Yes</b> to override the start and/or end times and parse the hardware error log from the beginning of the file. The default is no.</p>
Optional errpt log file location	<p>Type the path that represents an alternate location for the hardware error log. There is no default.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>◆ The log file you specify will be used by <code>errpt</code> and should be in a format <code>errpt</code> can read and should not be a plain text file.</li> <li>◆ When no optional hardware error file is specified, <code>errpt</code> uses the file named in the AIX error log configuration database.</li> </ul>
<b>Event Settings</b>	
Raise event if hardware error occurred?	<p>Select to <b>Yes</b> to raise an event if a hardware error occurred. The default is Yes.</p>
Event severity	<p>Specify the event severity level, from 1 to 40, to indicate the importance of a hardware error event. The default is 5.</p>
Raise event if AppManager fails to get metrics?	<p>Select to <b>Yes</b> to raise an event if AppManager cannot collect any information about the hardware error log. The default is yes.</p>
Event severity	<p>Specify the event severity, from 1 to 40, to indicate the importance of an event when AppManager cannot collect any information about the hardware error log. The default is 5.</p>
Event severity when job fails	<p>Specify the event severity, from 1 to 40, to indicate the importance of an event when this job fails. The default is 5.</p>
Informative event severity	<p>Specify the event severity, from 1 to 40, to indicate the importance of an informative event. The default is 25.</p>

Description	How to Set It
Aggregate event per iteration?	<p>Select to <b>Yes</b> to aggregate multiple events during an iteration into one event per matched regular expression. The default is unselected.</p> <p>When you choose to aggregate events, this Knowledge Script subsequently raises events with the following short message:</p> <pre data-bbox="639 380 1029 401">Errors in errpt log recorded.</pre> <p>If this script creates two of these events in an interval, it collapses them by default, replacing the content of the first event with the content of the second one. To prevent this replacement, NetIQ recommends you uncheck <b>Collapse duplicate events into a single event</b> on the <b>Advanced</b> tab when you aggregate events.</p>
Enable debuggin?	<p>Select <b>Yes</b> to enable debugging or this Knowledge Script. The default is unselected.</p>

## 5.2.5 Understanding Start Time and End Time

The Start Time and End Time control the range of timestamps this Knowledge Script receives from the AIX `errpt` command. With parameter `Override scan` from beginning of the log, Start Time and End Time determine a number of parsing actions this Knowledge Script can take.

### Start and End Time in the AIX `errpt` Command

`errpt` accepts the following start and stop options:

**-s *StartDate***

Return all records posted on and after *StartDate*.

**-e *EndDate***

Return all records posted prior to and including *EndDate*.

### Knowledge Script Restarts and Data Failures

When this Knowledge Script restarts, either explicitly as part of an agent restart or because a parameter changes during execution, this script discards old time states and re-reads all script parameters.

If this Knowledge Script fails to get data during a run, it will retain and use the same base time for the next run.

## Start Time, End Time, and Scan from Top of Log

The following table describes the permutations of Start Time, End Time, and Override scan from beginning of log. The character “n” indicates the parameter value is not set, while “y” indicates a time value is set or the override is set to Yes.

**NOTE:** Where the term “Epoch time” is used, it is equivalent to 00:00:00 UTC on Thursday, January 1, 1970.

Start Time	Stop Time	Beginning of Log	Knowledge Script Action
n	n	n	During its first run, this Knowledge Script uses the current time. In subsequent runs, it raises events for hardware records posted since the previous run.
n	y	n	<p>During its first run, this Knowledge Script uses the current time. In subsequent runs, it raises events for hardware records posted since the previous run and before Stop Time.</p> <p>In the first run after Stop Time, this script raises an information event indicating Stop Time has elapsed. It continues to run as scheduled but does not raise events while Stop Time is in the past.</p> <p>If Stop Time precedes the first run time, this script raises an event for hardware records posted from Start Time to Stop Time and raises an information event indicating Stop Time has elapsed.</p>
y	n	n	During its first run, this Knowledge Script raises events for hardware records posted between Start Time and the current time. In subsequent runs, this script raises events for hardware records posted since the previous run.
y	y	n	<p>During its first run, this Knowledge Script raises events for hardware records posted between Start Time and the current time. In subsequent runs, this script raises events for hardware records posted since the previous run and before Stop Time.</p> <p>Reporting does not begin until on or after Start Time. This script will run as scheduled before Start Time, but will not receive hardware records or raise events until on or after Start Time.</p> <p>In the first run after Stop Time, this script raises an information event indicating Stop Time has elapsed. This script continues to run as scheduled but does not raise events while Stop Time is in the past.</p>
n/y	n	y	During its first run, this Knowledge Script uses the Epoch time and does not raise events. In subsequent runs, it raises events for hardware records posted since the previous run.



Start Time	Stop Time	Beginning of Log	Knowledge Script Action
n/y	y	y	<p>During its first run, this Knowledge Script uses the Epoch time and does not raise events. In subsequent runs, it raises events for hardware records posted since the last run and before Stop Time.</p> <p>In the first run after Stop Time, this script raises an information event indicating Stop Time has elapsed. It continues to run as scheduled but does not raise events while Stop Time is in the past.</p> <p>If Stop Time precedes the first run time, this script raises an event for hardware records posted from the Epoch time to Stop Time and raises an information event indicating Stop Time has elapsed.</p>

## 5.3 Fan

Use this Knowledge Script to monitor the server fan status for HP and Dell computers. For Dell computers, this script raises an event if the fan revolutions per minute (RPM) exceeds the thresholds you set, or if the fan RPM falls outside the system's configured range. For HP computers, this script raises an event if the fan RPM exceeds the system-configured operating threshold by a percentage you set.

For information about fan object properties, see [Section 5.1.1, "Fan Properties," on page 152](#).

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.3.1 Resource Objects

Any fan on an HP or Dell computer running Linux

### 5.3.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 5.3.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Raise event if fan status is not OK?	Set to <code>Yes</code> to raise an event if the fan status is other than OK. The default is <code>yes</code> .

<b>Description</b>	<b>How to Set It</b>
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
<b>HP specific settings</b>	
Raise event if fan speed exceeds threshold in percent?	Set to <code>Yes</code> to raise an event if the fan speed exceeds the percentage threshold value you set. The default is <code>yes</code> .
Threshold value	Specify the event threshold as a percent, from 1 to 100, of the acceptable fan speed. AppManager calculates the percent using a range of 0 to the maximum as specified by the hardware vendor. The default is 20.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
<b>Dell specific settings</b>	
Raise event if fan speed exceeds threshold in RPM?	Set to <code>Yes</code> to raise an event if the fan speed exceeds the RPM threshold value you set. The default is <code>yes</code> .
Threshold value (RPM)	Specify the event threshold value as the maximum fan speed in RPM. The default is 2000.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event if fan speed is out of system configured range?	
Minimum warning threshold - Maximum warning threshold range?	Set to <code>Yes</code> to raise an event if the fan speed lies outside the warning threshold range defined by the minimum and maximum warning threshold values. The default is <code>no</code> .
Minimum failure threshold - Maximum failure threshold range?	Set to <code>Yes</code> to raise an event if the fan speed lies outside the failure threshold range defined by the minimum and maximum failure threshold values. The default is <code>no</code> .
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the warning or failure event. The default is 5.
Raise event if AppManager fails to get metrics?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the hardware fans. The default is <code>yes</code> .
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity when job fails	Specify the event severity, from 1 to 40, to indicate the importance of an event when this job fails. The default is 5.
<b>Data Collection</b>	
Collect data for fan speed in percent or RPM?	Set to <code>Yes</code> to collect data for fan speed. For Dell computers, fan speed is measured in RPM. For HP computers, fan speed is measured in percentage of the maximum fan speed. By default, the data is not collected.

## 5.4 LogicalDrive

Use this Knowledge Script to monitor the operational status of disk partitions, called logical drives, on HP or Dell computers running Linux. The script raises an event if a monitored logical drive is in a state other than one of the states that you specify to be operational states. The script can also report events based on error conditions that occur when the software is not properly installed, configured, or running.

For information about logical drive object properties, see [Section 5.1.2, “LogicalDrive Properties,” on page 152.](#)

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.4.1 Resource Objects

Any logical disk or disks on an HP or Dell computer running Linux

### 5.4.2 Default Schedule

The default interval for this script is **Every 15 minutes.**

### 5.4.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when AppManager fails to get logical drive metrics ?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the logical drive. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when logical drive is not functional?	Set to <code>Yes</code> to raise an event if the logical drive is in any state other than the states that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional states</b> . The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

Description	How to Set It
Raise event when logical drive is fully functional?	Set to <code>Yes</code> to raise an event if the logical drive is in a state that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional states</b> . The default is <code>no</code> .
Event severity when logical drive is fully functional	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Comma-separated list of fully functional status	Specify one or more states that you want AppManager to consider functional. If you specify more than one state, separate them with commas and no spaces. For example, <code>locked,unassigned</code> . The default is <code>OK</code> .

## 5.5 PhysicalDrive

Use this Knowledge Script to monitor the operational status of physical drives on HP or Dell computers running Linux. This script raises an event if a monitored drive is in a state other than one of the states that you specify to be operational states. This script can also report events based on error conditions that occur when the software is not properly installed, configured, or running.

For information about physical drive object properties, see [Section 5.1.3, “PhysicalDrive Properties,” on page 153](#).

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.5.1 Resource Objects

Any physical disk or disks on an HP or Dell computer running Linux

### 5.5.2 Default Schedule

The default interval for this script is **Every 15 minutes**.

### 5.5.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when AppManager fails to get physical drive metrics ?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the drive. The default is <code>yes</code> .

Description	How to Set It
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when physical drive is not functional?	Set to <code>Yes</code> to raise an event if the drive is in any state other than the states that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional states</b> . The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when physical drive is fully functional?	Set to <code>Yes</code> to raise an event if the drive is in a state that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional status</b> . The default is <code>no</code> .
Event severity when physical drive is fully functional	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Comma-separated list of fully functional status	Specify one or more states that you want AppManager to consider functional. If you specify more than one state, separate them with commas and no spaces. For example, <code>OK,locked,unassigned</code> . The default is <code>OK</code> .

## 5.6 PhysicalMemory

Use this Knowledge Script to monitor the operational status of physical memory on HP or Dell computers running Linux. The script raises an event if the status of physical memory is other than OK.

For information about physical memory object properties, see [Section 5.1.4, “PhysicalMemory Properties,”](#) on page 153.

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.6.1 Resource Objects

Physical memory on an HP or Dell computer running Linux

### 5.6.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 5.6.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Raise event if physical memory status is not OK?	Set to <code>Yes</code> to raise an event if the physical memory status is other than OK. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event if AppManager fails to get metrics?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the physical memory. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of an event when this job fails. The default is 5.

## 5.7 PowerConsumption

Use this Knowledge Script to monitor the power consumption on Dell computers running Linux. This script raises an event if the power consumption status is not OK, or when the power consumption falls outside configured bounds or the thresholds you set.

For information about power consumption object properties, see [Section 5.1.5, “PowerConsumption Properties,”](#) on page 153.

