NetIQ® AppManager® for Hardware

Management Guide

December 2018

Legal Notice

Contents

About this Book and the Library 5

About NetIQ Corporation 7

1 Introducing AppManager for Hardware 9

Features and Benefits 9
About AppManager and Cisco UCS Servers 9
About AppManager and Dell Servers 10
About AppManager and HP Servers 10
About AppManager and IBM Servers 10
About AppManager and EMC Servers 11
About AppManager and NetApp Servers 11
Counting AppManager Licenses 11

2 Installing AppManager for Hardware 13

System Requirements 13
Scalability Considerations 15
Installing the Module 16
Deploying the Module with Control Center 18
Silently Installing the Module 18
Configuring the SMI-S Provider 19
Configuring Security Manager 23
Discovering Hardware Resources. 25

3 Hardware Knowledge Scripts 27

Understanding Hardware Resource States 28
Specifying Inclusion or Exclusion Filters 29
Using Regular Expression Filters 30
Metric Availability of Storage Knowledge Scripts 32
BatteryHealth 33
FanHealth 36
LogicalDriveHealth 39
MemoryHealth 42
NICHealth 44
PhysicalDriveHealth 47
PowerSupplyHealth 50
ProcessorHealth 52
SmartArrayControllerHealth 55
StorageBoxHealth 58
TemperatureHealth 61
VoltageHealth 63
LogicalDiskDataTransfer 66
LogicalDiskIO 69
LogicalDiskResponseTime 72
LogicalDiskUtilization 75
PhysicalDiskDataTransfer 78

PhysicalDiskIO 80
PhysicalDiskResponseTime 83
StorageArrayUtilization 86

4 Troubleshooting AppManager for Hardware 91

AppManager agent and SAN device are not responding 91

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 for Hardware 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.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ web site 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. You can also email 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 http://community.netiq.com.

1 Introducing AppManager for Hardware

AppManager for Hardware allows you to use a single set of Knowledge Scripts to monitor the hardware resources on VMware ESX or ESXi servers running on Cisco UCS, Dell, HP, or IBM systems. You can also monitor the storages running on EMC, NetApp, HP, and Dell systems.

AppManager for Hardware enables you to monitor server and disk availability. In addition to providing support and optimizing performance, this module ensures availability of hardware resources through automated event detection and collects data for analysis.

Features and Benefits

AppManager for Hardware provides the following features and benefits:

- Monitors hardware resources from multiple vendors using a single set of Knowledge Scripts.
- Monitors multiple servers with a single set of credentials.
- Monitors the EMC, NetApp, HP, and Dell storages.
- Allows you to choose the hardware resources to monitor on specific servers to simplify monitoring.
- Remotely monitors hardware resources through proxy agents, and monitors multiple servers with different versions of the hardware monitoring agent for that vendor.
- Automatically determines the hardware vendor during the discovery process.

About AppManager and Cisco UCS Servers

AppManager for Hardware monitors the following hardware resources on Cisco UCS B-Series Blade Servers and C-Series Rack Servers:

- CPU
- Fan (applicable only to C-Series Rack Server)
- Logical drives in an array
- Memory
- Network interface controller (NIC)
- Physical drives in an array
- Power supply (applicable only to C-Series Rack Server)
- RAID controller
- Temperature
- Voltage

NOTE: If battery is available on the Cisco UCS server, AppManager discovers it. To monitor the operational status of the battery, run the BatteryHealth Knowledge Script.

About AppManager and Dell Servers

AppManager for Hardware monitors the following hardware resources on Dell servers:

- Battery (CMOS only)
- CPU
- Fan
- Logical drives in an array
- Memory
- Network interface controller (NIC)
- Physical drives in an array
- Power supply
- RAID controller
- Temperature
- Voltage

About AppManager and HP Servers

AppManager for Hardware monitors the following hardware resources on HP servers:

- CPU
- Fan (status only)
- Logical drives in an array
- Memory
- Network interface controller (NIC)
- Physical drives in an array
- Power supply
- RAID controller
- Storage box
- Temperature

About AppManager and IBM Servers

AppManager for Hardware monitors the following hardware resources on IBM servers:

- Battery
- CPU
- Fan
- Logical drives in an array
- Memory
- Network interface controller (NIC)
- Physical drives in an array
- Power supply

- RAID controller
- Temperature
- Voltage

About AppManager and EMC Servers

AppManager for Hardware monitors the following hardware resources on EMC servers:

- Battery
- Storage processor
- Fan
- Power Supply
- Array physical disk
- Array logical disk
- Smart array controller

About AppManager and NetApp Servers

AppManager for Hardware monitors the following hardware resources on NetApp servers:

- Battery
- Array physical disks
- Flex volumes (includes LUN)

Counting AppManager Licenses

AppManager for Hardware consumes one license for each discovered ESX or ESXi server. For example, if you are monitoring ten ESX or ESXi servers from one computer that has AppManager for Hardware installed on it, you need ten AppManager licenses.

2 Installing AppManager for Hardware

This chapter provides installation instructions and describes system requirements for AppManager for Hardware.

The chapter assumes you have AppManager 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.

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 Hardware has the following system requirements:

Software	Version
NetIQ AppManager installed on the AppManager repository (QDB) computer, on all proxy agent computers, and on all console computers	8.0.3, 8.2, 9.1, 9.2, 9.5, or later One of the following AppManager agents are required: ◆ AppManager agent 7.0.4 with hotfix 72616 or later ◆ AppManager agent 8.0.3, 8.2, 9.1, 9.2, 9.5, or later
Microsoft Windows operating system on the proxy agent computers	One of the following: ◆ Windows Server 2012 R2 ◆ Windows Server 2012 ◆ Windows 8 (32-bit or 64-bit) ◆ Windows 7 (32-bit or 64-bit) ◆ Windows Server 2008 R2 ◆ Windows Server 2008 (32-bit or 64-bit) ◆ Windows Server 2003 R2 (32-bit or 64-bit)
AppManager for Microsoft Windows module installed on the repository, proxy agent, and console computers	Support for Windows Server 2008 R2 on AppManager 7.*x* requires the AppManager for Windows module, version 7.6.170.0 or later. For more information, see the AppManager Module Upgrades & Trials page.

Software	Version
VMware hypervisor and the software required for monitoring the hardware resources on the hypervisor	One of the following: ◆ ESXi 6.0 ◆ Monitoring Cisco UCS mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring Dell mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring HP resources require HPE ESXi Offline Bundle for VMware VSphere 6.0. ◆ Monitoring IBM mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ ESXi 5.1 ◆ Monitoring Cisco UCS mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring Dell mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring HP resources does not require additional software. ◆ Monitoring IBM mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ ESXi 5.0 ◆ Monitoring Cisco UCS mass storage resources requires LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring Dell resources requires Dell OpenManage Offline Bundle and VIB for ESXi. To monitor mass storage resources, also install LSI Logic MegaRAID VMware 5.x SMIS Provider VIB. ◆ Monitoring HP resources requires HP ESXi 5.0 Offline Bundle version 1.1 or later. ◆ Monitoring IBM resources requires VMware vSphere Hypervisor 5.0 with IBM Customization. ◆ ESX or ESXi 4.1 ◆ Monitoring HP resources requires HP ESXi Offline Bundle for VMware ESXi 4.1 U2. ◆ Monitoring IBM resources requires VMware vSphere Hypervisor 4.1 with IBM Customization. ◆ ESX or ESXi 4.0 ◆ Monitoring hardware resources does not require additional software.

Software	Version
SMI-S Providers for EMC, NetApp, HP (MSA and 3PAR), and Dell (MDI) storages	EMC SMI-S Provider version 4.6 and later. For more information about installing and configuring EMC SMI-S provider, see "Installing and Configuring the SMI-S Provider for EMC" on page 22. NetApp Data ONTAP SMI-S Agent 5.1 and later. For more information about installing and configuring Data ONTAP SMI-S provider, see "Installing and Configuring the Data ONTAP SMI-S Provider for NetApp Storages" on page 21 HP 3PAR SMI-S Provider version 2.9. For more information about installing and configuring HP SMI-S provider, see "Installing and Configuring the SMI-S Provider for HP" on page 22. HP MSA SNIA SMI-S Provider version 1.5.0. For more information about installing and configuring HP SMI-S provider, see "Installing and Configuring the SMI-S Provider for HP" on page 22. Dell SMI-S Provider version 10.30. For more information about installing and configuring Dell SMI-S provider, see "Installing and Configuring the SMI-S Provider for Dell" on page 23.
Microsoft Visual C++ Redistributable Package installed on all computers where you plan to install the module	Microsoft Visual C++ 2008 Service Pack 1 (32-bit) The module installer automatically installs the package.
CIMOM(CIM Server)	Ensure that the CIM Server is running on the ESX or ESXi server. By default, the CIM Server is configured to run on port 5989.
CIMOM(CIM Servers in SAN/NAS environments)	Ensure that the CIM Server is running where it is hosted. By default, the CIM Server is configured to run on ports 5988 (unsecured connection) and 5989 (secured connection) for EMC, NetApp, HP (MSA and 3PAR), and Dell (MDI).
Microsoft SQL Server Native Client 11.0 **(for TLS 1.2 support)**	11.3.6538.0 or later **NOTE:** The SQL Server Native client can be installed from this Microsoft download link.

If you encounter problems using this module with a later version of your application, contact NetIQ Technical Support.

NOTE: If you want TLS 1.2 support and are running AppManager 9.1 or 9.2, then you are required to perform some additional steps. To know about the steps, see the article.

Scalability Considerations

Consider the following recommendations before deploying AppManager for Hardware:

- When running this module on AppManager 8 or later, if you use the Delta Discovery feature in Control Center, NetIQ Corporation recommends that you schedule the discovery job to run in regular intervals of no less than an hour.
- If you want to monitor more than 50 hardware devices with the Hardware Knowledge Scripts, consider disabling agent logging.

To disable agent logging:

1. Navigate to the following location in the Registry Editor:
   - **On 32-bit OS:** `\SOFTWARE\NetIQ\AppManager\4.0\NetIQmc\Tracing`
   - **On 64-bit OS:** `\SOFTWARE\Wow6432Node\NetIQ\AppManager\4.0\NetIQmc\Tracing`
2. Ensure that `TraceKS` is set to 0.
3. Set `TraceMC` to 0.
4. (Conditional) If you are using AppManager 7.*x*, restart the NetIQmc service.

NOTE: If you do not disable these registries on the agent, every iteration for Hardware Knowledge Script jobs takes significantly longer to run compared to the amount of time the jobs would have taken if the registries were disabled.

- This module might create a high number of events and data points in environments having many hardware resources. If you monitor more than 50 hardware devices with multiple Knowledge Scripts, the number of data points and events might cause delays in other AppManager components. Specifically, the system process on the agent computer can consume high amounts of CPU during the job iteration. After the Hardware Knowledge Script jobs are completed, the CPU consumption reduces.
- Use monitoring policies to automatically update the monitoring jobs when changes in the environment, such as a new fan device, are discovered.

NOTE: A monitoring policy is applied on the agent and runs an AppManager job for each Knowledge Script in the Knowledge Script Group. A monitoring policy may apply to many objects, and in large environments the policy might not work for configuring AppManager. For assistance with configuring Knowledge Scripts and Knowledge Script Groups in a large environment, contact NetIQ Technical Support.

- The AppManager for Hardware module can collect a large amount of data and can raise many events, depending on the number of hardware devices you are monitoring. For assistance in setting up your AppManager management server cache files, contact NetIQ Technical Support.

Installing the Module

To monitor hardware resources on VMware ESX, ESXi or SAN/NAS storages, you must install the module on a Windows computer that serves as a proxy agent computer.

Run the module installer only once on any computer. The module installer automatically identifies and updates all relevant AppManager components on the computer.