This Knowledge Script requires OMSA components on the Dell computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

### 5.7.1 Resource Objects

Any Dell computer running Linux

### 5.7.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 5.7.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Raise event if power supply status is not OK?	Set to <code>Yes</code> to raise an event if the power supply status is not OK. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.

<b>Description</b>	<b>How to Set It</b>
Raise event if power consumption of server is out of the specified threshold range?	Set to <code>Yes</code> to raise an event if the server power consumption falls outside the range you specified. The default is <code>no</code> .
Minimum value	Set the minimum power consumption value in Watts to define the lower bound of an acceptable power consumption range. If enabled, this job raises an event when the server power consumption falls below the acceptable power consumption range. The default is 200 Watts.
Maximum value	Set the maximum power consumption value in Watts to define the upper bound of an acceptable power consumption range. If enabled, this job raises an event when the server power consumption goes above the acceptable power consumption range. The default is 400 Watts.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event if power supply reading exceeds threshold?	Set to <code>Yes</code> to raise an event if the power supply output in Amperes exceeds the threshold you set. The default is <code>no</code> .
Threshold value (in Amperage)	Set the maximum acceptable power supply output in Amperes. If enabled, this job will raise an event when the power supply output exceeds this value. The default is 0.5.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event if power consumption exceeds configured system warning or failure thresholds?	Set to <code>Yes</code> to raise an event when the power consumption reaches the system defined warning or failure thresholds. The default is <code>yes</code> .
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event if AppManager fails to get metrics?	Set to <code>Yes</code> to raise an event when AppManager fails to collect any information about power consumption. The default is <code>yes</code> .
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of the event. The default is 5.
Event severity when job fails	Specify the event severity, from 1 to 40, to indicate the importance of an event when this job fails. The default is 5.
<b>Data Collection</b>	
Collect data for power consumption?	Set to <code>Yes</code> to collect data for the server power consumption sensors. By default, the data is not collected.

## 5.8 PowerSupply

Use this Knowledge Script to monitor the operational status of power supplies on HP or Dell computers running Linux. This script raises an event if a monitored power supply is not operating properly. You can also choose to raise events for other conditions and set severities to indicate the importance of each type of event.

For information about power supply object properties, see [Section 5.1.6, "PowerSupply Properties," on page 154](#).

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

## 5.8.1 Resource Objects

An HP or Dell computer running Linux

## 5.8.2 Default Schedule

The default interval for this script is **Every 15 minutes**.

## 5.8.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when AppManager fails to get metrics ?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the power supply. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when power supply is not fully functional ?	Set to <code>Yes</code> to raise an event if the power supply does not work properly. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when power supply is fully functional?	Set to <code>Yes</code> to raise an event if the power supply works properly. The default is <code>no</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Raise event when power supply is absent ?	Set to <code>y</code> to raise events if the power supply cannot be identified. The default is <code>no</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 15.



## 5.9 SmartArrayController

Use this Knowledge Script to monitor the operational status of storage controllers, such as HP Smart Array RAID controllers, on computers running Linux. This script raises an event if a controller is in a state other than one of the states that you specify to be an operational state. This script can also report events based on error conditions that occur when the software is not properly installed, configured, or running.

For information about smart array controller object properties, see [Section 5.1.7, “SmartArrayController Properties,” on page 154.](#)

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.9.1 Resource Objects

Any Smart Array RAID controller on Linux

### 5.9.2 Default Schedule

The default interval for this script is **Every 15 minutes.**

### 5.9.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when AppManager fails to get storage controller metrics ?	Set to <code>Yes</code> to raise an event if AppManager cannot collect any information about the controller. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when storage controller is not functional?	Set to <code>Yes</code> to raise an event if the controller is in any state other than the states that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional status</b> . The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 5.
Raise event when storage controller is fully functional?	Set to <code>Yes</code> to raise an event if the controller is in a state that you specify as functional. You specify which states are considered functional using the parameter <b>Comma-separated list of fully functional states</b> . The default is <code>no</code> .

Description	How to Set It
Event severity when storage controller is fully functional	Specify the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
Comma-separated list of fully functional status	Specify one or more states that you want AppManager to consider functional. If you specify more than one state, separate them with commas and no spaces. For example, <code>OK,locked,unassigned</code> . The default is <code>OK</code> .

## 5.10 SolarisHWLog

Use this Knowledge Script to monitor hardware errors reported in Solaris logs. This script monitors logs based on regular expression patterns you can specify for the following:

- ◆ hardware log name
- ◆ device name
- ◆ information priority
- ◆ warning priority
- ◆ error priority

This script is intended to monitor Solaris hardware logs. This script raises one event per log when it finds messages that match your regular expression criteria. The event detailed message orders the matched hardware messages by device name and priority.

---

**NOTE:** This Knowledge Script is available as soon as you install it. It does not require that you run the `Discovery_HardwareUNIX` Knowledge Script to discover resources.

---

### 5.10.1 Filtering

This Knowledge Script provides two levels of filtering for Solaris hardware messages: source and priority. Source filtering lets you select the source of the messages this script parses. Source filtering consists of the following:

- ◆ The log name filter selects logs matching your UNIX-like globbing patterns
- ◆ The device name filter selects device names matching your regular expression criteria
- ◆ The Fault Management Daemon (FMD)-only option selects messages only from the FMD. This option requires that you configure the FMD to redirect messages to a system log.

The second type of filtering, by priority, parses and classifies hardware messages as information, warning, or error. Priority filtering consists of the following:

- ◆ The error filter selects messages matching your error regular expressions. This script processes these messages as errors.
- ◆ The warning filter selects messages matching your warning regular expressions. This script processes these messages as warnings.
- ◆ The information filter selects messages matching your information regular expressions. This script processes these messages as informative.

At each run, this script receives hardware messages from the logs you specified. This script tests each message for source as follows:

1. If FMD-only is Yes, is this a FMD message?
2. Does the message device name match one of your device name regular expressions?

Each hardware message that passes the source tests is tested against the priority filters, in descending priority order: error, then warning, then information. The first priority match determines the message priority and removes it consideration by the remaining priority filters. Messages that do not match any priority filter are discarded.

This script groups and presents the hardware messages by priority in the event detailed message.

## Selecting FMD-only Entries

If parameter *Select only FMD entries* is set to `Yes`, this script selects only those hardware messages produced by the Solaris Fault Management Daemon (FMD) from log files. All non-FMD messages are discarded.

When parameter *Select only FMD entries* is set to `No`, this script selects all hardware messages, including, if they exist, hardware messages from FMD.

## Selecting a Lowest Priority

Parameter *Lowest level of priority for matching* sets the lowest priority this script will report in the event detailed message. For example, if you choose `warn` as the lowest priority, this script will only test for and report errors and warnings.

## 5.10.2 Script Logs for Large Message Volumes

Each event raised by this script can report up to 7000 lines of hardware messages per priority in the detailed message. If the script reports all three priorities, error, warning, and information, the event detailed message can include a maximum of 21,000 lines of hardware messages.

If the lines of hardware messages exceeds 7000 lines for a priority in an iteration, this script raises an event with the first 7000 lines in the detailed message and writes all the lines for the priority to a log it creates. The event detailed message includes the path to the log.

When this script creates a log, it writes it to this folder:

```
$AM_HOME/log/solaris_hw_log/
```

where `$AM_HOME` represents the AppManager home directory on the agent computer. The log name is a concatenation of the AppManager job ID, the path to the log from which the messages were parsed, and the hardware message priority:

```
Job<jobID>.<hardware_log_path>[-enumeration].<log_info|log_warn|log_err>
```

This script replaces forward slashes in the log path with underscores when it creates the log name. For example, if this script runs as AppManager job 1731, parsing more than 7000 warning and 7000 information hardware messages from `log /var/adm/messages.log` during an iteration, it creates one log for the information messages and one for the warning messages, naming them:

```
Job1731._var_adm_messages.log_info  
Job1731._var_adm_messages.log_warn
```

If this script again receives more than 7000 hardware messages for the warning priority in a subsequent iteration, it enumerates rather than overwrites the existing log by appending `-1` to the existing log name. For example:

```
Job1731._var_adm_messages.log_warn  
Job1731._var_adm_messages-1.log_warn
```

This script can create up to 12 logs for each job ID, hardware log file name, and priority. The unenumerated log always contains the most recent hardware messages and the highest enumerated log contains the oldest. If subsequent iterations again return a high hardware message volume, this script deletes the log enumerated -11, if it exists, increments the enumeration on the other logs, and writes the new hardware messages to the unenumerated log.

### 5.10.3 Resource Objects

Any computer running Solaris.

### 5.10.4 Default Schedule

The default interval for this script is **Every 30 minutes**.

### 5.10.5 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Monitoring Settings</b>	
File names to parse (full path, unix-like shell pattern matching notation and comma-separated)	Type a list of hardware log names for this Knowledge Script to monitor, separating the names with commas, and providing the full path. You can use UNIX-like shell pattern matching in the log names. The default is <code>/var/adm/messages*</code> .
Device name regex (comma-separated)	Type the device names for this Knowledge Script to monitor. Separate multiple names with commas. You can use regular expressions in the device name. The default is <code>c[0-9]+t[0-9]+d[0-9]+[sp][0-9]+,net[0-9]+,zfs-diagnosis</code> .
<b>NOTE</b>	
<ul style="list-style-type: none"> <li>◆ When this field is empty, this script will monitor all devices.</li> <li>◆ Device name changes do not cause the job to parse any logs from the beginning even when <i>Parse log from beginning</i> is yes.</li> </ul>	
Info Regex (comma-separated)	Type the keywords used to find information records within hardware log files. Separate multiple keywords with commas. You can use regular expressions in the keywords. The default is <code>notice,info,init</code> .
<b>NOTE</b>	
<ul style="list-style-type: none"> <li>◆ When this field is empty, this script will not raise information events.</li> <li>◆ Information keyword changes do not cause the job to parse any logs from the beginning even when <i>Parse log from beginning</i> is yes.</li> </ul>	

Description	How to Set It
Warn Regex (comma-separated)	<p>Type the keywords used to find warning records within hardware log files. Separate multiple keywords with commas. You can use regular expressions in the keywords. The default is <code>warn,timeout,retry,degrade</code>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>◆ When this field is empty, this script will not raise warning events.</li> <li>◆ Warning keyword changes do not cause this script to parse any logs from the beginning even when <i>Parse log from beginning</i> is yes.</li> </ul>
Error Regex (comma-separated)	<p>Type the keywords used to find error records within hardware log files. Separate multiple keywords with commas. You can use regular expressions in the keywords. The default is <code>error,fault,fail,crit,panic,defect,major</code>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>◆ This script will not raise error events when this field is empty.</li> <li>◆ Error keyword changes do not cause this script to parse any logs from the beginning even when <i>Parse log from beginning</i> is yes.</li> </ul>
Select only FMD entries?	<p>Select <b>Yes</b> to select only those messages that come from the Solaris Fault Management Daemon (FMD). Otherwise, this script selects all hardware messages including, if they exist, hardware messages from FMD. The default is unselected.</p> <p><b>NOTE:</b> To use this option, you must configure the FMD to redirect its records to the syslog. This Knowledge Script can parse FMD records from the syslog, but has no direct interaction with the FMD.</p>
Lowest level of priority for matching	<p>Choose the lowest priority of information you wish to receive from the hardware log files. The choices are <code>info</code>, <code>warn</code>, and <code>error</code>. The default is <code>info</code>.</p>
Event severity	<p>Specify the event severity, from 1 to 40, to indicate the importance of an event when a hardware log record matches a specified priority and keyword. The default is 5.</p>

Description	How to Set It
Parse log file from beginning?	<p>Select <b>Yes</b> to parse logs one time from the beginning rather than from the end. The default is unselected.</p> <p>By default, this script parses each log for hardware messages added since the last run. This parameter allows you to override the default behavior and parse each log one time from the beginning before resuming default behavior. This script stores parsing information internally to prevent it from repeatedly parsing a log from the beginning.</p> <p>This parameter affects log file parsing as follows:</p> <ul style="list-style-type: none"> <li>◆ If yes, parse each log from the beginning one time and raise events for qualified hardware messages. In subsequent runs, parse each log file for hardware messages added since the last run.</li> <li>◆ If no, store parsing information the first run but do not raise events. In subsequent runs, parse each log for hardware messages added since the last run.</li> <li>◆ If changed from no to yes, parse each log from the beginning at next run. In subsequent runs, parse each log for hardware messages added since the last run.</li> <li>◆ If changed from yes to no, parse each log for hardware messages added since the last run.</li> </ul> <p><b>TIP:</b> If you want to parse each log from the beginning and anticipate a high initial log message count, NetIQ recommends you run this script with <code>schedule run once</code> the first time to raise events for all the hardware messages in each log. When the job completes, restart the script on a schedule to raise events for hardware messages added since the last run.</p>
<b>Event Settings</b>	
Raise event if specified log is missing?	Select <b>Yes</b> to raise an event if one of the hardware logs you specified is missing. The default is yes.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of an event when one of the hardware log files you specified is missing. The default is 5.
Raise event if AppManager fails to get metrics?	Select <b>Yes</b> to raise an event if AppManager cannot collect any information about the Solaris hardware logs. The default is Yes.
Event severity	Specify the event severity, from 1 to 40, to indicate the importance of an event when AppManager cannot collect any information about the Solaris hardware logs. The default is 5.
Event severity when job fails	Specify the event severity, from 1 to 40, to indicate the importance of an event when this job fails. The default is 5.
Enable debugging?	Select <b>Yes</b> to enable debugging of this.

## 5.11 Temperature

Use this Knowledge Script to monitor the temperature of HP or Dell computers running Linux. This script raises an event if the temperature exceeds the threshold you specify. This script can also raise an event when the temperature exceeds the vendor recommended threshold for the sensor.

For information about temperature object properties, see [Section 5.1.8, “Temperature Properties,” on page 154](#).

If you are monitoring Dell equipment, this Knowledge Script requires OMSA components on the computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

If you are monitoring HP equipment, this Knowledge Script requires the HP Array Configuration Utility CLI for Linux and HP System Health Application and Command Line Utilities for Linux installed on the computer you are monitoring.

### 5.11.1 Resource Objects

Any HP or Dell computer running Linux

### 5.11.2 Default Schedule

The default interval for this script is **Every 15 minutes**.

### 5.11.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event settings</b>	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of the event when this job fails. The default severity level is 5.
Raise event when AppManager fails to get metrics?	Set to <code>Yes</code> to raise an event if the job completes but does not return any temperature data. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event in which AppManager fails to get metrics. The default is 5.
Raise event when temperatures are over thresholds?	Set to <code>Yes</code> to raise an event if any sensor reports that the temperature is above a specified percent of the level that the vendor considers acceptable. The default is <code>yes</code> .
Threshold percentage	Set the event threshold by specifying a percentage, from 0 to 200, of the acceptable temperature. AppManager calculates the percent using the range of 0 to the maximum as specified by the hardware vendor. Because Celsius and Fahrenheit define 0 degrees differently, the threshold will vary depending on which temperature scale you select. The default is 90.
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event in which the temperature reaches the percentage you specified in the <b>Threshold percentage</b> parameter. The default is 15.

Description	How to Set It
Hardware vendor temperature threshold event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event in which the temperature reaches the vendor-specified limit for the sensor. The default is 5.
<b>HP specific settings</b>	
Temperature measurement unit	Select <code>Celsius</code> or <code>Fahrenheit</code> to specify the scale that the sensors use to report temperature data. AppManager uses this scale for calculations and reporting. The default is <code>Fahrenheit</code> .  This parameter is only available for HP-UX computers.
Collect data?	Set to <code>Yes</code> to collect data for the temperatures reported by the hardware sensors. By default, data is not collected.

## 5.12 Voltage

Use this Knowledge Script to monitor the server voltage probe on Dell computers running Linux. This script raises an event if the voltage probe status is other than OK and when the voltage probe reading falls outside system-defined thresholds or the thresholds you set.

For information about voltage probe object properties, see [Section 5.1.9, “Voltage Properties,” on page 154](#).

This Knowledge Script requires OMSA components on the Dell computer you are monitoring. You can install these components using the `srvadmin-all` meta package.

### 5.12.1 Resource Objects

Voltage probe on a Dell computer running Linux

### 5.12.2 Default Schedule

The default interval for this script is **Every 5 minutes**.

### 5.12.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Settings</b>	
Raise event if voltage probe status is not OK?	Set to <code>Yes</code> to raise an event if the voltage probe has a status value other than <code>OK</code> . The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event in which the voltage probe status is other than <code>OK</code> . The default is 5.
Raise event if voltage probe reading is not good?	Set to <code>Yes</code> to raise an event if the voltage probe reading is not good. The default is <code>yes</code> .



<b>Description</b>	<b>How to Set It</b>
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event AppManager reports when the voltage probe reading is not good. The default is 5.
Raise event if voltage probe reading exceeds threshold?	Set to <code>Yes</code> to raise an event if the voltage probe reading exceeds the threshold value you set. The default is <code>yes</code> .
Threshold value (in Volts)	Set the maximum acceptable voltage probe reading in Volts. If enabled, this job will raise an event when the voltage probe reading exceeds this value. The default is 2.5.
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event where the voltage probe reading exceeds the threshold you set. The default is 5.
Raise event if voltage probe reading is out of system configured range?	
Minimum warning threshold - Maximum warning threshold range?	Set to <code>Yes</code> to raise an event if the voltage probe reading is outside the range defined by the minimum and maximum warning threshold values. The default is <code>no</code> .
Minimum failure threshold - Maximum failure threshold range?	Set to <code>Yes</code> to raise an event if the voltage probe reading is outside the range defined by the minimum and maximum failure threshold values. The default is <code>no</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event where the voltage probe reading is outside the warning and/or failure threshold range. The default is 5.
Raise event if AppManager fails to get metrics?	Set to <code>Yes</code> to raise an event when AppManager fails to collect any information about the voltage probe. The default is <code>yes</code> .
Event severity	Specify the event severity level, from 1 to 40, to indicate the importance of an event where AppManager fails to get any information about the voltage probe. The default is 5.
Event severity when job fails	Specify the event severity level, from 1 to 40, to indicate the importance of an event where this job fails. The default is 5.
<b>Data Collection</b>	
Collect data for voltage probe reading?	Set to <code>Yes</code> to collect data for the chassis voltage probe. By default, the data is not collected.



# 6 AMAdminUNIX Knowledge Scripts

AppManager for UNIX provides the following Knowledge Scripts to perform administrative tasks for UNIX agents and your AppManager system. In addition to the AMAdminUNIX Knowledge Scripts, the AppManager for Self Monitoring Knowledge Scripts provides information about the health of your AppManager components.

From the Knowledge Script view of the Control Center Console, you can access more information about any NetIQ-supported Knowledge Script by selecting it and pressing **F1**. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
<a href="#">AgentHealthProxy</a>	Checks the availability of a remote managed UNIX computer and monitors the health of the remote UNIX agent. This Knowledge Script uses a proxy UNIX agent to monitor remote UNIX agents.
<a href="#">AgentInstallProxy</a>	Installs the 8.0.11 AppManager UNIX agent on remote UNIX and Linux computers in your network. This Knowledge Script uses a proxy AppManager UNIX agent to install on remote computers. To remotely install NetIQ UNIX Agent 7.5 or later, use NetIQ UNIX Agent Manager.
<a href="#">AgentUpdate</a>	Updates the 7.5 AppManager UNIX agents remotely on computers in your network. To update NetIQ UNIX Agent 7.5, use NetIQ UNIX Agent Manager.
<a href="#">AgentUpdateSecurityLevel</a>	Updates the security level for the UNIX agent remotely on UNIX client computers in your network.
<a href="#">SchedMaint</a>	Sets a server maintenance period for a managed computer. During the maintenance period, regularly scheduled jobs are prevented from running.
<a href="#">SetPrimaryMS</a>	Sets the primary and secondary management server for UNIX agents in multiple management server configurations.

## 6.1 AgentHealthProxy

Run this Knowledge Script on an AppManager 7.0 or later UNIX agent to monitor the health of one more remote AppManager 7.0 or later UNIX agents.

When you drag this Knowledge Script to a computer in the TreeView, the Knowledge Script runs on that machine and tries to communicate with each of the remote computers in the machine list. This Knowledge Script:

- Checks the availability of a managed UNIX computer by first sending an ICMP Echo request to the managed UNIX computer. If the remote computer does not respond, this Knowledge Script sends an ICMP Echo request to the managed UNIX computer's default router and an event is raised.

- ◆ Monitors the health of the UNIX agent by checking a timestamp value created by the UNIX agent. Normally, the UNIX agent creates a timestamp value every 90 seconds. If the age of the timestamp value exceeds the threshold, an event is raised and the UNIX agent is restarted.
- ◆ This Knowledge Script enables self-monitoring of the UNIX agent health by raising appropriate events. You can use these events to correct unhealthy agents by restarting etc. This feature also enables you to restart unhealthy agents automatically without any manual intervention.

Use this Knowledge Script to remotely validate the health of the UNIX agent on a scheduled basis or for diagnostic purposes (for example, if there are gaps in data collection). This Knowledge Script is useful because it can detect a problem with a remote agent and reliably notify the AppManager administrator.

The proxy UNIX agent that runs the Knowledge Script must be configured to run as the **root** user account.

The remote UNIX agents you want to monitor, and the proxy UNIX agent that runs the Knowledge Script, must be Version 7.0 or later. The remote UNIX agents must be accessible through the network from the computer where the proxy UNIX agent is installed. If you attempt to use this Knowledge Script to monitor a UNIX agent that is earlier than version 7.0, an event is raised that indicates “the timestamp is not found.”

Do not use this Knowledge Script to monitor the health of the UNIX agent that runs the Knowledge Script. To successfully monitor the health of the proxy UNIX agent, run this Knowledge Script on another proxy UNIX agent.

To use this Knowledge Script to monitor more than one remote managed UNIX computer, all of the computers you want must be accessible using the same **root** user account information.

---

**NOTE:** Ensure that the `nqmdaemon` config file in the remote managed UNIX computers are not renamed to effectively monitor them.

---

This Knowledge Script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX or Linux computer. By default, SSH is used, but you can select **Telnet/FTP** from the **Connection Transport** list to use Telnet instead. If you choose to use Telnet, you must supply a non-root user account name and password.