Access the `AM70-Hardware-8.`*`1.x`*`.0.msi` module installer from the `AM70_Hardware_8.`*`1.x`*`.0` self-extracting installation package on the AppManager Module Upgrades & Trials page.

For Windows environments where User Account Control (UAC) is enabled, install the module using an account with administrative privileges. Use one of the following methods:

- Log in to the server using the account named Administrator. Then, run `AM70-Hardware-8.`*`1.x`*`.0.msi` from a command prompt or by double-clicking it.
- Log in to the server as a user with administrative privileges and run `AM70-Hardware-8.`*`1.x`*`.0.msi` as an administrator from a command prompt. To open a command-prompt window at the administrative level, right-click a command-prompt icon or a Windows menu item and select **Run as administrator**.

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

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

You can install the module manually, or you can use Control Center to deploy the module on a remote computer that has an agent installed. For more information, see "Deploying the Module with Control Center" on page 18. However, if you use Control Center to deploy the module, Control Center only installs the *agent* components of the module. The module installer installs the QDB and console components, and the agent components on the agent computer.

To install the module manually:

1 Double-click the module installer `.msi` file.

2 Accept the license agreement.

3 Review the results of the pre-installation check. You can expect one of the following three scenarios:

- **No AppManager agent is present:** In this scenario, the pre-installation check fails, and the installer does not install agent components.
- **An AppManager agent is present, but some other prerequisite fails:** In this scenario, the default is to not install agent components because of one or more missing prerequisites. However, you can override the default by selecting **Install agent component locally**. A missing application server for this particular module often causes this scenario. For example, installing the AppManager for Microsoft SharePoint module requires the presence of a Microsoft SharePoint server on the selected computer.
- **All prerequisites are met:** In this scenario, the installer installs the agent components.

4 To install the Knowledge Scripts into the QDB:

4a Select **Install Knowledge Scripts** to install the repository components, including the Knowledge Scripts, object types, and SQL stored procedures.

4b Specify the SQL Server name of the server hosting the QDB, and the case-sensitive QDB name.

NOTE: Microsoft .NET Framework 3.5 is required on the computer where you run the installation program for the QDB portion of the module. For computers running more recent versions of Windows operating systems that use a newer version of .NET, install .NET 3.5 with the Add Roles and Features wizard in Windows Server Manager, as described in this Microsoft article.

5 Run the module installer for each QDB attached to Control Center.

6 Run the module installer on all console computers to install the Help and console extensions.

7 Run the module installer on all proxy agent computers to install the agent components.

8 Configure AppManager Security Manager with the security information required to allow access to gather data for discovering hardware resources. For more information about configuring Security Manager, see "Configuring Security Manager" on page 23.

9 (Conditional) If you have not discovered Hardware resources, run the Discovery_Hardware Knowledge Script on all agent computers where you installed the module. For more information, see "Discovering Hardware Resources" on page 25.

After the installation has completed, the `Hardware_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<`*`ServerName`*`>` folder, lists any problems that occurred.

Deploying the Module with Control Center

You can use Control Center to deploy the module on a remote computer where an agent is installed. This topic briefly describes the steps involved in deploying a module and provides instructions for checking in the module installation package. For more information, see the *Control Center User Guide for AppManager*, which is available on the AppManager Documentation page.

Deployment Overview

This section describes the tasks required to deploy the module on an agent computer.

To deploy the module on an agent computer:

1. Verify the default deployment credentials.
2. Check in an installation package. For more information, see "Checking In the Installation Package" on page 18
3. Configure an e-mail address to receive notification of a deployment.
4. Create a deployment rule or modify an out-of-the-box deployment rule.
5. Approve the deployment task.
6. View the results.

Checking In the Installation Package

You must check in the installation package, `AM70-Hardware-8.x.x.0.xml`, before you can deploy the module on an agent computer.

To check in a module installation package:

1. Log on to Control Center using an account that is a member of a user group with deployment permissions.
2. Navigate to the **Deployment** tab (for AppManager 8.*x* or later) or **Administration** tab (for AppManager 7.*x*).
3. In the Deployment folder, select **Packages**.
4. On the Tasks pane, click **Check in Deployment Packages** (for AppManager 8.*x* or later) or **Check in Packages** (for AppManager 7.*x*).
5. Navigate to the folder where you saved `AM70-Hardware-8.x.x.0.xml` and select the file.
6. Click **Open**. The Deployment Package Check in Status dialog box displays the status of the package check in.

Silently Installing the Module

To silently (without user intervention) install the module using the default settings, run the following command from the folder in which you saved the module installer:

```
msiexec.exe /i "AM70-Hardware-8.1.x.0.msi" /qn
```

where *x.x* is the actual version number of the module installer.

To create a log file that describes the operations of the module installer, add the following flag to the command noted above:

```
/L* "AM70-Hardware-8.1.x.0.msi.log"
```

The log file is created in the folder in which you saved the module installer.

NOTE: To perform a silent install on an AppManager agent running Windows 2008 R2, open a command prompt at the administrative level and select **Run as administrator** before you run the silent install command listed above.

To silently install the module on a remote AppManager repository, you can use Windows authentication or SQL authentication.

Windows authentication:

```
AM70-Hardware-8.1.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_SQLSVR_WINAUTH=1
MO_SQLSVR_NAME=SQL_Server_Name MO_QDBNAME=AM-Repository Name
```

SQL authentication:

```
AM70-Hardware-8.1.x.0.msi /qn MO_B_QDBINSTALL=1 MO_B_SQLSVR_WINAUTH=0
MO_SQLSVR_USER=SQL login MO_SQLSVR_PWD=SQL Login Password MO_SQLSVR_NAME=SQL
Server Name MO_QDBNAME=AM-Repository Name
```

Configuring the SMI-S Provider

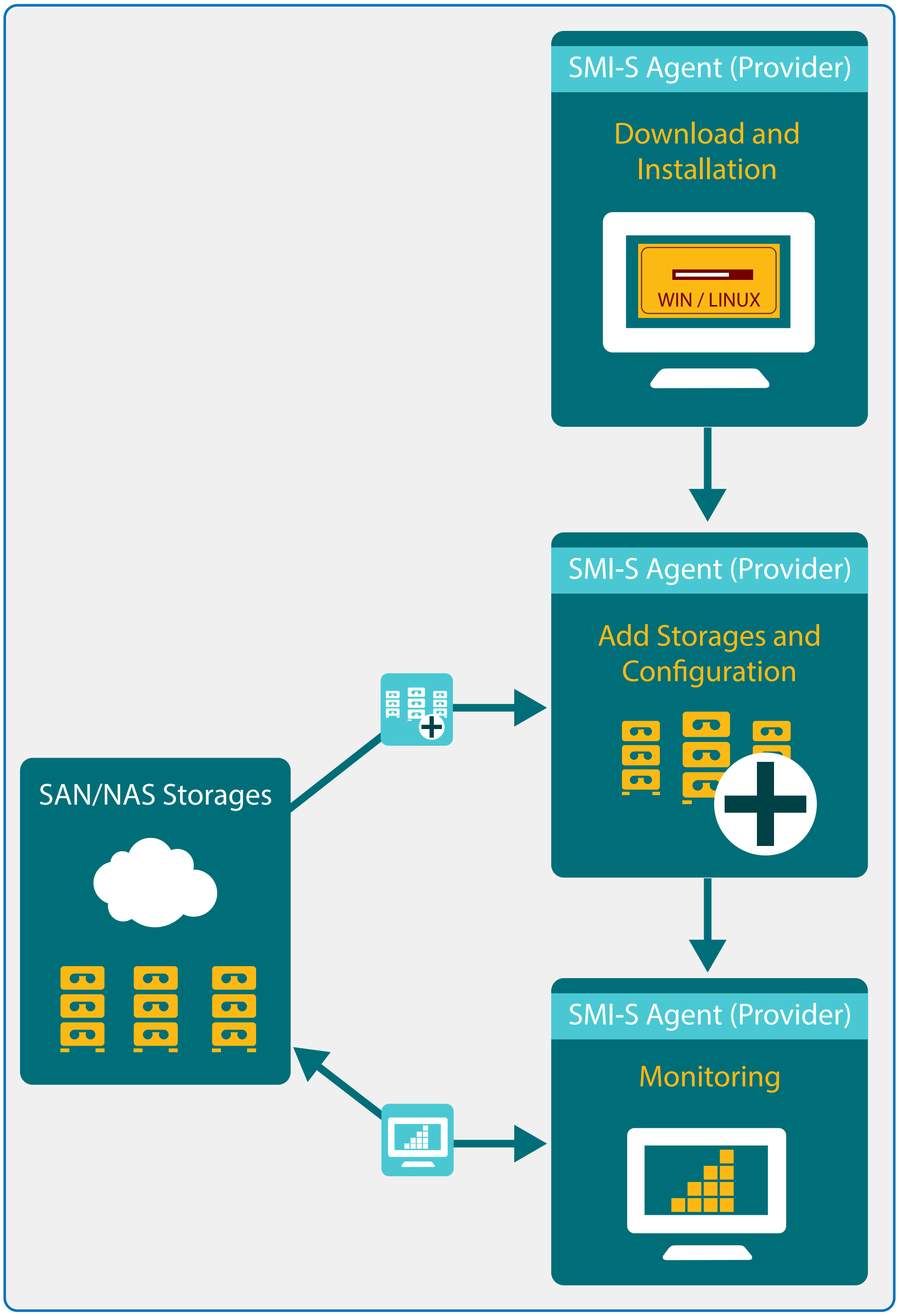
This release of AppManager for Hardware supports discovering and monitoring the Network Attached Storage (NAS) and Storage Area network (SAN) storage environments of NetApp, EMC, HP (3 PAR and MSA), and Dell (MSI) storages.

To discover and monitor the storage environments, you must configure the Storage Management Initiative Specification (SMI-S) provider (termed as SMI-S agent in NetApp). You can install the SMI-S provider either on a computer that runs the AppManager agent or on a separate computer. If you plan to install the SMI-S provider on the AppManager agent computer, ensure that the AppManager agent runs on an operating system that the SMI-S provider supports.

For more information about the supported operating systems, see the following:

- **For EMC:** “Environment and system requirements” section in EMC SMI-S Provider Release Notes.
- **For NetAPP:** “Supported operating system versions” section in Data ONTAP SMI-S Agent Installation and Configuration Guide.

The following figure demonstrates the workflow of configuring the SMI-S provider:



Prerequisites

To install the SMI-S provider, the computer must meet the following specifications:

- The host computer cannot be used to host a Hyper-V node.
- The host computer should not run System Center Virtual Machine Manager (SCVMM).
- You must have administrator rights to install this software.
- The host computer should not have any version of the SMI-S provider from any vendor.

For more information about prerequisites, see the following:

- **For EMC:** “Supported operating system versions” section in EMC SMI-S Provider Release Notes.
- **For NetAPP:** “Environment and system requirements” section in Data ONTAP SMI-S Agent Installation and Configuration Guide.
- **For Dell**: “System Requirements For SMI-S Provider” section in Dell PowerVault MD Series Storage Arrays SMI-S Provider Installation Guide.

Installing and Configuring the Data ONTAP SMI-S Provider for NetApp Storages

To install and configure the Data ONTAP SMI-S provider, follow this procedure:

1 Use the support account from the NetApp support site and download the SMI-S provider.

2 Follow the installation instructions available in the Data ONTAP SMI-S Agent Installation and Configuration Guide to install the SMI-S provider.

NOTE: Depending on the operating system, the instructions to install the agent differ.

3 Add storages to the SMI-S provider as per the instructions available in the Data ONTAP SMI-S Agent Installation and Configuration Guide.

4 Change the directory path to `SMI-S provider/bin` and then enter the following command at the command prompt to verify if the storages are added:

```
SMI-s list
```

5 Log in to the SMI-S provider computer and enter the following command to enable SMI-S provider authentication:

```
cimconfig -p -s enableAuthentication=true
```

NOTE: The SMI-S provider does not use Windows authentication.