---

**NOTE:** Telnet and FTP send your username, password, and other information across the network in cleartext, making it easy for others to see this data.

---

If you are using Telnet to monitor the remote managed UNIX computer, ensure that su permission are given in the remote managed UNIX computer for that username.

---

## 6.1.1 Resource Objects

A managed UNIX computer where the NetIQ UNIX Agent 7.5 is installed. The UNIX agent must be configured to run as the **root** user account.

## 6.1.2 Default Schedule

The default interval for this script is **Every 10 minutes**.

To avoid raising false events, do not configure this Knowledge Script to run more frequently than the interval that the UNIX agent updates its timestamp. Ideally, the default interval should be more than 4 minutes.

## 6.1.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Notification</b>	
Use the following parameters to raise events and set the severity level.	
Raise event if age of timestamp exceeds threshold?	Select <b>Yes</b> to raise an event when the age of the timestamp exceeds the maximum threshold you set. The default is Yes.
Threshold -- Maximum age of timestamp	Enter the maximum age of timestamp before an event is raised. The minimum threshold is 3 minutes and the maximum threshold is 99999 minutes. The default is 9 minutes.
Event severity when age of timestamp exceeds threshold	If the age of the UNIX agent's timestamp value exceeds the specified threshold, set the event severity level, from 1 through 40, to indicate the importance of this event condition. The default severity is 8.
<b>Remote Host Connection</b>	
UNIX computers to monitor (comma-separated)	Enter the IP addresses of the remote UNIX computers you want to monitor, separated by commas and no spaces.
Password for root user account	Enter the root user account password that the proxy agent must use to connect to the remote UNIX computer. This is a mandatory field.
<b>Connection Transport</b>	Specify the connection mode between the proxy agent and the monitored UNIX computer: <ul style="list-style-type: none"><li>◆ <b>Telnet/FTP</b> to connect using Telnet.</li><li>◆ <b>SSH/FTP</b> to connect using SSH.</li></ul>
Telnet non-root user account	Enter the Telnet non-root user account if you are using Telnet to connect to the monitored computer.
Telnet non-root user password	Enter the Telnet non-root user password if you are using Telnet to connect to the monitored computer. Leave this parameter value blank if you are using SSH to connect to the monitored computer.
Restart UNIX agent if age of timestamp exceeds threshold?	Select Yes to restart the UNIX agent if the age of the timestamp exceeds the maximum age you set. The default is Yes.
Event severity for internal failure	Set the event severity level, from 1 to 40, to indicate the importance of an event if the maximum pool threshold is exceeded. The default is 5.

---

**NOTE:** When running the AMADMINUNIX\_AgentHealthProxy Knowledge Script with Secure Shell (SSH) as the connection method to the remote UNIX or Linux computer, if you specify an incorrect password for the root account, the Knowledge Script raises an event that incorrectly states that the login attempt was successful. If you see an event message similar to the event message below, you must update the job properties to specify the correct root password and start the job:

```
Output: Permission denied at /usr/netiq/AM/bin/UnixAgentHealthProxy.pl
More Info:
"SSH login OK to <machine> with root Using SSH/SFTP combination."
```

---

## 6.2 AgentInstallProxy

Use this Knowledge Script on a version 8.0 proxy AppManager UNIX agent to install a version 8.0.11 agent on remote UNIX and Linux computers in your AppManager site.

You cannot use this Knowledge Script to install a version 7.5 or higher NetIQ UNIX agent.

To install the AppManager UNIX agent on a remote UNIX or Linux computer, the remote computer must be accessible through the network from the computer where the proxy AppManager UNIX agent is installed. This Knowledge Script can use either the Secure Shell (SSH) program with root password authentication or Telnet to make a secure connection to the remote UNIX or Linux computer. By default, Telnet is used, but you can select SSH/SFTP from the **Connection Transport** list to use Secure Shell instead. If you choose to use Telnet, you must supply a non-root user account name and password.

This Knowledge Script uses a version 8.1.0.11 AppManager UNIX agent as the proxy to install the version 8.1.0.11 AppManager UNIX agent on remote UNIX and Linux computers.

### 6.2.1 Running this Knowledge Script

The proxy AppManager UNIX agent where you run this Knowledge Script must be configured to run as the `root` user account.

All of the computers where you want to install the AppManager UNIX agent using this Knowledge Script must be accessible using the same root user account information.

The failure messages associated with a scenario where you inadvertently tried to run with an invalid root user account password might not clearly state this fact. If you see a failure that states, for example, "Cannot switch to root user on [X computer]," "Permission denied at UnixAgentInstallProxy.pl line X," "unable to get a session to start the Installation," or "Unable to get a session to start the Installation for [X computer]," **first check to make sure you are using a valid root password.**

If the `.tar` file or `.ini` file that you have specified for the "**Installation Source Configuration**" parameter (that is, the file that you intend to use for the installation on a remote computer) already exists in the directory you listed for the **Temporary directory on the remote computer** parameter, you see a failure. The event states, "Can't FTP File <File Name>: permission denied." If this occurs, run the job again. After the initial failure, the `.tar` or `.ini` files are removed from the directory.

When you run this Knowledge Script using a hosts file, the hosts file should list any file locations of `.ini` files before it lists locations of `.tar` files. The job fails and the Knowledge Script transfers the `.tar` file and never transfer the `.ini` file unless you make sure to list the `.ini` files first.

## 6.2.2 Platform Support

This Knowledge Script supports all platforms supported by the AppManager UNIX agent 7.0.1, with the following exceptions:

- ♦ HP-UX in 32-bit and 64-bit mode is supported. Most AMAdminUNIX and UNIX Knowledge Scripts can run on HP-UX in 64-bit mode (because you can install and run the AppManager UNIX agent there). However, a computer running HP-UX in 64-bit mode cannot serve as a proxy.
- ♦ Red Hat Advanced Server (AS) 3.0 on Opteron with 64-bit operating system is supported with the AppManager UNIX agent running in 32-bit mode.
- ♦ Red Hat AS 3.0 on Itanium in 64-bit mode is supported.

## 6.2.3 Resource Objects

A managed UNIX computer where the AppManager UNIX Agent 7.0.1 is installed. The AppManager UNIX agent must be configured to run as the root user account.

## 6.2.4 Default Schedule

By default, this Knowledge Script is **only run once on each proxy UNIX computer**.

## 6.2.5 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
<b>Event Notification</b>	
Set parameters for event notification.	
Raise event if installation fails?	Set to y to raise an event indicating that the installation has failed. By default, events are enabled.
Event severity when installation fails	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 10.
Raise event if installation succeeds?	Set to y to raise an event indicating that the installation is complete and has succeeded. The default is y.
Event severity when installation succeeds	Set the event severity level, from 1 to 40, to indicate the importance of the event. The default is 25.
<b>Remote Host Connection</b>	
Configure access to the remote managed computers by specifying their root password. All of the remote computers must use the same root password. This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.	
Password for root user account	If you want to use Secure Shell (SSH) for the connection to the remote computers, make sure SSH with root authentication is enabled on the remote UNIX computers where you want to install the AppManager UNIX agent.  For this parameter, you must specify the password for the root user to securely access the remote UNIX computers. This Knowledge Script does not support SSH root authentication with an RSA key.

Description	How to Set It
<b>Connection Transport</b>	<p>This Knowledge Script can use SSH with root password authentication or Telnet to communicate with the remote managed computer.</p> <p>If you select the Telnet/FTP option (the default), the Telnet prompt on the remote computer must end with a space or one of the following characters:</p> <pre data-bbox="634 384 651 485">% &gt; # \$</pre> <p>Here is an example of a supported Telnet prompt:</p> <pre data-bbox="634 562 813 583">user@hostname&gt;</pre> <p>Here is an example of an unsupported Telnet prompt:</p> <pre data-bbox="634 661 1073 709">&lt;user@hostname:/tmp - 2005-Mar-09&gt; -&gt;</pre> <p>In the example above, the last character in the first line of the 2-line prompt is a line feed character, which is not supported.</p>
Telnet non-root user account	<p>If you selected Telnet to connect to the remote UNIX computers, specify a non-root user account to use for the connection. When connecting to a remote UNIX computer using Telnet and FTP, this Knowledge Script switches from the non-root user to the root user.</p>
Telnet non-root user password	<p>If you selected Telnet as the connection transport medium, specify the password for the non-root user account to connect to the remote UNIX computers.</p>
<b>Installation Source Configuration</b>	
<p>Set parameters to specify the remote computers where you want to install the AppManager UNIX agent, and the location of installation tar package and the silent installation file.</p>	
<p>The simplest way to configure and run this Knowledge Script is to store the installation .tar packages and the silent installation files in the same directory, using the standard naming convention. If these files are in the same directory and use the standard naming convention, you simply specify the remote UNIX computers where you want to install the AppManager UNIX agent and the directory where the installation files are located.</p>	
<p>For installation .tar packages, the following naming convention applies:</p>	
<ul style="list-style-type: none"> <li>◆ UnixClient-aix.tar for IBM AIX computers</li> <li>◆ UnixClient-hpux.tar for HP-UX computers</li> <li>◆ UnixClient-linux.tar for Red Hat and SuSe Linux computers</li> <li>◆ UnixClient-solaris.tar for Sun Solaris computers</li> </ul>	
<p>For silent installation files, the following naming convention applies:</p>	
<ul style="list-style-type: none"> <li>◆ UnixClient-aix.ini for IBM AIX computers</li> <li>◆ UnixClient-hpux.ini for HP-UX computers</li> <li>◆ UnixClient-linux.ini for Red Hat and SuSe Linux computers</li> <li>◆ UnixClient-solaris.ini for Sun Solaris computers</li> <li>◆ UnixClient-linux64 for Red Hat Linux on Itanium processors</li> </ul>	
<p>If you do not use these standard names, you must specify the directory path and filename.</p>	



Description	How to Set It
Full path to hosts file or comma-separated list of computers where agent should be installed	<p>Specify the computers you want by either:</p> <ul style="list-style-type: none"> <li>♦ Entering the full directory path and filename for the hosts file that contains a list of the remote managed UNIX computers where you want to install AppManager UNIX agents. For example, <code>/home/appmgr/agtinstalltarget</code>.</li> </ul> <p>This option enables you to configure different installation <code>.tar</code> packages and silent installation files for each computer.</p> <p>In the hosts file, list each hostname on a new line, for example:</p> <pre>labuws202::/agt/ua-usr.ini::/agt/UnixClient-linux.tar</pre> <p>where:</p> <ul style="list-style-type: none"> <li>♦ <code>labuws202</code> is the name of the computer where you want to install the AppManager UNIX agent</li> <li>♦ <code>/agt/ua-usr.ini</code> is the file path to the silent installation file</li> <li>♦ <code>/agt/UnixClient-linux.tar</code> is the directory path to the agent installation package. The naming convention for the <code>.tar</code> files is explained in the help for the previous parameter.</li> </ul> <p><b>TIP:</b> To comment out a line in the hosts file, use a <code>#</code> character. The hosts file should list any file locations of <code>.tar</code> files before it lists locations of <code>.ini</code> files. See <a href="#">Section 6.2.1, “Running this Knowledge Script,” on page 182</a>, above, for more information.</p> <ul style="list-style-type: none"> <li>♦ Specifying a comma-separated list of UNIX computers. If you use a list of computers instead of using a hosts file, you must also configure this Knowledge Script to specify the name and location of the silent installation file and the installation tar package. All the computers in the list must be installed using the same installation <code>.tar</code> package and silent installation file.</li> </ul> <p>This Knowledge Script attempts to install the AppManager UNIX agent on the first computer in the list. If an error occurs, or when the installation completes, the Knowledge Script attempts to install the AppManager UNIX agent on the next computer in the list.</p> <p><b>Tip</b> To use this Knowledge Script to install the AppManager UNIX agent on multiple remote UNIX or Linux computers, all of the target computers must be using the same root password.</p>
<b>Installation without Hosts File</b>	If you do not configure this Knowledge Script to use a hosts file, you must specify where the AppManager UNIX agent installation tar package and the silent installation file are located.
Directory path to agent installation <code>.tar</code> package(s)	<p>If you have configured this Knowledge Script to use a hosts file, you do not need to configure this parameter.</p> <p>Enter the full path from the remote UNIX or Linux computer to the directory where the installation <code>.tar</code> package is located. For example:</p> <pre>/usr/local/agt</pre> <p>You do not need to specify the name of the installation tar package if the name of the installation tar package follows the naming convention. If the name of the file does not follow the naming convention, you must specify the path and filename.</p>

Description	How to Set It
Name of silent installation file	<p>If you have configured this Knowledge Script to use a hosts file, you do not need to configure this parameter.</p> <p>You do not need to configure this parameter if the name of the silent installation file follows the naming convention <b>and</b> the silent installation file is located in the same directory as the AppManager UNIX agent installation .tar package.</p> <p>If the name of the silent installation file does not follow the convention (but it is in the same directory as the installation package), enter the name of the silent installation file.</p> <p>If the silent installation file is not in the same directory as the installation .tar package, enter the directory path and name of the silent installation file. For example: /usr/local/agt/UnixClient-Linux.ini.</p>
<b>Installation Destination</b>	
<p>Specify a temporary directory on the remote computer to store a copy of installation files. Note that if AppManager UNIX agent communication is authenticated and encrypted (security level 2), this Knowledge Script does not copy the security key with the installation files. Make sure that the remote UNIX computer can access the key file according to the location specified in the silent installation file.</p>	
Temporary directory on the remote computer	<p>Specify the name of a temporary directory on the remote computer where you want to install the AppManager UNIX agent. This Knowledge Script copies the installation tar package and related files, such as the hosts file and the silent installation file to the temporary directory.</p> <p>Note that some operating systems have small /tmp directories, which can prevent this Knowledge Script from successfully copying the installation files and untarring the installation .tar package. For this reason, you can specify a directory other than /tmp.</p> <p>If the .tar file already exists in this directory, you see a failure the first time you run this Knowledge Script. See <a href="#">Section 6.2.1, “Running this Knowledge Script,” on page 182</a>, above, for more information.</p>
Installation command to run on the remote computer	<p>Type the full command to use to install the AppManager UNIX agent on the target computer.</p> <p>The default is <code>UnixClient/netiq_agent_install</code>.</p>
Event severity for internal failure	<p>Set the event severity level, from 1 to 40, to indicate the importance of an event if the maximum pool threshold is exceeded. The default is 5.</p>

## 6.3 AgentUpdate

Use this Knowledge Script to remotely update a 6.0.2 or 6.5 AppManager UNIX agent to version 8.1.0.11, and to update a module on the 8.1.0.11 agent computer. To use this Knowledge Script, the AppManager UNIX agent you want to update must run as **root**.

To update a version 7.5 AppManager UNIX agent to version 8.1.0.11, and to update modules on a version 8.1.0.11 NetIQ UNIX agent, use NetIQ UNIX Agent Manager. For more information, see the UNIX Agent Manager online help.

This Knowledge Script updates the AppManager UNIX agent and any modules on the computer separately. For example, if you have a managed client with the 6.5 version of the AppManager UNIX agent and AppManager for Apache management files, run this Knowledge Script to update the AppManager UNIX agent to version 7.0.1. After you update the agent, configure this Knowledge Script to update the AppManager for Apache module on that computer.

To update the AppManager UNIX agent and preserve the agent's existing configuration, you must set the `INHERITCFG` flag in the silent installation file to `y`. For more information, see [AgentUpdate](#).

This Knowledge Script does **not** change the user account under which the AppManager UNIX agent runs. To change the AppManager UNIX agent's account, you must manually run the installation script on the managed client computer.

This Knowledge Script is configured by default to raise an event when:

- ♦ The agent update completes successfully. In this case, the following event message is displayed: "Agent successfully upgraded to version *build\_number*."
- ♦ The update is in progress but was not completed within the expected 4-minute time period. In this case, the following event message is displayed: "Agent upgrade started. Run this job again to check the status of the upgrade and clean up temporary files." To verify that the update completed successfully, re-run this Knowledge Script on the managed UNIX client computer.

### 6.3.1 User Account Requirements for this Script

To run this Knowledge Script, the AppManager UNIX agent you want to upgrade must run as **root**. If the AppManager UNIX agent runs as a non-root user, you must run the interactive installation script on the local computer to upgrade the AppManager UNIX agent.

### 6.3.2 Resource Objects

A 6.0.2 or 6.5 AppManager UNIX agent or a module on a 7.0.1 (or earlier) AppManager UNIX agent.

### 6.3.3 Default Schedule

By default, this script is only run once for each computer.

### 6.3.4 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Raise event if the update succeeds? (y/n)	Set to <b>y</b> to raise an event indicating the upgrade was successful. If the upgrade fails for any reason, an event is generated regardless of how you set this parameter. The default is <b>y</b> .

Description	How to Set It
Type of installation package (d for directory, t for tar file)	<p>Type <b>d</b> if the installation files are uncompressed and located in a distribution directory. For example, type <b>d</b> if the installation files are located on a mounted CD drive or have been copied to a specific directory. Type <b>t</b> if the installation files are packaged in a tar file. The default is <b>d</b>.</p> <ul style="list-style-type: none"> <li>◆ If set to “d” for directory, the path you specify for the following parameter needs to point to the fully qualified path of the expanded tarball.</li> <li>◆ If set to “t” for tarball packaging, the path you specify for the following parameter needs to point to the fully qualified file name of the tarball, for example, <code>/home/appmanager/upgrdefiles/UnixClient-aix.tar</code> for an AIX upgrade, where “aix” is the operating system on the target computer.</li> </ul> <p><b>NOTE:</b> Using the <code>tar</code> file requires additional scratch space in the temporary directory you specify on the target computer.</p>
Full path to directory with UNIX agent .tar files	<p>Enter the full path to the AppManager UNIX agent installation .tar file or the extracted contents of the .tar file. Typically the installation package is located on an accessible distribution computer. If you are working with the extracted contents of more than one .tar file, to avoid overwriting installation files you should extract each .tar file into its own shared directory. If the type of installation package is:</p> <ul style="list-style-type: none"> <li>◆ a .tar file, specify the full path to the .tar file.</li> <li>◆ extracted contents of the .tar file, specify the directory where the <code>netiq_agent_install</code> script is located.</li> </ul>
Temporary working directory on the target computer	<p>Specify a directory on the target computer to use as a temporary work space for upgrading the AppManager UNIX agent.</p> <p>Because the upgrade process creates a backup of your previous installation and verifies the success of the upgrade before removing any temporary files, the file system must have at least 200 MB of disk space available.</p> <p>The default is <code>/tmp</code>.</p>
Full path to silent configuration file	<p>Enter the full directory path to the silent installation file you’d like to use for the update.</p> <p>The default is <code>/tmp/silent.ini</code>.</p>
Event severity when job aborts	<p>Set the event severity level, from 1 to 40, to indicate the importance of the event when the job failed to update the agent. The default is 10.</p>
Event severity when update fails	<p>Set the event severity level, from 1 to 40, to indicate the importance of an event when the agent was not successfully updated. The default is 10.</p>
Event severity when update succeeds	<p>Set the event severity level, from 1 to 40, to indicate the importance of the event when the agent has been successfully updated. The default is 20.</p>
Event severity for internal failure	<p>Set the event severity level, from 1 to 40, to indicate the importance of an event if the maximum pool threshold is exceeded. The default is 5.</p>

## 6.4 AgentUpdateSecurityLevel

Use this Knowledge Script to remotely update the agent security level on the managed UNIX computers in your site. When configuring the security level for the agent, keep in mind that all managed UNIX clients in an AppManager site must be configured to use the same security level.

Use this Knowledge Script to change the security level on the managed UNIX clients in your AppManager site either before or after you change the security level on the repository database. The new security level takes effect on the managed UNIX client as soon as the Knowledge Script completes.

Keep in mind that managed UNIX clients cannot communicate with the management server until the security level on the managed UNIX client and the repository database are the same. After you restart the management server to use the latest security settings in the repository, managed UNIX clients with the corresponding security level can resume communication with the management server, and the Operator Console displays a success event message for this Knowledge Script job.

For more information about implementing AppManager secure communication, see the *Administrator Guide*.

The following security levels are available:

- ♦ **0 - Cleartext -- no security** indicates that all communication between the agent and the management server is in cleartext and is not encrypted.
- ♦ **1 - Encryption -- medium security** indicates that all communication between the agent and the management server is encrypted but the agent does not authenticate the identity of the management server.
- ♦ **2 - Encryption and authentication -- highest security** indicates that the agent attempts to authenticate the identity of the management server before sending and receiving encrypted communication. This option is only applicable if you installed the agent with **Encryption and Authentication**.

**Tip** If you configured the agent at installation to use **Cleartext** or **Encryption** and you want to change the security level to **Encryption and authentication**, you must reinstall the agent or manually change the agent's configuration file.

### 6.4.1 Resource Objects

UNIX Server computers with the agent.

### 6.4.2 Default Schedule

By default, this Knowledge Script is only run once for each computer.


## 6.4.3 Setting Parameter Values

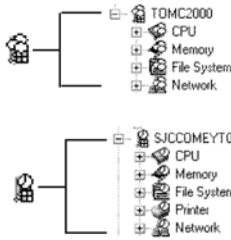
Set the following parameters as needed.

Description	How to Set It
Raise event when update succeeds or fails? (y/n)	<p>Set to y if you want AppManager to raise an event when the security level is successfully updated. This Knowledge Script always raises an event if the job does not run successfully.</p> <p>If enabled, you can configure the severity level of the event. The default is y.</p>
Event severity when update succeeds or fails	<p>Set the event severity level, from 1 to 40, to reflect the importance when the job successfully complete or when the job fails. The default is 5.</p>
Security level	<p>Select the security level you want the managed UNIX computer to use:</p> <ul style="list-style-type: none"><li>◆ <b>0 - Cleartext</b> if you want all communications between the agent and the management server to be in cleartext and is not encrypted. This option is best for closed network environments, testing, or troubleshooting communication issues.</li><li>◆ <b>1 - Encryption</b> if you want all communications between the agent and the management server to be encrypted.</li><li>◆ <b>2 - Encryption and authentication</b> if you want the management server to be authenticated before sending and receiving encrypted communication.</li></ul> <p>Keep in mind that, for a single repository, all managed UNIX clients must use the same security level setting. Any time you update security, you must do so for all of your UNIX agents. If you cannot update all of your UNIX agents at once, the management server cannot communicate with those agents and the interruption in communication might result in missing critical events or data. Therefore, you should plan any change to the security level carefully to minimize the chance of communication failures.</p> <p>The default is 0 - Cleartext.</p>

## 6.5 SchedMaint

Use this Knowledge Script to schedule a maintenance period for a specific application or for all resources on a managed client computer. During the maintenance period, regularly scheduled AppManager jobs do not run. You can specify the jobs you want to prevent from running by Knowledge Script category, or you can prevent all jobs from running on a server. For example, if you are planning routine maintenance on an Apache Server, you might want to block only the ApacheUNIX Knowledge Script jobs but if you are taking a computer offline to upgrade hardware or replace parts, you might want to prevent all jobs from running temporarily.