6 Restart the SMI-S provider.

7 Use the following command to add the local user or domain administrator user on the SMI-S provider to the CIM server database:

```
cimuser -a -u Administrator –w password
```

For more information about adding a user, see Data ONTAP SMI-S Agent Installation and Configuration Guide.

8 Enter the following command to enable the HTTP connection:

```
cimconfig -s enableHttpConnection=true –p
```

9 (Conditional) Enter the following command to enable the HTTPS connection:

```
cimconfig -s enableHttpsConnection=true –p
```

9a Generate an own self-signed SSL authentication certificate, though SSL authentication is enabled by default.

For more information, see the “Generating a self-signed certificate for the CIM server” section in Data ONTAP SMI-S Agent Installation and Configuration Guide.

Installing and Configuring the SMI-S Provider for EMC

To install and configure the SMI-S Provider, follow this procedure:

1 Use the support account from the EMC online support site and download the appropriate SMI-S provider installer.

2 Follow the installation instructions available in the EMC SMI-S Provider Release Notes and install the SMI-S provider.

3 Add the CLARiiON and/or VNX storage arrays to the SMI-S Provider. For more information, see the “Out-of-band discovery method” section in EMC SMI-S Provider Release Notes.

4 Follow these steps to set up the administrator authentication:

4a Open a browser and enter the url `https://<ipaddress>:5989/ecomconfig`.

`ipaddress` is the ipaddress of the CIM server.

4b (Conditional) If you have not changed the default login ID and password for the SMI-S provider, log in with the default username `admin` and password `#1Password`. Otherwise, use the appropriate login ID and password.

Using this page, you can modify the password for the existing user, create a new user, and set other logging and security options.

4c Click **Dynamic Settings**.

4d (Conditional) If you are using an HTTP connection, unselect all the options under the Security_settings.xml section and then click **Apply**.

4e (Conditional) If you are using an HTTPS connection:

4e1 Select **SSLClientAuthentication**.

4e2 Select `None` under **Value**, click **Apply**, and then click **Back to ECOM Server Configuration** page.

4e3 Click **SSL Certificate Management**.

4e4 Download the latest certificate and add it to the client’s trust store.

For more information, see EMC SMI-S Provider Release Notes.

Installing and Configuring the SMI-S Provider for HP

The SMI-S Provider for HP 3PAR is integrated with the HP 3PAR storage array and does not require a separate installation. To configure the SMI-S Provider:

1 Log in to CLI using SSH.

2 Enter the `showcim` command.

3 (Conditional) If the state is inactive, enter the `setcim` command to enable the https or http port state.

4 To start and stop the SMI-S Provider, enter the `startcim` and `stopcim` commands.

The SMI-S Provider for HP MSA is integrated with the HP MSA storage array and does not require a separate installation.

To enable the HP MSA SMI-S Provider, select the SMI-S check box in User Management.

Installing and Configuring the SMI-S Provider for Dell

To install and configure the SMI-S provider, follow this procedure:

1. Use the storage account from the Dell community site and download the appropriate SMI-S Provider installer.
2. Follow the installation instructions available in the Dell PowerVault MD Series Storage Arrays SMI-S Provider Installation Guide to install the SMI-S Provider installer.
3. Specify the IP address of the Arrays Controllers.
4. Select the required authentication type and click **Finish** to complete the installation.
5. Use the commands in the Dell PowerVault MD Series Storage Arrays SMI-S Provider Installation Guide to configure the SMI-S Provider.

Configuring Security Manager

To discover hardware resources, AppManager requires an account with permission to gather remote device information. You must provide the account information in AppManager Security Manager.

For the proxy agent computer, complete the following fields on the **Custom** tab in Security Manager:

Field	Description
Label	Hardware

Sub-Label	Do one of the following:
	◆ Specify the server host name and the WBEM protocol as follows:
	`[`*`Monitored Server Hostname`*`]:WBEM`
	For example: `Server01:WBEM`
	◆ Specify the server IP address and the WBEM protocol as follows:
	`[`*`Monitored Server IP address`*`]:WBEM`
	For example: `10.99.120.1:WBEM`
	To discover a range of servers, provide the IP range.
	For example: `10.99.120.1-10.99.120.10:WBEM`
	When you run the Discovery_Hardware Knowledge Script, the Knowledge Script job converts the IP address to the fully-qualified domain name (FQDN). In the Operator Console and Control Center console, the FQDN identifies the servers.
	◆ Specify **default** to create a default account for which you have to provide the username, password and port in the Value 1, Value 2, and Value 3 fields respectively.
	Use the default account settings to discover servers that do not have the server information configured in Security Manager.
	◆ For SAN/NAS environments, specify the SMI-S agent IP address and the WBEM protocol as follows:
	`[`*`SMI-S Agent IP address`*`]:WBEM`
	For example: `10.99.135.5:WBEM`
	NOTE: Do not specify the IP address of the storage that you want to monitor.

Value 1	User name for the account that has permissions to gather remote device information You can specify a local or domain user. If you specify a domain user, use the format *`domain\username`*.
Value 2	Password for the user name identified in Value 2 field.
Value 3	Specify the port to gather remote device information. The default port is 5989.
Extended application support	Required field. Encrypts the user name and password in Security Manager. Do not leave this option unselected.

Discovering Hardware Resources

Use the Discovery_Hardware Knowledge Script to discover Cisco UCS, Dell, HP and IBM server. This script also discovers EMC and NetApp storages. This Knowledge Script raises events for successful, partial, and failed discoveries. You can also set severities to indicate the importance of each type of event.

To discover a server, you must configure the server information in AppManager Security Manager before you run the Discovery_Hardware Knowledge Script. For more information on configuring the Security Manager, see "Configuring Security Manager" on page 23.

This module does not support discovery of mass storage devices on some Dell Server, including Dell PowerEdge 1850 and Dell PowerEdge 2850.

By default, the discovery job schedule is set to run once. In a dynamically changing environment, NetIQ Corporation recommends that you schedule the discovery job in regular intervals of no less than an hour.

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

Description	How to Set It
Discovery Parameters	
List of servers to discover	Specify the remote server or servers on which you want to discover hardware resources. Use commas with no spaces to separate the server names. For example: `Server01,Server02,Server03` For EMC and NetApp, specify the SMI-S Provider DNS name or IP address.

Full path to file with list of servers to discover	Specify the full path to the text file on the local server containing the server or list of servers on which you want to discover hardware resources. For example:
	`C:\<`*`folder name`*`>\<`*`file name`*`>`
	To list the servers in the file, do one of the following:
	◆ Use commas with no spaces to separate the servers. For example: `Server01,Server02,Server03`
	◆ List the servers on separate lines. For example:
	`Server01`
	`Server02`
	`Server03`

Address range of servers to be discovered	Specify the address range of the servers on which you want to discover hardware resources. To discover a range of servers, you must also specify the same range in the **Sub-Label** field when you define the Hardware label in Security Manager. The range you specify in this Knowledge Script must match exactly the range you specified in Security Manager. You cannot specify a smaller range than you specified in Security Manager. For more information about creating the Hardware label in Security Manager, see "Configuring Security Manager" on page 23.

Description	How to Set It
Connection Timeout	Specify the number of seconds that the script should attempt to connect to the server for discovery before stopping as unsuccessful. The default is 20 seconds.
Event Details	
Event detail format	Specify how you want the event detail information formatted. Your options include: ◆ **HTML Table:** Displays the information in an HTML-formatted table. ◆ **Plain Text:** Displays the information in a table that uses plain text. The default is HTML Table.
Event Settings	
Raise event if discovery succeeds?	Select **Yes** to raise an event if the discovery process is successful. The default is Yes.
Event severity when discovery succeeds	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the discovery process is successful. The default is 25.
Raise event if discovery is partial?	Select **Yes** to raise an event if the discovery process is only partially successful. For example, if the discovery process was not able to detect the required resources for monitoring voltage levels. The default is Yes.
Event severity when discovery is partial	Set the event severity level, from 1 to 40, to indicate the importance of an event in which a discovery returns some data but also generates warning messages. The default is 15.
Raise event if discovery fails?	Select **Yes** to raise an event if the discovery process fails. The default is Yes.
Event severity when discovery fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the discovery process fails to discover hardware resources. The default is 5.
Event severity when unexpected error in Knowledge Script	Set the event severity level, from 1 to 40, to indicate the importance of an event in which when the script fails because of an unexpected error. The default is 5.

NOTE: The Discovery_Hardware raises a warning event that Voltage devices were not discovered for IBM server model (IBM x3850 M2), because this model does not have Voltage devices.

The Discovery_Hardware raises a partial discovery event for IBM HS23 blade running on ESXi 5.5, because the script does not discover fan and temperature objects due to unavailability of CIM classes.

3 Hardware Knowledge Scripts

The Hardware category provides the following Knowledge Scripts for monitoring Cisco UCS, Dell, HP, and IBM hardware resources and the storages of SAN/NAS environments of EMC and NetApp. From the Knowledge Script view of Control Center, you can access more information about any Knowledge Script by selecting it and clicking **Help**. In the Operator Console, select any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
Hardware Knowledge Scripts	
BatteryHealth	Monitors the operational status of system batteries.
FanHealth	Monitors the operational status of system fans.
LogicalDriveHealth	Monitors the operational status of system logical drives in an array.
MemoryHealth	Monitors the operational status of system memory.
NICHealth	Monitors the operational status of system network interface controllers (NICs).
PhysicalDriveHealth	Monitors the operational status of system physical drives in an array.
PowerSupplyHealth	Monitors the operational status of system power supplies.
ProcessorHealth	Monitors the operational status of system CPUs.
SmartArrayControllerHealth	Monitors the operational status of Smart Array controllers.
StorageBoxHealth	Monitors the operational status of storage boxes.
TemperatureHealth	Monitors the operational status of system temperature.
VoltageHealth	Monitors voltage levels on the system board.
Storage Specific Knowledge Scripts **IMPORTANT:** *In EMC and NetApp environments, schedule your Knowledge Script to run at an interval not less than the statistic time of the monitored object. For example, if the monitored object collects statistical data every 15 minutes, then schedule your Knowledge Script to run at an interval of either 15 minutes or more than that. If you schedule your job to run at an interval less than 15 minutes, the jobs return a value of zero.*	
LogicalDiskDataTransfer	Monitors the data transfer operations of logical disks or Flex volumes in an array
LogicalDiskIO	Monitors the input and output operations of logical disks in an array
LogicalDiskResponseTime	Monitors the response time, IO rate, wait time, and queue depth of logical disks or Flex volumes in an array.
LogicalDiskUtilization	Monitors the total, used, and free space of logical disk arrays in the monitored NetApp environment.
PhysicalDiskDataTransfer	Monitors the data transfer operations of physical disks in an array.
PhysicalDiskIO	Monitors the input and output operations of physical disks in an array.

Knowledge Script	What It Does
PhysicalDiskResponseTime	Monitors the response time, IO rate, wait time, and queue depth of physical disks in the monitored EMC environment.
StorageArrayUtilization	Monitors the consumable, used and available space of physical disk arrays in a network.

Understanding Hardware Resource States

Each Knowledge Script in the Hardware category provides options to raise an event when the monitored hardware resource is in the following states:

- Good
- Miscellaneous
- Degraded
- Undefined
- Error

The following table lists the values that the Knowledge Script job uses to determine the state of a monitored resource:

This value...	Indicates this condition...	Results in this state...	Returns this value if you choose to collect data about device status...
2	OK	Good	0
8	Starting	Miscellaneous	1
11	In service		
13	Lost communication		
15	Dormant		
17	Completed		
3	Degraded	Degraded	2
4	Stressed		
9	Stopping		
0	Unknown	Undefined	3
1	Other		
12	No contact		

This value...	Indicates this condition...	Results in this state...	Returns this value if you choose to collect data about device status...
5	Predictive failure	Error	4
6	Error		
7	Non-recoverable error		
10	Stopped		
14	Aborted		
16	Supporting entity in error		

Specifying Inclusion or Exclusion Filters

The Hardware Knowledge Scripts allow you to define inclusion and exclusion patterns and give you the option of limiting the resources matching the inclusion or exclusion pattern. By default, all resources are included. When you define an inclusion or exclusion pattern, it limits the resources that matches the defined pattern and allows the filtering of data you are transferring from/to a server.