The maintenance icon , indicates that a computer is in unscheduled maintenance mode (machine maintenance mode) or that all resources on a computer are in scheduled maintenance mode (that is, all jobs are blocked). When you see this icon, AppManager has temporarily stopped monitoring the computer.



If **all jobs** for a computer are blocked, because of scheduled maintenance or because the computer has been selected for unscheduled maintenance, the maintenance icon is displayed for all resources.

If a **particular category** is blocked for scheduled maintenance, the schedule icon is displayed for all resources on the computer. Although the icon is displayed for all resources, only jobs for the specified category are blocked. You need to review the script properties to determine the specific server jobs that are blocked.

You define the start and end time for the scheduled maintenance period on the **Schedule** tab when you set the job properties. Jobs resume running on the managed computer when the maintenance period expires.

## 6.5.1 Resource Object

Any UNIX computer

## 6.5.2 Default Schedule

By default, this script set to run **Daily** for a managed computer. However, you should use AppManager’s scheduling capabilities found on the **Schedule** tab to set a schedule appropriate to your environment and maintenance needs. For more information about scheduling, see [Section 6.5.4, “Example of How this Script Is Used,” on page 192.](#)

## 6.5.3 Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
Knowledge Script category to block (for example, ORACLEUNIX)	Enter the Knowledge Script category for the jobs you do not want to run during a maintenance period (for example, NetBackupUNIX to block only NetBackupUNIX Knowledge Script jobs). You must specify the full category name, but the name is not case-sensitive. You can specify either a single category or an asterisk (*) for all jobs on a target computer. The default is all jobs (*).
Raise event if schedule successfully implemented? (y/n)	Set to <b>y</b> to raise an event indicating the success of the operation. The default is n.
Event severity when schedule successfully implemented	Set the event severity level, from 1 to 40, to reflect the importance of the event. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful operation. The default is 25.
Event severity when schedule implementation fails	Set the event severity level, from 1 to 40, to reflect the importance of the event. The default is 5.

## 6.5.4 Example of How this Script Is Used

In many environments, specific application servers have regularly scheduled periods when they are brought down by administrators so administrative tasks can be performed.

For example, an organization has have 20 Web servers that are shut once a month at 10 p.m. This interruption causes all of the AppManager jobs that are not explicitly stopped to error out and forces the administrator to restart the jobs manually when the servers are brought back online.

With this Knowledge Script, administrators can define a specific schedule for temporarily blocking jobs during a planned maintenance period.

For example, you can use the **Schedule** tab to define a monthly schedule that blocks jobs on the last weekend of each month during a two-hour window. Jobs that would normally run during this period, starting at 9:55 PM and ending at 11:55 PM are temporarily inactive. In this example, the actual maintenance period is short (just two hours once a month), but AppManager's scheduling capabilities provide enough flexibility for you to define a maintenance schedule that best meets your needs.

On the **Values** tab, you can identify a specific Knowledge Script category to block such as ApacheUNIX or you can use the default (\*) to block all of the jobs if the computers are going to be physically shut down. For example, to block all of the UNIX Knowledge Script jobs you might set the **Knowledge Script category to block** parameter to `Unix`.

At 9:55 PM local time (on the computer where the job is running), the maintenance period begins and all UNIX Knowledge Script jobs running on the target computers become inactive to allow for the scheduled maintenance. At 11:55 local time, the maintenance period expires and the jobs resume running at their regularly scheduled intervals.

## 6.6 SetPrimaryMS

Use this Knowledge Script to set or change the primary or secondary management server for version 8.1.0.11 or earlier UNIX agents, or to change the port number of the primary or secondary management server.

To change the management server designation for a version 7.5 UNIX agent, use NetIQ UNIX agent Manager. For more information, see the UNIX Agent Manager online Help.

This Knowledge Script allows you to explicitly designate a primary and a secondary management server and therefore explicitly control the communication between the managed UNIX clients and the management servers authorized to communicate with those managed clients. This Knowledge Script allows you to specifically assign a single primary management server for specified UNIX agents. Once you have identified a primary management server, the UNIX agent sends all information to that computer.

To help ensure communication is maintained even if the primary management server goes down, you can also use this Knowledge Script to explicitly designate a secondary or backup management server for the managed client. If the primary management server for the managed client fails, the backup management server takes over communication with the managed client until communication with the primary management server is restored.

If the target UNIX agent computer does not have the specified management server defined in the configuration file (`NqmComms.xml`), the agent adds it to the configuration file and then sets the flags according to the value you set for the **Select the management server operation to perform** parameter.



If you run the job from a management server computer, be aware that the job can only set a primary or backup management server when the specified management server is associated with the same repository. For example, Management Server A for Repository 1 cannot specify that Management Server B for Repository 2 should now become the primary or backup management server for Repository 1.

---

**NOTE:** When you install the UNIX agent, you implicitly establish a primary management server and can use this Knowledge Script to change the primary management server or designate a secondary management server. We recommend, however, that you explicitly designate the primary and secondary management servers by running this Knowledge Script twice.

The first time you run the job, you should identify the primary management server. After you receive notification that setting the management server has been successful, you can run the script a second time to set the secondary management server. You can also use this Knowledge Script to remove a management server for a target UNIX agent.

---

## 6.6.1 Resource Object

UNIX computer icon

## 6.6.2 Default Schedule

By default, this script is **only run once for each computer**.

## 6.6.3 Setting Parameter Values

Set the following parameters as needed:

---

Description	How to Set It
Event if job succeeds? (y/n)	Set to <b>y</b> to raise events that indicate whether the management server configuration succeeded. The default is <b>y</b> .
Event if job fails? (y/n)	Set to <b>y</b> to raise events that indicate whether the management server configuration was not successful. When this parameter is enabled, a failure in the configuration of the management server raises a severe event. The default is <b>y</b> .
Management server hostname or IP address	Enter the name or IP address of the management server you want to set as a primary or secondary management server or that you want to remove for a UNIX agent.  Keep in mind that you should set the primary management server first, then rerun this script to set the secondary management server or to make any changes to either the primary or secondary management server.  <b>NOTE:</b> Although you can specify the management server by hostname or IP address, based on how you have your site configured, the event detail message always identifies the computer by IP address.

---

Description	How to Set It
Management server operation to perform	<p>Select the appropriate option for the management server you have specified.</p> <ul style="list-style-type: none"> <li>◆ <b>Set primary management server</b> to change the primary management server</li> <li>◆ <b>Set secondary management server</b> to change the backup management server</li> <li>◆ <b>Unset management server</b> to remove the specified management server as a valid management server for the target computer</li> </ul> <p><b>NOTE:</b> If the target computer does not have the specified management server defined in its configuration file (<code>NqmComms.xml</code>), the UNIX agent adds it to the configuration file and then sets the flags according to the value you set here.</p> <p>The default is Set primary.</p>
Port number for the management server	<p>Type the port number you want to use on the management server for communications from UNIX agents. The port number should be the same port you specified when you installed the management server or the port number you have set for the <code>UNIX port</code> in the management server registry.</p> <p><b>NOTE:</b> If you have changed the port number for UNIX agents in the management server registry, run this script to set the new port number on your UNIX agents, then restart the management server to restore communication.</p> <p>The default is 9001.</p>
Event severity when job succeeds	<p>Set the event severity level, from 1 to 40, to indicate the importance of the event when setting the management server succeeds. The default severity level is 25.</p>
Event severity when job fails	<p>Set the event severity level, from 1 to 40, to indicate the importance of the event when setting the management server fails. The default severity level is 5.</p>

## 6.6.4 Example of How this Script Is Used

When you establish a primary management server for a managed client, that management server becomes the only management server that the managed client communicates with for a single repository/management server configuration. A secondary or backup management server can also be defined for each managed client in case the primary management server fails. The secondary management server only communicates with the managed client when the primary management server is unavailable. When communication with the primary management server resumes, the managed client resumes exclusive communication with the primary management server.

Because a multiple management server environment is chiefly intended for failover functionality (to provide an alternative management server if the primary management server fails), each managed client can have one primary management server and one backup management server for each repository.

# 7 Counter Reference

AppManager for UNIX provides the following UNIX\_Counter\_Reference Knowledge Scripts. Keep in mind that you need to specify object and counter names exactly as they are listed, including using the appropriate case and any spaces, as indicated.

Some counters require you to specify an instance name as well as the object and counter. In most cases, if a counter requires an instance name, you can specify the specific instance—for example, a specific CPU, such as 0, or a device name, or `_Total` for all instances—in the GeneralCounter Knowledge Script. Counters that only support `_Total` as the instance do not require you to explicitly specify `_Total` when setting the parameters for the GeneralCounter Knowledge Script. For more information about specifying instances, see [Specifying Instances](#).

---

**NOTE:** Although many objects and counters can apply to any server, not all counters are available for all types of UNIX and Linux servers.

---

## 7.1 Specifying Instances

Some performance information is linked to a specific instance, such as a specific device name or CPU number, while other performance information applies generally to a computer or reflects an overall or average value. Therefore, some performance counters have instances and some performance counters do not.

For counters that do not have instances, you can leave the instance portion of the parameter out or you can specify `_Total` as the instance. For counters that do rely on instance information, you should specify a particular instance or `_Total` to return information for all instances.

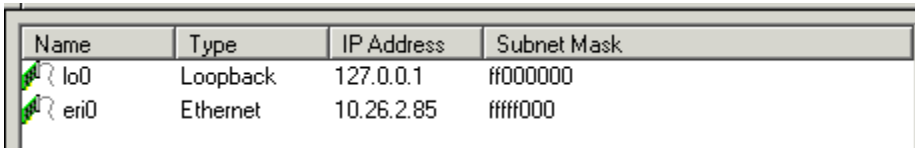
In general, if you need to specify an instance, use the following guidelines.

---

Instance	Value
CPU	CPU number. For example: 0, 1, 2
Physical disk	Device name. For example: dad0
Network	Interface name. For example: eri0
Printer	Printer name. For example: lp01

---

You can view instance names for any computer's system resources in the Operator Console by selecting an object icon in the TreeView pane, then clicking the **Details** tab in the List pane. The following is an example showing details for the Network Interface object:



Name	Type	IP Address	Subnet Mask
lo0	Loopback	127.0.0.1	ff000000
eri0	Ethernet	10.26.2.85	ffff0000

## 7.2 UX Processor

The `UX Processor` object provides counters for monitoring the processor on UNIX systems.