You can specify the resources based on the Knowledge Scripts that you are working on. For example, if you are working with BatteryHealth Knowledge Script, then you can either include or exclude the servers for which you want to or do not want to monitor the health of the battery.

Similarly, you can specify the physical disks, logical disks, or physical drive depending on the Knowledge Script that you are working. Based on the selection in the *Inclusion or exclusion criteria* parameter, the resource that you specify will either be included or excluded from monitoring.

For inclusion and exclusion filters, specify the resources separated by commas with no spaces.

For example: `PhysicalDrive01,PhysicalDrive02,PhysicalDrive03`

Based on the selected criteria, the specified drives of all the monitored servers are included or excluded from monitoring.

All regular expressions are supported. For example, if you want to monitor `PhysicalDisk01`, `PhysicalDisk02`, and `PhysicalDisk03`, then specify `PhysicalDisk0[1-3]`.

To monitor the disks for a specific server, specify the server name and the device name in the following format:

<*server name*>:<*device name*>

For example: `Server01:PhysicalDrive1`

`PhysicalDrive1` is included in the monitoring of `Server01` only if you have selected the **Inclusion** criteria.

Based on the selected criteria, the format <*servername*>`:*` includes or excludes monitoring of all physical drive devices for the specified server. For example: `Server01:*` includes or excludes monitoring of all physical drive devices for `Server01`.

You can also specify a list of servers in the following format:

`Server01:*`, `Server02:*`, `Server03:*`

All the physical drive devices of `Server01`, `Server02`, and `Server03` are included in the monitoring only if you have selected the **Inclusion** criteria.

You can use the regular expressions while specifying the pattern matching. For more information on regular expressions, see “Using Regular Expression Filters” on page 30.

Using Regular Expression Filters

A regular expression is a pattern that describes a specific portion of text. The Hardware Knowledge Scripts enable you to use regular expressions to define inclusion and exclusion filters for pattern-matching against the text being evaluated.

The following table lists some commonly used regular expression types and their usage.

For more information about regular expression syntax, see related Web sites such as www.wikipedia.org/wiki/Regular_expression or www.regular-expressions.info.

<table>
<tr><th>Regular Expression Type</th><th>Description</th></tr>
<tr><td>Alternate Matches</td><td>A pipe character, |, indicates alternate possibilities.
For example:
◆ The expression a|b|c indicates a match with a, or b, or c.
◆ The expression fan1|fan2|fan3 indicates a match with fan1, or fan2, or fan3.</td></tr>
<tr><td>Anchor</td><td>Anchors do not match characters. Instead, they match a position before, after, or between characters. They anchor the regular expression match at a certain point.
◆ A ^ matches a position before the first character in a text string. For example, the expression ^a applied to the text string abc returns a because a is at the beginning of the text string. The expression ^b applied to the same text string returns no value, because b is not at the beginning of the text string.
◆ A $ matches a position right after the last character in a text string. For example, the expression c$ applied to the text string abc returns c because c is at the end of the text string. The expression a$ applied to the same string returns no value, because a is not at the end of the text string.</td></tr>
<tr><td>Escape Metacharacter</td><td>A backslash character, \, preceded with special characters such as ., @, |, *, ?, +, (,), {, }, [,], ^, $ and \ forces the special characters to be interpreted as normal characters.
For example:
◆ A dot (.) is usually used as a wildcard metacharacter, but if preceded by a backslash it represents the dot character itself. For information on wildcard metacharacter, see “Wildcard” on page 31.
◆ A colon (:) when preceded by a backslash excludes or includes all device names that contains : in their names.
◆ An equal sign (=) when preceded by a backslash excludes or includes all device names that contains = in their names.</td></tr>
</table>

Regular Expression Type	Description
Literal	A literal expression consists of a single character that matches all the occurrences of that character in the text string. For example, if the expression is a and the text string is `The gray cat is purring`, then the match is the a in `gray` and a in `cat`. All characters except for the following are literals: `.`, |, *, ?, +, `(`, `)`, `{`, `}`, `[`, `]`, ^, $ and `\`. These characters are treated as literals when preceded by a `\`.
Matching Characters or Digits	◆ **`\d:`** Matches a digit. ◆ **`\D:`** Matches a non-digit. ◆ **`\s:`** Matches a whitespace character. ◆ **`\S:`** Matches any character except a whitespace. ◆ **`\w:`** Matches an alphanumeric character. ◆ **`\W:`** Matches an non-alphanumeric character.
Parentheses	Use parentheses, `()`, to group characters and then apply a repetition operator to the group. For example, the expression `(ab)*` returns all of the string `ababab`.
Repeat	A repeat is an expression that is repeated an arbitrary number of times. ◆ A question mark, ?, indicates that the preceding character in the expression is optional. For example, the expression `ba`? returns `b` or `ba`. ◆ An asterisk, `*`, indicates that the preceding character is to be matched zero or more times. For example, the expression `ba*` returns all instances of `b`, `ba`, `baaa`, and so on. ◆ A plus sign, +, indicates that the preceding character is to be matched one or more times. The expression `ba`+ returns all instances of `ba` or `baaaa`, for example, but not `b`. ◆ Curly braces, `{}`, indicate a specific amount of repetition. For example, the expression `a{2}` returns the letter a repeated exactly twice. The expression `a{2,4}` returns the letter a repeated between 2 and 4 times. The expression `a{2,}` returns the letter a repeated at least twice, with no upper limit. For example, the expression `ba{2,4}` returns `baa`, `baaa`, and `baaaa`.
Square Brackets	Use square brackets, `[]`, to group characters to specify individual characters or ranges. Examples: ◆ The expression `fan[2-5]` returns all instances matching `fan2`, `fan3`, `fan4`, and `fan5`. ◆ The expression `fan[1-1]` returns all instances matching `fan1`.
Wildcard	The dot wildcard, `.`,matches any single character except line break characters. For example, the expression `gr.y` matches `gray`, `grey`, `gr%y`, and so on.

Regular Expression Type	Description
Word Boundary	- **\b:** Matches a zero-width word boundary, such as between a letter and a space. For example: `er\b` matches the `er` in `never` but not the `er` in `verb`. - **\B:** Matches a word non-boundary. For example: `er\B` matches the `er` in `verb` but not the `er` in `never`.

Metric Availability of Storage Knowledge Scripts

The following table details the various metrics available on EMC and NetApp storage environment for the storage specific Knowledge Scripts.

Metrics	EMC	NetApp (Flex Volumes)	NetApp (LUNs)
Logical Disk Data Transfer			
Total data transfer	Yes	Yes	Yes
Read data transfer	Yes	No	Yes
Write data transfer	Yes	No	Yes
Logical Disk IO			
Disk total IOs	Yes	Yes	Yes
Disk reads	Yes	No	Yes
Disk read hits	Yes	No	Yes
Disk read misses	Yes	No	Yes
Disk writes	Yes	No	Yes
Disk write hits	Yes	No	Yes
Disk write misses	Yes	No	Yes
Logical Disk Response Time			
Disk IO response time	Yes	Yes	Yes
Disk IO rate	Yes	Yes	Yes
Disk wait time	Yes	Yes	Yes
Disk queue depth	Yes	Yes	Yes
Logical Disk Utilization			
Array capacity	No	Yes	Yes
Array utilization	No	Yes	Yes
Array free space	No	Yes	Yes
Physical Disk Data Transfer			
Total data transfer	Yes	Yes	Yes
Read data transfer	Yes	Yes	Yes

Metrics	EMC	NetApp (Flex Volumes)	NetApp (LUNs)
Write data transfer	Yes	Yes	Yes
Physical Disk IO			
Disk total IOs	Yes	Yes	Yes
Disk reads	Yes	Yes	Yes
Disk writes	Yes	Yes	Yes
Physical Disk Response Time			
Disk IO response time	Yes	No	No
Disk IO rate	Yes	No	No
Disk wait time	Yes	No	No
Disk queue depth	Yes	No	No
Storage Array Utilization			
Array capacity	Yes	Yes	Yes
Array utilization	Yes	Yes	Yes
Array free space	Yes	Yes	Yes

BatteryHealth

Use this Knowledge Script to monitor the operational status of system batteries. The script raises an event if a monitored battery is not operating properly. You can also choose to raise events for conditions such as when a battery is in degraded state. You can set severities to indicate the importance of each type of event.

This Knowledge Script does not apply to HP servers and HP 3PAR SAN devices.

NOTE: If battery is available on the Cisco UCS server, AppManager discovers it. To monitor the operational status of the battery, run the BatteryHealth Knowledge Script.

Resource Objects

Battery object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain battery metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the battery. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain battery metrics	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the battery. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor battery status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor battery status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Battery Status	For more information about the various battery states, see “Understanding Hardware Resource States” on page 28.
Raise event if battery is in Good state?	Select **Yes** to raise an event if the operational status of the battery is Good. The default is unselected.
Event severity when battery is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the battery is Good. The default is 25.
Raise event if battery is in Error state?	Select **Yes** to raise an event if the operational status of the battery is Error. The default is Yes.
Event severity when battery is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the battery is Error. The default is 5.

Description	How to Set It
Raise event if battery is in Degraded state?	Select **Yes** to raise an event if the operational status of the battery is Degraded. The default is Yes.
Event severity when battery is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the battery is Degraded. The default is 15.
Raise event if battery is in Undefined state?	Select **Yes** to raise an event if the operational status of the battery is Undefined. The default is unselected.
Event severity when battery is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the battery is Undefined. The default is 12.
Raise event if battery is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the battery is Miscellaneous. The default is unselected.
Event severity when battery is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the battery is Miscellaneous. The default is 25.
Data Collection	
Collect data for battery device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified battery devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified battery devices.
Include or exclude batteries	Specify a list of battery devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Description	How to Set It

Full path to file containing list of batteries to include or exclude	Specify the path of the file that lists the battery devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `Battery01,Battery02,Battery03`
	- List the devices on separate lines. For example:
	`Battery01`
	`Battery02`
	`Battery03`
	All regular expressions are supported. For examples, see “Include or exclude batteries” on page 35.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

FanHealth

Use this Knowledge Script to monitor the operational status of system fans. The script raises an event if a monitored fan is not operating properly. You can also choose to raise events for other conditions such as when a fan is in a degraded state. You can set severities to indicate the importance of each type of event.

This Knowledge Script does not support monitoring the fan speed on HP and NetApp servers.

NOTE: In case of Cisco UCS servers, monitoring fans is only applicable to Cisco UCS C-Series Rack Server.

Resource Objects

Fan object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain fan metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the fan. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain fan metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the fan. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor fan status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor fan status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Fan Status	For more information about the various fan states, see "Understanding Hardware Resource States" on page 28.
Raise event if fan is in Good state?	Select **Yes** to raise an event if the operational status of the fan is Good. The default is unselected.
Event severity when fan is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the fan is Good. The default is 25.
Raise event if fan is in Error state?	Select **Yes** to raise an event if the operational status of the fan is Error. The default is Yes.
Event severity when fan is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the fan is Error. The default is 5.
Raise event if fan is in Degraded state?	Select **Yes** to raise an event if the operational status of the fan is Degraded. The default is Yes.