For counters that accept a processor instance, an individual CPU identifier is an integer: 0, 1, 2, and so on. For example, to monitor the idle time percentage counter on CPU 3, type:

```
UX Processor|Idle Time|3
```

To monitor a counter that does not accept a processor instance, such as the average blocked process queue length per second, use the `_Total` instance and type one of the following:

```
UX Processor|Block Queue Length/s|_Total
UX Processor|Block Queue Length/s
```

The following table describes the counters for the `UX Processor` object.

Counter Name	Description	Platforms
<code>%Utilization</code>	Percentage of time that the central processing unit is in use. On multi-processor systems, the percentage is averaged across all CPUs. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux HP-UX Solaris
<code>%System Time</code>	Percentage of time that the central processing unit is being used by system processes. On multiprocessor systems, the percentage is averaged across all CPUs. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux HP-UX Solaris
<code>%User Time</code>	Percentage of time that the central processing unit is being used by user processes. On multiprocessor systems, the percentage is averaged across all CPUs. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux HP-UX Solaris
<code>%Idle Time</code>	Percentage of time that the central processing unit is idle. On multiprocessor systems, the percentage is averaged across all CPUs. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux HP-UX Solaris
<code>%Wait Time</code>	Percentage of time that the central processing unit (CPU) is waiting. For example, the percentage of time processes are blocked and waiting for Input/Output to complete. On all operating systems, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX HP-UX Solaris

Counter Name	Description	Platforms
Context Switch/s	<p>Number of context switches per second. For Solaris and AIX, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For Linux and HP-UX, specify <code>_Total</code> as the instance.</p>	AIX Linux HP-UX Solaris
Interrupt/s	<p>Number of user or system interrupts per second. For Solaris and Linux, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For HP-UX, specify <code>_Total</code> as the instance.</p>	HP-UX Linux Solaris
System Call/s	<p>Number of system calls per second. For Solaris and AIX, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For HP-UX, specify <code>_Total</code> as the instance.</p>	AIX HP-UX Solaris
Trap/s	<p>Number of traps per second. For Solaris, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For HP-UX, specify <code>_Total</code> as the instance.</p>	HP-UX Solaris
Run Queue Length/s	<p>Average number of processes that are queued as ready to run per second. For HP-UX, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For Solaris, Linux, and AIX, specify <code>_Total</code> as the instance.</p>	AIX Linux HP-UX Solaris
Block Queue Length/s	<p>Average number of processes that are blocked and waiting for resources per second. For all platforms, specify <code>_Total</code> as the instance.</p>	Linux Solaris
Swap-out Queue Length/s	<p>Number of processes that are ready to run, but currently swapped out. For all platforms, specify <code>_Total</code> as the instance.</p>	AIX Linux HP-UX Solaris

## 7.3 UX Virtual Memory

The `UX Virtual Memory` object provides counters for monitoring the virtual memory usage on UNIX systems.

For counters that accept a processor instance, an individual CPU identifier is an integer: 0, 1, 2, and so on. For example, to monitor the total amount of swap space on your disk for CPU 1 on an HP-UX computer, type:

```
UX Virtual Memory|Avail Swap|1
```

To monitor a counter that does not accept a processor instance, such as the total free memory in KB, use the `_Total` instance and type one of the following:

```
UX Virtual Memory|Free List|_Total
UX Virtual Memory|Free List
```

The following table describes the counters for the `UX Virtual Memory` object.

Counter Name	Description	Platforms
Avail Swap	Total amount of swap space available on your hard disk. For HP-UX, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual CPU identifier</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> For Solaris, Linux, and AIX, specify <code>_Total</code> as the instance.	AIX Linux HP-UX Solaris
Buffers	Size of memory used by system buffers in KB. Specify <code>_Total</code> as the instance.	Linux
Cached	Size of memory being cached in KB. Specify <code>_Total</code> as the instance.	Linux
Free List	Total amount of free memory in KB. Specify <code>_Total</code> as the instance.	AIX HP-UX Solaris
Page Reclaims	Number of page reclaims per second. Specify <code>_Total</code> as the instance.	AIX HP-UX Solaris
Page Freed	Number of pages freed per second. Specify <code>_Total</code> as the instance.	HP-UX Solaris
Memory Free	Memory available on the heap in KB. Specify <code>_Total</code> as the instance.	Linux HP-UX
Memory Shared	Size of shared memory in KB. Specify <code>_Total</code> as the instance.	Linux
Minor Faults	Number of minor page faults per second. Minor page faults occur when the CPU cannot find memory because it is swapped out and must be swapped in again. Specify <code>_Total</code> as the instance.	Solaris
Total Reclaims	Total number of reclaims since the computer was last booted up. Specify <code>_Total</code> as the instance.	AIX HP-UX Solaris

Counter Name	Description	Platforms
Reclaims From Free List	Number of reclaims from free list per second. Specify <code>_Total</code> as the instance.	HP-UX Solaris
Zero Fill Page Faults	Number of zero fill page faults on demand per second. Specify <code>_Total</code> as the instance.	AIX HP-UX Solaris
Page Faults	Number of page faults (of all kinds) per second. Specify <code>_Total</code> as the instance.	AIX

## 7.4 UX Disk

The `UX Disk` object provides counters for monitoring the physical disk activity on UNIX systems. On Solaris, the `_Total` instance includes `cdrom` in calculating counter values.

For counters that accept a disk instance, physical disk names for a computer are available in the Operator Console. For example, to monitor the percentage of time fixed disk 1 (device `fd1`) is busy reading or writing, type:

```
UX Disk|%Time Disk Busy|fd1
```

To monitor a counter for all disks instead of a particular disk, such as the average number of KBs written per second, use the `_Total` instance and type:

```
UX Disk|Kilobytes Write/s|_Total
```

The following table describes the counters for the `UX Disk` object.

Counter Name	Description	Platforms
Kilobytes Read/s	Average number of kilobytes transferred from the disk per second during read operations. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux Solaris
Kilobytes Write/s	Average number of kilobytes transferred to the disk per second during write operations. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX Linux Solaris
Average Wait Service Time/ms	Average amount of time in milliseconds that disk requests are waiting. For either platform, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX Solaris
Average Run Service Time/ms	Average amount of time in milliseconds that disk operations are occurring. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX Linux Solaris

Counter Name	Description	Platforms
Average Service Time/ ms	Average amount of time in milliseconds for a disk operation to complete. This counter represents the sum of the wait time and the run time. For either platform, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX Solaris
Average # of Trans. Waiting	Average number of transfers waiting to occur. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX
%Time Trans. Waiting	Percentage of time that a transfer is waiting to occur. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX
%Time Disk Busy	Percentage of time that the disk is physically reading or writing. For either platform, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a physical disk name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX HP-UX

## 7.5 UX Swapping

The `UX Swapping` object provides counters for monitoring the swap activity on UNIX systems.

These counters do not accept individual instances; all counters use the `_Total` instance. For example, to monitor the number of swap-out requests per second, type one of the following:

```
UX Swapping|Swap out Request/s|_Total
UX Swapping|Swap out Request/s
```

The following table describes the counters for the `UX Swapping` object.

Counter Name	Description	Platforms
Swap in Request/s	Number of swap-in requests per second. For either platform, specify <code>_Total</code> as the instance.	HP-UX Solaris
Swap out Request/s	Number of swap-out requests per second. For either platform, specify <code>_Total</code> as the instance.	HP-UX Solaris
Swap in KBytes/s	Number of KBs swapped-in per second. For all platforms, specify <code>_Total</code> as the instance.	HP-UX Linux Solaris
Swap out KBytes/s	Number of KBs swapped-out per second. For all platforms, specify <code>_Total</code> as the instance.	HP-UX Linux Solaris



## 7.6 UX Paging

The `UX Paging` object provides counters for monitoring the paging activity on UNIX systems.

These counters do not accept individual instances; all counter use the `_Total` instance. For example, to monitor the number of pages scanned per second, type one of the following:

```
UX Paging|Scanned Pages/s|_Total
UX Paging|Scanned Pages/s
```

The following table describes the counters for the `UX Paging` object.

Counter Name	Description	Platforms
Page-out Requests/s	Number of page-out requests per second. For all platforms, specify <code>_Total</code> as the instance.	AIX HP-UX Solaris
Page-out KBytes/s	Number of KBs paged-out per second. For all platforms, specify <code>_Total</code> as the instance.	AIX HP-UX Linux Solaris
Page-in Requests/s	Number of page-in requests per second. For all platforms, specify <code>_Total</code> as the instance.	AIX HP-UX Solaris
Page-in KBytes/s	Number of KBs paged-in per second. For all platforms, specify <code>_Total</code> as the instance.	AIX HP-UX Linux Solaris
Scanned Pages/s	Number of pages scanned per second. For both platforms, specify <code>_Total</code> as the instance.	AIX Solaris
Page Faults on Copy-on-Write/s	Number of page faults per second caused by copy-on-write operations. Specify <code>_Total</code> as the instance.	Solaris
Page Faults on Address Translation/s	Number of page faults per second caused by address translations. Specify <code>_Total</code> as the instance.	Solaris
Page Faults on Software Lock/s	Number of page faults per second caused by software locks. Specify <code>_Total</code> as the instance.	Solaris

## 7.7 UX Block IO

The `UX Block IO` object provides counters for monitoring the processing activity on UNIX systems.

For counters that accept a block IO device instance, block IO device names are available in the Operator Console. For example, to monitor the average number of kilobytes read per second from the block IO device `scanner`, type:

```
UX Block IO|Kilobytes Read/s|scanner
```

To monitor a counter for all block IO devices instead of a particular device, such as average number of transfer operations waiting, type:

```
UX Block IO|Average # of Trans. Waiting|_Total
```

The following table describes the counters for the `UX Block IO` object.

Counter Name	Description	Platforms
Reads/s	Number of read operations per second. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX Linux Solaris
Writes/s	Number of write operations per second. For all platforms, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a blockIO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX Linux Solaris
Kilobytes Read/s	Average number of kilobytes transferred from the disk per second during read operations. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX
Kilobytes Write/s	Average number of kilobytes transferred from the disk per second during write operations. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	HP-UX
Average # of Trans. Waiting	Average number of disk transfer operations that are waiting. For either platform, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	Linux Solaris
Average # of Trans. Serviced	Average number of disk transfer operations that are serviced. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	Solaris
%Time Trans. Waiting	Percentage of time that input/output transfers are waiting. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	Solaris
%Time Disk Busy	Percentage of time that the disk is busy with read or write operations. For either platform, specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a block IO device name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	Linux Solaris

## 7.8 UX Networking

The `UX Networking` object provides counters for monitoring the network activity on UNIX systems.

For counters that accept a network interface instance, network interface names are available in the Operator Console. For example, to monitor the percentage of data transmission collisions for ethernet adapter 0 (`eth0`), type:

```
UX Networking|%Collision|eth0
```

To monitor a counter for all network interfaces instead of a particular interface, such as the number of input packets received per second, use the `_Total` instance and type:

```
UX Networking|Input Packets|_Total
```

The following table describes the counters for the `UX Networking` object.