Description	How to Set It
Event severity when fan is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the fan is Degraded. The default is 15.
Raise event if fan is in Undefined state?	Select **Yes** to raise an event if the operational status of the fan is Undefined. The default is unselected.
Event severity when fan is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the fan is Undefined. The default is 12.
Raise event if fan is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the fan is Miscellaneous. The default is unselected.
Event severity when fan is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the fan is Miscellaneous. The default is 25.
Data Collection	
Collect data for fan device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see “Understanding Hardware Resource States” on page 28. The default is unselected.
Collect data for fan device speed?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns the current speed of the monitored resources. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified fan devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified fan devices.
Include or exclude fans	Specify a list of fan devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Description	How to Set It

Full path to file containing list of fans to include or exclude	Specify the path of the file that lists the fan devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `Fan01,Fan02,Fan03`
	◆ List the devices on separate lines. For example:
	`Fan01`
	`Fan02`
	`Fan03`
	All regular expressions are supported. For examples, see "Include or exclude fans" on page 38.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

LogicalDriveHealth

Use this Knowledge Script to monitor the operational status of system logical drives in an array. The script raises an event if a monitored logical drive is not operating properly. You can also choose to raise events for other conditions such as drive failure and set severities to indicate the importance of each type of event.

Resource Objects

Logical Drive object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.

Description	How to Set It
Raise event if job failed to obtain logical drive metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the logical drive. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain logical drive metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the logical drive. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor logical drive status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor logical drive status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Logical Drive Status	For more information about the various logical drive states, see "Understanding Hardware Resource States" on page 28.
Raise event if logical drive is in Good state?	Select **Yes** to raise an event if the operational status of the logical drive is Good. The default is unselected.
Event severity when logical drive is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the logical drive is Good. The default is 25.
Raise event if logical drive is in Error state?	Select **Yes** to raise an event if the operational status of the logical drive is Error. The default is Yes.
Event severity when logical drive is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the logical drive is Error. The default is 5.
Raise event if logical drive is in Degraded state?	Select **Yes** to raise an event if the operational status of the logical drive is Degraded. The default is Yes.
Event severity when logical drive is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the logical drive is Degraded. The default is 15.
Raise event if logical drive is in Undefined state?	Select **Yes** to raise an event if the operational status of the logical drive is Undefined. The default is unselected.

Description	How to Set It
Event severity when logical drive is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the logical drive is Undefined. The default is 12.
Raise event if logical drive is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the logical drive is Miscellaneous. The default is unselected.
Event severity when logical drive is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the logical drive is Miscellaneous. The default is 25.
Data Collection	
Collect data for logical drive device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see “Understanding Hardware Resource States” on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: - **Inclusion:** If you want to monitor the health status of the specified logical drive devices. - **Exclusion:** If you do not want to monitor the health status of the specified logical drive devices.
Include or exclude array logical disks	Specify a list of logical drive devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Full path to file containing list of array logical disks to include or exclude	Specify the path of the file that lists the logical drive devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `LogicalDrive1,LogicalDrive2,LogicalDrive3`
	- List the devices on separate lines. For example:
	`LogicalDrive1`
	`LogicalDrive2`
	`LogicalDrive3`
	All regular expressions are supported. For examples, see “Include or exclude array logical disks” on page 41.

Description	How to Set It
Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

MemoryHealth

Use this Knowledge Script to monitor the operational status of system memory. The script raises an event if the system memory 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.

NOTE: The memory device name of the IBM servers that are discovered on ESXi5.x display duplicate names in the Hardware tree view for the following models:

- x3850 M2
- x3650

Therefore, the data points that are collected are also duplicated.

Resource Objects

Global memory unit

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain memory device metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the system memory. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain memory device metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the system memory. The default is 5.

Description	How to Set It
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor system memory. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor system memory. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Memory Status	For more information about the various memory states, see "Understanding Hardware Resource States" on page 28.
Raise event if memory device is in Good state?	Select **Yes** to raise an event if the operational status of the system memory is Good. The default is unselected.
Event severity when memory device is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the system memory is Good. The default is 25.
Raise event if memory device is in Error state?	Select **Yes** to raise an event if the operational status of the system memory is Error. The default is Yes.
Event severity when memory device is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the system memory is Error. The default is 5.
Raise event if memory device is in Undefined state?	Select **Yes** to raise an event if the operational status of the system memory is Undefined. The default is unselected.
Event severity when memory device is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the system memory is Undefined. The default is 12.
Raise event if memory device is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the system memory is Miscellaneous. The default is unselected.
Event severity when memory device is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the system memory is Miscellaneous. The default is 25.
Data Collection	
Collect data for memory device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.

Description	How to Set It
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified memory devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified memory devices.
Include or exclude global memory units	Specify a list of memory devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of global memory units to include or exclude	Specify the path of the file that lists the memory devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `Memory01,Memory02,Memory03`
	◆ List the devices on separate lines. For example:
	`Memory01`
	`Memory02`
	`Memory03`
	All regular expressions are supported. For examples, see "Include or exclude global memory units" on page 44.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

NICHealth

Use this Knowledge Script to monitor the operational status of system network interface controllers (NICs). The script raises an event if a monitored NIC is down or 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.

Resource Objects

Network interface controller object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain NIC metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the NIC. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain NIC metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the NIC. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor NIC status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor NIC status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor NIC Status	For more information about the various NIC states, see "Understanding Hardware Resource States" on page 28.
Raise event if NIC is in Up state?	Select **Yes** to raise an event if the NIC is operating. The default is unselected.
Event severity when NIC is in Up state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the NIC is operating. The default is 25.
Raise event if NIC is in Down state?	Select **Yes** to raise an event if the NIC is not operating. The default is Yes.

Description	How to Set It
Event severity when NIC is in Down state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the NIC is not operating. The default is 5.
Raise event if NIC is in Error state?	Select **Yes** to raise an event if the operational status of the NIC is Error. The default is Yes.
Event severity when NIC is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the NIC is Error. The default is 5.
Raise event if NIC is in Undefined state?	Select **Yes** to raise an event if the operational status of the NIC is Undefined. The default is unselected.
Event severity when NIC is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the NIC is Undefined. The default is 12.
Raise event if NIC is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the NIC is Miscellaneous. The default is unselected.
Event severity when NIC is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the NIC is Miscellaneous. The default is 25.
Data Collection	
Collect data for NIC device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see “Understanding Hardware Resource States” on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified NIC devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified NIC devices.
Include or exclude Network Interface Controllers (NICs)	Specify a list of NIC devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Description	How to Set It

Full path to file containing list of Network Interface Controllers (NICs) to include or exclude	Specify the path of the file that lists the NIC devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `NIC01,NIC02,NIC03`
	◆ List the devices on separate lines. For example:
	`NIC01`
	`NIC02`
	`NIC03`
	All regular expressions are supported. For examples, see "Include or exclude Network Interface Controllers (NICs)" on page 46.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

PhysicalDriveHealth

Use this Knowledge Script to monitor the operational status of system physical drives in an array. The script raises an event if a monitored physical drive 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.

Resource Objects

Logical drive object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.

Description	How to Set It
Raise event if job failed to obtain physical drive metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the physical drive. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain physical drive metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the physical drive. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor physical drive status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor physical drive status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Physical Drive Status	For more information about the various physical drive states, see “Understanding Hardware Resource States” on page 28.
Raise event if Physical Drive is in Good state?	Select **Yes** to raise an event if the operational status of the physical drive is Good. The default is unselected.
Event severity when Physical Drive is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the physical drive is Good. The default is 25.
Raise event if Physical Drive is in Error state?	Select **Yes** to raise an event if the operational status of the physical drive is Error. The default is Yes.
Event severity when Physical Drive is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the physical drive is Error. The default is 5.
Raise event if Physical Drive is in Degraded state?	Select **Yes** to raise an event if the operational status of the physical drive is Degraded. The default is Yes.
Event severity when Physical Drive is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the physical drive is Degraded. The default is 15.
Raise event if Physical Drive is in Undefined state?	Select **Yes** to raise an event if the operational status of the physical drive is Undefined. The default is unselected.

Description	How to Set It
Event severity when Physical Drive is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the physical drive is Undefined. The default is 12.
Raise event if Physical Drive is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the physical drive is Miscellaneous. The default is unselected.
Event severity when Physical Drive is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the physical drive is Miscellaneous. The default is 25.
Data Collection	
Collect data for physical drive device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified physical drive devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified physical drive devices.
Include or exclude array physical disks	Specify a list of physical drive devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of array physical disks to include or exclude	Specify the path of the file that lists the physical drive devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `PhysicalDrive01,PhysicalDrive02,PhysicalDrive03`
	◆ List the devices on separate lines. For example:
	`PhysicalDrive01`
	`PhysicalDrive02`
	`PhysicalDrive03`
	All regular expressions are supported. For examples, see "Include or exclude array physical disks" on page 49.

Description	How to Set It
Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

PowerSupplyHealth

Use this Knowledge Script to monitor the operational status of system power supplies. The 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.

NOTE: In case of Cisco UCS servers, monitoring power supplies is only applicable to Cisco UCS C-Series Rack Server.

Resource Objects

Power supply object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain power supply metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the power supply. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain power supply metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the power supply. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.

Description	How to Set It
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor power supply status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor power supply status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Power Supply Status	For more information about the various power supply states, see "Understanding Hardware Resource States" on page 28.
Raise event if power supply is in Good state?	Select **Yes** to raise an event if the operational status of the power supply is Good. The default is unselected.
Event severity when power supply is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the power supply is Good. The default is 25.
Raise event if power supply is in Error state?	Select **Yes** to raise an event if the operational status of the power supply is Error. The default is Yes.
Event severity when power supply is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the power supply is Error. The default is 5.
Raise event if power supply is in Degraded state?	Select **Yes** to raise an event if the operational status of the power supply is Degraded. The default is Yes.
Event severity when power supply is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the power supply is Degraded. The default is 15.
Raise event if power supply is in Undefined state?	Select **Yes** to raise an event if the operational status of the power supply is Undefined. The default is unselected.
Event severity when power supply is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the power supply is Undefined. The default is 12.
Raise event if power supply is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the power supply is Miscellaneous. The default is unselected.
Event severity when power supply is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the power supply is Miscellaneous. The default is 25.
Data Collection	
Collect data for power supply device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.

Description	How to Set It
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: - **Inclusion:** If you want to monitor the health status of the specified power supply devices. - **Exclusion:** If you do not want to monitor the health status of the specified power supply devices.
Include or exclude power supplies	Specify a list of power supply devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of power supplies to include or exclude	Specify the path of the file that lists the power supply devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `PS01,PS02,PS03`
	- List the devices on separate lines. For example:
	`PS01`
	`PS02`
	`PS03`
	All regular expressions are supported. For examples, see "Include or exclude power supplies" on page 52.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

ProcessorHealth

Use this Knowledge Script to monitor the operational status of system CPUs. The script raises an event if a monitored CPU 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.

This Knowledge Script does not apply to HP 3PAR SAN devices.

Resource Objects

Processor object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain CPU metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the CPU. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain **CPU** metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the CPU. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor processor status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor processor status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor CPU Status	For more information about the various CPU states, see "Understanding Hardware Resource States" on page 28.
Raise event if CPU is in Good state?	Select **Yes** to raise an event if the operational status of the CPU is Good. The default is unselected.
Event severity when CPU is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the CPU is Good. The default is 25.
Raise event if CPU is in Error state?	Select **Yes** to raise an event if the operational status of the CPU is Error. The default is Yes.

Description	How to Set It
Event severity when CPU is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the CPU is Error. The default is 5.
Raise event if CPU is in Degraded state?	Select **Yes** to raise an event if the operational status of the CPU is Degraded. The default is Yes.
Event severity when CPU is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the CPU is Degraded. The default is 15.
Raise event if CPU is in Undefined state?	Select **Yes** to raise an event if the operational status of the CPU is Undefined. The default is unselected.
Event severity when CPU is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the CPU is Undefined. The default is 12.
Raise event if CPU is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the CPU is Miscellaneous. The default is unselected.
Event severity when CPU is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the CPU is Miscellaneous. The default is 25.
Data Collection	
Collect data for CPU device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.
Collect data for CPU device clockspeed?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns the current speed of the monitored resources. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified processor devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified processor devices.
Include or exclude processors	

Description	How to Set It

Full path to file containing list of processors to include or exclude	Specify the path of the file that lists the processor devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*path to file*`>` rather than `\\<`*server*`>\D$\<`*path to file*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `CPU01,CPU02,CPU03`
	◆ List the devices on separate lines. For example:
	`CPU01`
	`CPU02`
	`CPU03`
	All regular expressions are supported. For examples, see “Include or exclude processors” on page 54.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

SmartArrayControllerHealth

Use this Knowledge Script to monitor the operational status of Smart Array controllers. The script raises an event if a monitored controller 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.

This Knowledge Script does not apply to HP 3PAR SAN devices.

Resource Objects

Smart Array controller object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	

Description	How to Set It
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain Smart Array controller metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the controller. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain Smart Array controller metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the controller. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor Smart Array controller status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor Smart Array controller status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Smart Array Controller Status	For more information about the various Smart Array controller states, see “Understanding Hardware Resource States” on page 28.
Raise event if Smart Array controller is in Good state?	Select **Yes** to raise an event if the operational status of the controller is Good. The default is unselected.
Event severity when Smart Array controller is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the controller is Good. The default is 25.
Raise event if Smart Array controller is in Error state?	Select **Yes** to raise an event if the operational status of the controller is Error. The default is Yes.
Event severity when Smart Array controller is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the controller is Error. The default is 5.
Raise event if Smart Array controller is in Degraded state?	Select **Yes** to raise an event if the operational status of the controller is Degraded. The default is Yes.
Event severity when Smart Array controller is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the controller is Degraded. The default is 15.

Description	How to Set It
Raise event if Smart Array controller is in Undefined state?	Select **Yes** to raise an event if the operational status of the Smart Array controller is Undefined. The default is unselected.
Event severity when Smart Array controller is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the controller is Undefined. The default is 12.
Raise event if Smart Array controller is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the controller is Miscellaneous. The default is unselected.
Event severity when Smart Array controller is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the controller is Miscellaneous. The default is 25.
Data Collection	
Collect data for Smart Array controller device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified Smart Array controller devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified Smart Array controller devices.
Include or exclude Smart Array controllers	Specify a list of Smart Array controller devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Description	How to Set It

Full path to file containing list of Smart Array controllers to include or exclude	Specify the path of the file that lists the Smart Array controller devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `SmartArray01`,`SmartArray02`,`SmartArray03`
	◆ List the devices on separate lines. For example:
	`SmartArray01`
	`SmartArray02`
	`SmartArray03`
	All regular expressions are supported. For examples, see "Include or exclude Smart Array controllers" on page 57.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

StorageBoxHealth

Use this Knowledge Script to monitor the operational status of storage boxes on HP servers. The script raises an event if a monitored storage box 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.

This Knowledge Script does not apply to Cisco UCS, Dell, and IBM servers.

Resource Objects

Storage box object for HP servers

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	

Description	How to Set It
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain storage box device metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the storage box. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain storage box device metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the storage box. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor storage box status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor storage box status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Storage Box Status	For more information about the various storage box states, see "Understanding Hardware Resource States" on page 28.
Raise event if storage box device is in Good state?	Select **Yes** to raise an event if the operational status of the storage box is Good. The default is unselected.
Event severity when storage box device is in Good State	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the storage box is Good. The default is 25.
Raise event if storage box device is in Error state?	Select **Yes** to raise an event if the operational status of the storage box is Error. The default is Yes.
Event severity when storage box device is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the storage box is Error. The default is 5.
Raise event if storage box device is in Undefined state?	Select **Yes** to raise an event if the operational status of the storage box is Undefined. The default is unselected.
Event severity when storage box device is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the storage box is Undefined. The default is 12.

Description	How to Set It
Raise event if storage box device is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the storage box is Miscellaneous. The default is unselected.
Event severity when storage box device is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the storage box is Miscellaneous. The default is 25.
Data Collection	
Collect data for storage box device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see “Understanding Hardware Resource States” on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the health status of the specified storage box devices. ◆ **Exclusion:** If you do not want to monitor the health status of the specified storage box devices.
Include or exclude storage boxes	Specify a list of storage box devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Full path to file containing list of storage boxes to include or exclude	Specify the path of the file that lists the storage box devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `Box01,Box02,Box03`
	◆ List the devices on separate lines. For example:
	`Box01`
	`Box02`
	`Box03`
	All regular expressions are supported. For examples, see “Include or exclude storage boxes” on page 60.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

TemperatureHealth

Use this Knowledge Script to monitor the operational status of the system temperature. The script raises an event if there is a temperature-related issue. You can also choose to raise events for other conditions and set severities to indicate the importance of each type of event.

Resource Objects

Temperature object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain temperature sensor metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the temperature sensor. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain temperature sensor metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the temperature sensor. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor temperature sensor status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor temperature sensor status. The default is 35.
Event Details	

Description	How to Set It
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Temperature Sensor Status	For more information about the various temperature sensor states, see "Understanding Hardware Resource States" on page 28.
Raise event if temperature sensor is in Good state?	Select **Yes** to raise an event if the operational status of the temperature sensor is Good. The default is unselected.
Event severity when temperature sensor is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the temperature sensor is Good. The default is 25.
Raise event if temperature sensor is in Error state?	Select **Yes** to raise an event if the operational status of the temperature sensor is Error. The default is Yes.
Event severity when temperature sensor is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the temperature sensor is Error. The default is 5.
Raise event if temperature sensor is in Degraded state?	Select **Yes** to raise an event if the operational status of the temperature sensor is Degraded. The default is Yes.
Event severity when temperature sensor is in Degraded state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the temperature sensor is Degraded. The default is 15.
Raise event if temperature sensor is in Undefined state?	Select **Yes** to raise an event if the operational status of the temperature sensor is Undefined. The default is unselected.
Event severity when temperature sensor is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the temperature sensor is Undefined. The default is 12.
Raise event if temperature sensor is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the temperature sensor is Miscellaneous. The default is unselected.
Event severity when temperature sensor is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the temperature sensor is Miscellaneous. The default is 25.
Data Collection	
Collect data for temperature sensor status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see "Understanding Hardware Resource States" on page 28. The default is unselected.
Collect data for temperature sensor reading?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns the current temperature sensor reading for the monitored resources. The default is unselected.
Inclusion or Exclusion Filter	

Description	How to Set It
Inclusion or exclusion criteria	Select one of the following criteria: - **Inclusion:** If you want to monitor the health status of the specified temperature sensor devices. - **Exclusion:** If you do not want to monitor the health status of the specified temperature sensor devices.
Include or exclude temperature devices	Specify a list of temperature sensor devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of temperature devices to include or exclude	Specify the path of the file that lists the temperature sensor devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `Temp01,Temp02,Temp03`
	- List the devices on separate lines. For example:
	`Temp01`
	`Temp02`
	`Temp03`
	All regular expressions are supported. For examples, see "Include or exclude temperature devices" on page 63.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

VoltageHealth

Use this Knowledge Script to monitor voltage levels on a system board. The script raises an event if there is a voltage-related issue. You can also choose to raise events for other conditions and set severities to indicate the importance of each type of event.

This Knowledge Script is not applicable for HP servers.

Resource Objects

Voltage object

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to obtain voltage device metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to obtain data about the operational status of the voltage sensor. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to obtain voltage device metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to obtain data about the operational status of the voltage sensor. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor voltage sensor status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of computers for which you do not want to monitor voltage sensor status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Monitor Voltage Device Status	For more information about the various voltage device states, see "Understanding Hardware Resource States" on page 28.
Raise event if voltage device is in Good state?	Select **Yes** to raise an event if the operational status of the voltage sensor is Good. The default is unselected.
Event severity when voltage device is in Good state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the voltage sensor is Good. The default is 25.

Description	How to Set It
Raise event if voltage device is in Error state?	Select **Yes** to raise an event if the operational status of the voltage sensor is Error. The default is Yes.
Event severity when voltage device is in Error state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the voltage sensor is Error. The default is 5.
Raise event if voltage device is in Undefined state?	Select **Yes** to raise an event if the operational status of the voltage sensor is Undefined. The default is unselected.
Event severity when voltage device is in Undefined state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the voltage sensor is Undefined. The default is 12.
Raise event if voltage device is in Miscellaneous state?	Select **Yes** to raise an event if the operational status of the voltage sensor is Miscellaneous. The default is unselected.
Event severity when voltage device is in Miscellaneous state	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the operational status of the voltage sensor is Miscellaneous. The default is 25.
Data Collection	
Collect data for voltage device status?	Select **Yes** to collect data for charts and reports. If you select **Yes**, this Knowledge Script returns a value that indicates the status of the monitored resources. For more information about the possible values, see “Understanding Hardware Resource States” on page 28. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** Select **Inclusion** if you want to monitor the health status of the specified voltage devices. ◆ **Exclusion:** Select **Exclusion** if you do not want to monitor the health status of the specified voltage devices.
Include or exclude voltage devices	Specify a list of voltage devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Description	How to Set It

Full path to file containing list of voltage device to include or exclude	Specify the path of the file that lists the voltage devices that you want to include or exclude from monitoring based on your selection in the **Inclusion or exclusion criteria** parameter. You can also click **Browse [...]** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `Voltage01,Voltage02,Voltage03`
	◆ List the devices on separate lines. For example:
	`Voltage01`
	`Voltage02`
	`Voltage03`
	All regular expressions are supported. For examples, see "Include or exclude voltage devices" on page 65.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

LogicalDiskDataTransfer

Use this Knowledge Script to monitor the array logical disk or Flex volumes for total transfers, read, and write transfers per second. This script raises an event if this job fails to fetch metrics for monitored logical disks or Flex volumes and if the threshold exceeds for read, write, or total data transfer. You can also set severities to indicate the importance of each type of event.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Array logical disks (EMC environment)

Flex volumes (includes LUNs of NetApp environment)

Default Schedule

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

Setting Parameter Values

NOTE: In a NetApp environment, none of the metrics are available for Flex volumes except total data transfer. However, all the metrics are available for LUNs in a NetApp environment.

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get data transfer metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get metrics about the data transfer operations of the logical disk. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get data transfer metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get metrics about the data transfer operations of the logical disk. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want to or do not want to monitor disk status. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want to or do not want to monitor the disk status. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if total data transfers exceed threshold?	Select **Yes** to raise an event if the total number of data transfer per second to the logical disks exceeds the threshold you set. The default is unselected.
Event severity when total data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total data transfer exceeds the threshold. The default is 15.
Threshold - Maximum total data transfers	Specify the maximum count of data transfers that a logical disk can handle in a second before raising an event. The default is 30 MB per second.
Raise event if read data transfers exceed threshold?	Select **Yes** to raise an event if the number of read data transfers per second from the logical disks exceeds the threshold you set. The default is unselected.
Event severity when read data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the read data transfers exceed the threshold. The default is 15.