---

**NOTE:** On Solaris computers, the UNIX agent must run as root to collect the UX Networking counters.

---

Counter Name	Description	Platforms
<code>%Input Error</code>	<p>Percentage of packets with input errors. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
<code>%Output Error</code>	<p>Percentage of packets with network output errors. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
<code>%Collision</code>	<p>Percentage of network data-transmission collisions detected. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	HP-UX Linux Solaris

Counter Name	Description	Platforms
%Send-Q Busy	<p>Number of non-empty Send-Q connections divided by the total number of TCP connections. A high value indicates traffic congestion. Setting up subnets can help reduce the congestion.</p> <p>Specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	Solaris
Input Packets	<p>Number of network input packets received per second. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
Input Error	<p>Number of network input errors per second. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
IP Errors	<p>Number of network IP errors per second. For AIX, Linux, and Solaris, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For HP-UX, specify <code>_Total</code> as the instance.</p> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
Output Packets	<p>Number of network output packets sent per second. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris
Output Error	<p>Number of network output errors per second. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	AIX HP-UX Linux Solaris

Counter Name	Description	Platforms
Collision	<p>Number of network collisions per second. For all platforms, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p><b>NOTE:</b> This parameter returns incorrect data on computers running the Solaris 11 operating system in a zone that is not a global zone.</p>	HP-UX Linux Solaris
TCP Connections	<p>Number of TCP network connections. For Solaris, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For Linux, HP-UX and AIX, specify <code>_Total</code> as the instance.</p>	AIX HP-UX Linux Solaris
Established Connections	<p>Number of network connections established per second. For Solaris, specify one of the following as the instance:</p> <ul style="list-style-type: none"> <li>◆ an individual network interface name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul> <p>For Linux, HP-UX and AIX, specify <code>_Total</code> as the instance.</p>	AIX HP-UX Linux Solaris

## 7.9 UX NFS

The `UX NFS` object provides counters for monitoring file system activity on AIX systems.

These counters do not accept individual instances; all counters use the `_Total` instance. For example, to monitor the number of NFS calls from clients rejected by the NFS server, type one of the following:

```
UX NFS|Server NFS Badcalls|_Total
UX NFS|Server NFS Badcalls
```

The following table describes the counters for the `UX NFS` object.

Counter Name	Description	Platforms
Server RPC Calls	Number of RPC calls from clients. Specify <code>_Total</code> as the instance.	AIX
Server RPC Dupchecks	Number of RPC calls from clients that caused a check for duplicates in the pending request cache. NFS performs duplicate checks for requests that produce a different result when performed more than once, such as close file or remove file. Specify <code>_Total</code> as the instance.	AIX
Server NFS Calls	Number of NFS calls from clients. Specify <code>_Total</code> as the instance.	AIX
Server NFS Badcalls	Number of NFS calls from clients rejected by the server. Specify <code>_Total</code> as the instance.	AIX
Client RPC Calls	Number of client RPC calls. Specify <code>_Total</code> as the instance.	AIX
Client RPC Timeouts	Number of times a client RPC call timed-out while waiting for a server reply. Specify <code>_Total</code> as the instance.	AIX

Counter Name	Description	Platforms
Client RPC Badcalls	Number of client RPC calls rejected by the RPC layer. Specify <code>_Total</code> as the instance.	AIX
Client NFS Calls	Number of client calls made to NFS. Specify <code>_Total</code> as the instance.	AIX
Client NFS Badcalls	Number of client calls made to NFS that were rejected by the NFS server. Specify <code>_Total</code> as the instance.	AIX

## 7.10 UX File Access System

The `UX File Access System` object provides counters for monitoring file system activity on AIX systems.

These counters do not accept individual instances, all counters use the `_Total` instance. For example, to monitor the number of write operations per second to raw character devices, type one of the following:

```
UX File Access System|Pwrite/s|_Total
UX File Access System|Pwrite/s
```

The following table describes the counters for the `UX File Access System` object.

Counter Name	Description	Platforms
Iget/s	Number of calls per second to i-node lookup routines. Specify <code>_Total</code> as the instance.	AIX
Namei/s	Number of calls per second to find a v-node address given a path name. Specify <code>_Total</code> as the instance.	AIX
Bread/s	Number of block IO read operations per second. Specify <code>_Total</code> as the instance.	AIX
Bwrite/s	Number of block IO write operations per second. Specify <code>_Total</code> as the instance.	AIX
Lread/s	Number of logical IO read operations per second. Specify <code>_Total</code> as the instance.	AIX
Lwrite/s	Number of logical IO write operations per second. Specify <code>_Total</code> as the instance.	AIX
Pread/s	Number of read operations per second from raw character devices. Specify <code>_Total</code> as the instance.	AIX
Pwrite/s	Number of write operations per second to raw character devices. Specify <code>_Total</code> as the instance.	AIX
Character Read/s	Number of characters read per second by system calls. Specify <code>_Total</code> as the instance.	AIX
Character Written/s	Number of characters written per second by system calls. Specify <code>_Total</code> as the instance.	AIX

## 7.11 UX Terminal IO

The `UX Terminal IO` object provides counters for monitoring terminal input/output activity on IBM AIX v4.3.3 systems.

---

**NOTE:** These counter objects are not supported on IBM AIX 5L v5.1 and v5.2.

---

These counters do not support individual instances; all counters use the `_Total` instance. For example, to monitor the number of raw input characters per second, type one of the following:

```
UX Terminal IO|Raw Input Char/s|_Total
UX Terminal IO|Raw Input Char/s
```

The following table describes the counters for the `UX Terminal IO` object.

Counter name	Description	Platforms
Raw Input Char/s	Number of TTY input characters queued per second. Specify <code>_Total</code> as the instance.	AIX v4.3.3 only
Can Input Char/s	Number of TTY canonical input characters queued per second. Specify <code>_Total</code> as the instance.	AIX v4.3.3 only
Output Char/s	Number of TTY output characters queued per second. Specify <code>_Total</code> as the instance.	AIX v4.3.3 only

## 7.12 UX System Calls

The `UX System Calls` object provides counters for monitoring system calls on AIX systems.

For counters that accept a processor instance, an individual CPU identifier is an integer: 0, 1, 2, and so on. For example, to monitor the number of system exec calls per second counter on CPU 0, type:

```
UX System Calls|Exec Calls/s|0
```

To monitor a counter system wide, such as the number of fork system calls per second, use the `_Total` instance and type:

```
UX System Calls|Fork Calls/s|_Total
```

The following table describes the counter for the `UX System Calls` object.

Counter name	Description	Platforms
Total Calls/s	Number of system calls per second. Specify one of the following as the instance: <ul style="list-style-type: none"><li>◆ a processor number</li><li>◆ <code>_Total</code> (for all instances).</li></ul>	AIX
Read Calls/s	Number of read system calls per second. Specify one of the following as the instance: <ul style="list-style-type: none"><li>◆ a processor number</li><li>◆ <code>_Total</code> (for all instances).</li></ul>	AIX

Counter name	Description	Platforms
Write Calls/s	Number of write system calls per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a processor number</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX
Fork Calls/s	Number of fork system calls per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a processor number</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX
Exec Calls/s	Number of exec system calls per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ a processor number</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX

## 7.13 UX Processes

The `UX Processes` object provides counters for monitoring processes on AIX systems.

For counters that accept a process instance, use the process identifier (PID). For example, to monitor the private bytes used by a process whose PID is 3517, type:

```
UX Processes|Process Private Bytes|3517
```

To monitor a counter for all processes, such as the percentage of CPU utilization by all processes executing code in the user space, use the `_Total` instance and type:

```
UX Processes|% User CPU Time|_Total
```

The following table describes the counters for the `UX Processes` object.

Counter Name	Description	Platform
Process Image Size	Process image size in KB. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX
Process Private Bytes	Number of non-shared private memory bytes. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX
Nice Value	Nice value for processor resource allocation. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ <code>_Total</code> (for all instances).</li> </ul>	AIX



Counter Name	Description	Platform
% Process CPU Utilization	Percentage of CPU utilization. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
% System CPU Time	Percentage of time CPU was executing code in kernel space. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
% User CPU Time	Percentage of time CPU was executing code in the user space. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
Process Elapse Time	Time taken from the start to the end of the process. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
Process Minor Page Faults/s	Number of process minor page faults per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
Process Major Page Faults/s	Number of process major page faults per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX
Process Signals Received/s	Number of process signals received per second. Specify one of the following as the instance: <ul style="list-style-type: none"> <li>◆ an individual instance name</li> <li>◆ _Total (for all instances).</li> </ul>	AIX



# 8

## Reporting with Reporting Center

Reporting Center allows you to extract data from the databases of other NetIQ products and present the information as charts and tables in customizable reports. Reporting Center transforms the data into useful reports about the computing infrastructure that supports your business.

AppManager for UNIX ships with a package of Reporting Center reports templates. You can use a report template to retrieve data from multiple data sources and generate a consolidated report from the Control Center Database. You can set report contexts that are defined for each report, such as data source connections, report types, time frame, and server selections. The report template allows you to compare data collected from multiple data sources and displays the information in the Reporting Center Console. You can also generate historical data using the reports templates for the UNIX.

You can find these reports templates inside the **Reporting Center Home > Templates > AppManager Templates > AppManager For UNIX Reports** folder in the Reporting Center Navigation pane.

For more information about the Reporting Center and working with the reports, see the [Operations Center Dashboard Guide](#).

### 8.1 System Requirements for the UNIX Reports

UNIX reports for Reporting Center have the following system requirements:

- ♦ Reporting Center for AppManager 2.2 or later
- ♦ AppManager for UNIX and Linux Servers 7.8 or later

### 8.2 Installing the UNIX reports on Reporting Center

You can install the UNIX reports to either local or remote databases. You need to install the reports only once per database.

**To install the UNIX reports:**

- 1 `AM70-UNIX-7.x.x.0.msi` module installer from the `AM70_UNIX_7.x.x.0` self-extracting installation package.
- 2 From the Knowledge Script and Report Package Installation Options page of the installation wizard, select Install report package and click Next.
- 3 In the **SQL Server name\instance** field, specify the name of the SQL Server hosting the Reporting Center database.
- 4 In the **NetIQ Reporting Center database name** field, type the name of the Reporting Center database.
- 5 Select either Windows or SQL Server authentication and click Next. If you select SQL Server authentication, specify the user name and the password of the SQL Server service account of the Reporting Center database to which you want to connect.
- 6 When the installer finishes, launch the Reporting Center console.

## 8.3 UNIX Report Templates

AppManager for UNIX consists of the following reports templates:

Template	Description
Machine by CPUload	This report is based on the data streams generated by the SmartCPUload Knowledge Script. The report displays the Processor Utilization for the selected servers.
Machine by DiskLoad	This report is based on the data streams generated by the SmartPhysicalDiskStats Knowledge Script. The report displays Diskload, throughput per sec, and throughput KBs per sec for the selected servers.
Machine by FileSystemUsage	This report is based on the data streams generated by the DynamicFileSystemSpace Knowledge Script. The report displays the percentage of logical disk space used by the specified machine(s) and the percentage of logical disk space available for the specified machine(s).
Machine by NetworkLoad	This report is based on the data streams generated by the NetInterfacesIO Knowledge Script. The report displays the throughput per sec, bytes sent per sec, and bytes received per sec for the selected server.