Description	How to Set It
Threshold - Maximum read data transfers	Specify the maximum count of read data that a logical disk can transfer in a second before raising an event. The default is 30 MB per second.
Raise event if write data transfers exceed threshold?	Select **Yes** to raise an event if the number of write data transfers per second to the logical disks exceeds the threshold you set. The default is unselected.
Event severity when write data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the write data transfers exceed the threshold. The default is 15.
Threshold - Maximum write data transfers	Specify the maximum count of write data that a logical disk can transfer in a second before raising an event. The default is 30 MB per second.
Data Collection	
Collect data for total data transfers?	Select **Yes** to collect total data transfers from/to the logical disks for charts and reports. The default is unselected.
Collect data for read data transfers?	Select **Yes** to collect total read data transfers from logical disks for charts and reports. The default is unselected.
Collect data for write data transfers?	Select **Yes** to collect total write data transfers to logical disks for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the data transfers of the specified logical disks. ◆ **Exclusion:** If you do not want to monitor the data transfers of the specified logical disks.
Include or exclude logical disks	Specify a list of logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Full path to file containing list of physical disks to include or exclude	Specify the path of the file that lists the logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the disks. For example: `LogicalDisk01,LogicalDisk02,LogicalDisk03`
	◆ List the disks on separate lines. For example:
	`LogicalDisk01`
	`LogicalDisk02`
	`LogicalDisk03`
	All regular expressions are supported.

Description	How to Set It
Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

LogicalDiskIO

Use this Knowledge Script to monitor the array logical disk or Flex volumes for total diskIO, read/write count, read/write hits if read/write hit operations succeed to perform on logical disk cache, and read/write misses if read/write miss operations fail to perform on logical disk cache. This script raises an event if this job fails to fetch IO metrics for monitored logical disks and if the threshold exceeds for any of the metrics. You can also set severities to indicate the importance of each type of event.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Array logical disks (EMC environment)

Flex volumes (includes LUNs of NetApp environment)

Default Schedule

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

Setting Parameter Values

NOTE: In a NetApp environment, none of the metrics are available for Flex volumes except disk total IOs. However, all the metrics are available for LUNs in a NetApp environment.

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get disk metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get IO metrics of the logical disks. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get disk metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get IO metrics of the logical disks. The default is 5.

Description	How to Set It
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want or do not want to monitor logical disk IO operations. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want to or do not want to monitor IO operations. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if disk total IOs exceed the threshold?	Select **Yes** to raise an event if the total number of IOs per second to the logical disks exceeds the threshold you set. The default is Yes.
Event severity when disk total IOs exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total disk IOs of a logical disk exceed the threshold. The default is 15.
Threshold - Maximum disk total IOs	Specify the maximum count of input and output operations that a logical disk can handle in a second before raising an event. The default is 600 IOs/second.
Disk Reads	
Raise event if disk reads exceed the threshold?	Select **Yes** to raise an event if the number of reads per second from the logical disks exceed the threshold you set. The default is unselected.
Event severity when disk reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of disk reads from a logical disk exceeds the threshold. The default is 15.
Threshold - Maximum disk reads	Specify the maximum count of read operations that a logical disk can handle in a second before raising an event. The default is 300 reads/second.
Raise event if read hits exceed the threshold?	Select **Yes** to raise an event if the number of successful read operations per second from logical disk cache exceeds the threshold you set. The default is unselected.
Event severity when read hits exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of successful disk reads from logical disk cache exceeds the threshold. The default is 15.
Threshold - Maximum read hits	Specify the maximum count of successful read operations that a logical disk cache can handle in a second before raising an event. The default is 300 read hits/second.
Raise event if read misses exceed the threshold?	Select **Yes** to raise an event if the number of failed read operations per second on the logical disk cache exceeds the threshold you set. The default is unselected.

Description	How to Set It
Event severity when read misses exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of read operations that failed exceeds the threshold. The default is 15.
Threshold - Maximum read misses	Specify the maximum count of read operations that a logical disk cache can miss in a second before raising an event. The default is 300 read misses/second.
Disk Writes	
Raise event if disk writes exceed the threshold?	Select **Yes** to raise an event if the number of writes per second to the logical disks exceeds the threshold you set. The default is unselected.
Event severity when disk writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of disk writes to a logical disk exceeds the threshold. The default is 15.
Threshold - Maximum disk writes	Specify the maximum count of write operations that a logical disk can handle in a second before raising an event. The default is 300 writes/second.
Raise event if write hits exceed the threshold?	Select **Yes** to raise an event if the number of successful write operations per second to logical disk cache exceeds the threshold you set. The default is unselected.
Event severity when write hits exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of successful disk writes to logical disk cache exceeds the threshold. The default is 15.
Threshold - Maximum write hits	Specify the maximum count of write operations that a logical disk cache can handle in a second before raising an event. The default is 300 write hits/second.
Raise event if write misses exceed the threshold?	Select **Yes** to raise an event if the number of failed write operations per second to the logical disk cache exceeds the threshold you set. The default is unselected.
Event severity when write misses exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of disk write misses exceeds the threshold. The default is 15.
Threshold - Maximum write misses	Specify the maximum count of write operations that a logical disk cache can miss in a second before raising an event. The default is 300 write misses/second.
Data Collection	
Collect data for disk total IOs?	Select **Yes** to collect the total input and output data of logical disks for charts and reports. The default is unselected.
Collect data for disk reads?	Select Yes to collect the total read data of logical disks for charts and reports. The default is unselected.
Collect data for disk read hits?	Select Yes to collect the read hits data of logical disks for charts and reports. The default is unselected.
Collect data for disk read misses?	Select Yes to collect the read miss data of logical disks for charts and reports. The default is unselected.
Collect data for disk writes?	Select Yes to collect the total write data of logical disks for charts and reports. The default is unselected.

Description	How to Set It
Collect data for disk write hits?	Select Yes to collect the write hits data of logical disks for charts and reports. The default is unselected.
Collect data for disk write misses?	Select Yes to collect the write miss data of logical disks for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the IO operations of the specified logical disks. ◆ **Exclusion:** If you do not want to monitor the IO operations of the specified logical disks. By default, it is Inclusion.
Include or exclude logical disks	Specify a list of logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of logical disks to include or exclude	Specify the path of the file that lists the logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `LogicalDisk01,LogicalDisk02,LogicalDisk03`
	◆ List the disks on separate lines. For example:
	`LogicalDisk01`
	`LogicalDisk02`
	`LogicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

LogicalDiskResponseTime

Use this Knowledge Script to monitor the response time, wait time, IO rate, and queue depth of logical disks or Flex volumes in an array. This script raises an event if this job fails to get the metrics on response time. This script also raises an event if the threshold exceeds for response rate, IO rate, wait time, or queue depth. This script also generates data streams for these metrics.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Array logical disks (EMC environment)

Flex volumes (includes LUNs of NetApp environment)

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get disk metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get metrics of the logical disks or Flex volumes. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get disk metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get metrics about logical disk or Flex volumes. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want or do not want to monitor logical disk response time. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want to or do not want to monitor response time. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if the disk response time exceeds the threshold?	Select **Yes** to raise an event if the logical disk response time exceeds the threshold you set. The default is Yes.

Description	How to Set It
Event severity when the disk response time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the logical disk response time exceeds the threshold. The default is 15.
Threshold - Maximum disk response time	Specify the maximum time that a logical disk should take to respond before raising an event. The default is 30 milliseconds.
Raise event if the disk IO rate exceeds the threshold?	Select **Yes** to raise an event if the logical disk IO rate per second exceeds the threshold you set. The default is unselected.
Event severity when the disk IO rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the logical disk IO rate per second exceeds the threshold. The default is 15.
Threshold - Maximum disk IO rate	Specify the maximum number of IO rate that a logical disk can handle in a second before raising an event. The default is 300 IO/second.
Raise event if the disk wait time exceeds the threshold?	Select **Yes** to raise an event if the logical disk wait time exceeds the threshold you set. The default is unselected.
Event severity when the disk wait time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the logical disk wait time exceeds the threshold. The default is 15.
Threshold - Maximum disk wait time	Specify the maximum time that a logical disk IO request can wait for response before raising an event. The default is 5 milliseconds.
Raise event if the disk queue depth exceeds the threshold?	Select **Yes** to raise an event if the logical disk IO requests that are waiting in the queue for response exceed the threshold you set. The default is unselected. As the queue depth increases, the average wait time also increases because the requests that are waiting in the queue have to run first.
Event severity when the disk queue depth exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the logical disk IO requests that are in the queue for response exceed the threshold. The default is 15.
Threshold - Maximum disk queue depth	Specify the maximum requests that can be queued up for response before raising an event. The default is 5 requests.
Data Collection	
Collect data for disk response time?	Select **Yes** to collect the IO response time of logical disks for charts and reports. The default is unselected.
Collect data for disk IO rate?	Select Yes to collect the total IO rate of logical disks for charts and reports. The default is unselected.
Collect data for disk wait time?	Select Yes to collect the wait time that a logical disk request is waiting for response, for charts and reports. The default is unselected.
Collect data for disk queue depth?	Select Yes to collect the number of logical disk requests that are queued up for response, for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	

Description	How to Set It
Inclusion or exclusion criteria	Select one of the following criteria: - **Inclusion:** If you want to monitor the response time of the specified logical disks. - **Exclusion:** If you do not want to monitor the response time of the specified logical disks.
Include or exclude logical disks	Specify a list of logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of logical disks to include or exclude	Specify the path of the file that lists the logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `LogicalDisk01,LogicalDisk02,LogicalDisk03`
	- List the disks on separate lines. For example:
	`LogicalDisk01`
	`LogicalDisk02`
	`LogicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

LogicalDiskUtilization

Use this Knowledge Script to monitor the space utilization of Flex volumes and LUNs in NAS environments. This script raise events for conditions such as when the job cannot get the logical disk capacity metrics or when the used space per disk exceeds the threshold you set. You can set severities to indicate the importance of each type of event. This script collects data for disk capacity, utilization and free space in a storage environment.

This Knowledge Script applies only to NAS environments.

Resource Objects

Flex Volumes (includes LUNs of NetApp environment)

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get disk utilization metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get metrics on disk utilization of logical disks or Flex volumes. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get disk utilization metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get logical disk utilization metrics. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want or do not want to get the disk utilization. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of logical disks for which you either want or do not want to monitor disk utilization. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if disk utilization exceeds the threshold?	Select **Yes** to raise an event if the logical disk utilization exceeds the threshold you set. The default is Yes.
Event severity when disk utilization exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the logical disk utilization exceeds the threshold. The default is 15.
Threshold - Maximum disk utilization	Specify the percentage up to which the logical disk space can be utilized before raising an event. The default is 85%.

Description	How to Set It
Include summary for disk utilization in event details?	Select **Yes** to display the elaborated logical disk utilization details of all the disks in an array. The default is unselected.
Data Collection	
Collect data for disk capacity?	Select **Yes** to collect data for the logical disk capacity, for charts and reports. This data is the actual consumable space that is available. The default is unselected.
Collect data for disk utilization?	Select **Yes** to collect data for the logical disk utilized space, for charts and reports. The default is unselected.
Collect data for disk free space?	Select **Yes** to collect data for the logical disk free space, for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the disk utilization of the specified logical disks. ◆ **Exclusion:** If you do not want to monitor the disk utilization of the specified logical disks.
Include or exclude logical disks	Specify a list of logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Full path to file containing list of logical disks to include or exclude	Specify the path of the file that lists the logical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the devices. For example: `LogicalDisk01,LogicalDisk02,LogicalDisk03`
	◆ List the disks on separate lines. For example:
	`LogicalDisk01`
	`LogicalDisk02`
	`LogicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

PhysicalDiskDataTransfer

Use this Knowledge Script to monitor the array physical disks for total transfer, read, and write transfers per second. This script raises an event if this job fails to fetch metrics for monitored physical disks and if the threshold exceeds for read, write, or total data transfer. You can also set severities to indicate the importance of each type of event.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Array physical disks

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get data transfer metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get data about the data transfer operation of the physical disk. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get data transfer metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get metrics about the data transfer operations of the physical disk. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of physical disks for which you either want to or do not want to monitor data transfer. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of physical disks for which you either want to or do not want to monitor data transfer. The default is 35.

Description	How to Set It
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if the total data transfers exceed threshold?	Select **Yes** to raise an event if the total number of data transfer per second to the physical disks exceeds the threshold you set. The default is unselected.
Event severity when total data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total data transfer of a physical disk exceeds the threshold. The default is 15.
Threshold - Maximum total data transfers	Specify the maximum count of data transfers that a physical disk can handle in a second before raising an event. The default is 50 MB per second.
Raise event if read data transfers exceed threshold?	Select **Yes** to raise an event if the number of read data transfers per second from the physical disks exceeds the threshold you set. The default is unselected.
Event severity when read data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the read data transfer of a physical disk exceeds the threshold. The default is 15.
Threshold - Maximum read data transfers	Specify the maximum count of read data that a physical disk can transfer in a second before raising an event. The default is 30 MB per second.
Raise event if write data transfers exceed threshold?	Select **Yes** to raise an event if the number of write data transfers per second to the physical disks exceeds the threshold you set. The default is unselected.
Event severity when write data transfers exceed threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the write data transfer of a physical disk exceeds the threshold. The default is 15.
Threshold - Maximum write data transfers	Specify the maximum count of write data that a physical disk can transfer in a second before raising an event. The default is 30 MB per second.
Data Collection	
Collect data for total data transfers?	Select **Yes** to collect the data transfers from/to the physical disks for charts and reports. The default is unselected.
Collect data for read data transfers?	Select Yes to collect the total read data transfers from physical disks for charts and reports. The default is unselected.
Collect data for write data transfers?	Select Yes to collect the total write data transfers to physical disks for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the data transfers of the specified physical disks. ◆ **Exclusion:** If you do not want to monitor the data transfers of the specified physical disks.

Description	How to Set It
Include or exclude physical disks	Specify a list of physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Full path to file containing list of physical disks to include or exclude	Specify the path of the file that lists the physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the disks. For example: `PhysicalDisk01,PhysicalDisk02,PhysicalDisk03`
	◆ List the disks on separate lines. For example:
	`PhysicalDisk01`
	`PhysicalDisk02`
	`PhysicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

PhysicalDiskIO

Use this Knowledge Script to monitor the array physical disks for total disk IO and read/write count. This script raises an event if this job fails to fetch IO metrics for monitored physical disks and if the threshold exceeds for any of the metrics. You can also set severities to indicate the importance of each type of event.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Array physical disks

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get disk metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get IO metrics of the physical disks. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get disk metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get IO metrics of the physical disks. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of physical disks for which you either want to or do not want to monitor disk IO operations. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want to or do not want to monitor physical disk IO operations. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if disk total IOs exceed the threshold?	Select **Yes** to raise an event if the total number of IOs per second to the physical disks exceeds the threshold you set. The default is Yes.
Event severity when disk total IOs exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the total disk IOs of a physical disk exceed the threshold. The default is 15.
Threshold - Maximum disk total IOs	Specify the maximum count of input and output operations that a physical disk can handle in a second before raising an event. The default is 300 IOs/second.
Raise event if disk reads exceed the threshold?	Select **Yes** to raise an event if the number of reads per second from the physical disks exceed the threshold you set. The default is unselected.

Description	How to Set It
Event severity when disk reads exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of disk reads from a physical disk exceeds the threshold. The default is 15.
Threshold - Maximum disk reads	Specify the maximum count of read operations that a physical disk can handle in a second before raising an event. The default is 300 reads/ second.
Raise event if disk writes exceed the threshold?	Select **Yes** to raise an event if the number of writes per second to the physical disks exceeds the threshold you set. The default is unselected.
Event severity when disk writes exceed the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of disk writes to a physical disk exceeds the threshold. The default is 15.
Threshold - Maximum disk writes	Specify the maximum count of write operations that a physical disk can handle in a second before raising an event. The default is 300 writes/ second.
Data Collection	
Collect data for disk total IOs?	Select **Yes** to collect the total input and output data of physical disks for charts and reports. The default is unselected.
Collect data for disk reads?	Select Yes to collect the total read data of physical disks for charts and reports. The default is unselected.
Collect data for disk writes?	Select Yes to collect the total write data of physical disks for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the IO operations of the specified physical disks. ◆ **Exclusion:** If you do not want to monitor the IO operations of the specified physical disks.
Include or exclude physical disks	Specify a list of physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see "Specifying Inclusion or Exclusion Filters" on page 29.

Description	How to Set It

Full path to file containing list of physical disks to include or exclude	Specify the path of the file that lists the physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	◆ Use commas with no spaces to separate the disks. For example: `PhysicalDisk01`,`PhysicalDisk02`,`PhysicalDisk03`
	◆ List the disks on separate lines. For example:
	`PhysicalDisk01`
	`PhysicalDisk02`
	`PhysicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

PhysicalDiskResponseTime

Use this Knowledge Script to monitor the response time, IO rate, wait time, and queue depth of physical disks in an array. This script raises an event if this job fails to get the metrics on response time. This script also raises an event if the threshold exceeds for response rate, IO rate, wait time, or the queue depth. This script also generates data streams for these metrics.

This Knowledge Script applies only to SAN environment.

Resource Objects

Array physical disks

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	

Description	How to Set It
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get disk metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get metrics of the physical disk. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get disk metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get metrics about the physical disk. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want or do not want to monitor physical disk response time. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want to or do not want to monitor physical disk response time. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if disk response time exceeds the threshold?	Select **Yes** to raise an event if the physical disk response time exceeds the threshold you set. The default is Yes.
Event severity when disk response time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the physical disk response time exceeds the threshold. The default is 15.
Threshold - Maximum disk response time	Specify the maximum time that a physical disk should take to respond before raising an event. The default is 30 milliseconds.
Raise event if disk IO rate exceeds the threshold?	Select **Yes** to raise an event if the number of IO rate of a physical disk per second exceeds the threshold you set. The default is unselected.
Event severity when disk IO rate exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the number of IO rate of a physical disk per second exceeds the threshold. The default is 15.
Threshold - Maximum disk IO rate	Specify the maximum number of IO rate that a physical disk can handle in a second before raising an event. The default is 300 IOs/second.
Raise event if disk wait time exceeds the threshold?	Select **Yes** to raise an event if the physical disk wait time exceeds the threshold you set. The default is unselected.

Description	How to Set It
Event severity when disk wait time exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the physical disk wait time exceeds the threshold. The default is 15.
Threshold - Maximum disk wait time	Specify the maximum time that a physical disk IO request can wait for a response before raising an event. The default is 5 milliseconds.
Raise event if disk queue depth exceeds the threshold?	Select **Yes** to raise an event if the physical disk IO requests that are waiting in the queue for response exceed the threshold you set. The default is unselected. As the queue depth increases, the average wait time also increases because the requests that are waiting in the queue have to run first.
Event severity when disk queue depth exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the physical disk IO requests that are in the queue for response exceed the threshold. The default is 15.
Threshold - Maximum disk queue depth	Specify the maximum requests for physical disk that can be queued up for response before raising an event. The default is 5 requests.
Data Collection	
Collect data for disk response time?	Select **Yes** to collect the IO response time of physical disks for charts and reports. The default is unselected.
Collect data for disk IO rate?	Select Yes to collect the total IO rate of physical disks for charts and reports. The default is unselected.
Collect data for disk wait time?	Select Yes to collect the wait time that a physical disk request is waiting for response, for charts and reports. The default is unselected.
Collect data for disk queue depth?	Select Yes to collect the number of physical disk requests that are queued up for response, for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the response time of the specified physical disks. ◆ **Exclusion:** If you do not want to monitor the response time of the specified physical disks.
Include or exclude physical disks	Specify a list of physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Description	How to Set It

Full path to file containing list of physical disks to include or exclude	Specify the path of the file that lists the physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<`*`path to file`*`>` rather than `\\<`*`server`*`>\D$\<`*`path to file`*`>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the disks. For example: `PhysicalDisk01,PhysicalDisk02,PhysicalDisk03`
	- List the disks on separate lines. For example:
	`PhysicalDisk01`
	`PhysicalDisk02`
	`PhysicalDisk03`
	All regular expressions are supported.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

StorageArrayUtilization

Use this Knowledge Script to monitor the space utilization of physical disks in an array. This script raise event for conditions such as when the job cannot get the physical disk array capacity metrics of when the used space in an array exceeds the threshold you set. You can set severities to indicate the importance of each type of event. This script collects data for array capacity, array utilization and array free space in a storage environment.

This Knowledge Script applies to SAN or NAS environments.

Resource Objects

Storage Array

NOTE: This Knowledge Script runs only on the storage array root object and not on the individual disks.

Default Schedule

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

Setting Parameter Values

Set the following parameters as needed:

Description	How to Set It
General Settings	
Job Failure Notification	
Event severity when job fails	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job fails. The default is 5.
Raise event if job failed to get array metrics?	Select **Yes** to raise an event if the Knowledge Script job is not able to get the capacity of the physical disk array. The default is Yes.
Raise event only once?	Select **Yes** to raise the *Metric not available* event only once if the Knowledge Script job is not able to obtain any of the selected metrics of the monitored object. The default is Yes.
Event severity when job failed to get array metrics	Set the event severity, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to get data about the physical disk array capacity. The default is 5.
Raise event if XML is modified?	Select **Yes** to raise an event if the XML for this Knowledge Script is modified. The default is Yes.
Event severity when XML is modified	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the XML for this Knowledge Script is modified. The default is 22.
Raise event if full path to file containing filters does not exist?	Select **Yes** to raise an event if the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want to or do not want to get the physical disk capacity. The default is unselected.
Event severity when full path to file containing filters does not exist	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the Knowledge Script job is not able to locate the file that specifies the list of disks for which you either want to or do not want to monitor physical disk capacity. The default is 35.
Event Details	
Event detail format	Select whether to view event details in an HTML table or in plain text. The default is HTML Table.
Event Notification	
Raise event if array utilization exceeds the threshold?	Select **Yes** to raise an event if the physical disk array utilization exceeds the threshold you set. The default is Yes.
Event severity when array utilization exceeds the threshold	Set the event severity level, from 1 to 40, to indicate the importance of an event in which the physical disk array utilization exceeds the threshold. The default is 15.
Threshold - Maximum array utilization	Specify the percentage up to which the physical disk array space can be utilized before raising an event. The default is 85%.

Description	How to Set It
Include summary for individual disks or aggregates in event details?	Select **Yes** to display the summary of the utilized space of all the physical disks in an array or the aggregates of an array. On EMC storage device, selecting this parameter displays the summary of all the physical disks in an array, their capacity, used and free space available in the detail message. On NetApp storage device, selecting this parameter displays only the aggregates of the utilized space. The default is unselected.
Data Collection	
Collect data for array capacity?	Select **Yes** to collect data for the physical disk array capacity, for charts and reports. This data is the actual consumable space that is available in an array. The default is unselected.
Collect data for array utilization?	Select **Yes** to collect data for the utilized space in a physical disk array, for charts and reports. The default is unselected.
Include summary for individual disks or aggregates in data details	Select **Yes** to display the details of the utilized space of all the physical disks in chart or reports. On EMC storage device, selecting this parameter displays the summary of all the physical disks in an array, their capacity, used and free space available in the data detail. On NetApp storage device, selecting this parameter displays only the aggregates of the utilized space. The default is unselected.
Collect data for free array space?	Select **Yes** to collect data for the free space available in a physical disk array, for charts and reports. The default is unselected.
Inclusion or Exclusion Filter	
Inclusion or exclusion criteria	Select one of the following criteria: ◆ **Inclusion:** If you want to monitor the array utilization of the specified physical disks. ◆ **Exclusion:** If you do not want to monitor the array utilization of the specified physical disks.
Include or exclude physical disks	Specify a list of physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. Use commas with no spaces to separate the devices. For more information on inclusion or exclusion filters, see “Specifying Inclusion or Exclusion Filters” on page 29.

Description	How to Set It

Full path to file containing list of physical disks to include or exclude	Specify the path of the file that lists the physical disks that you want to include or exclude from monitoring based on your selection in the *Inclusion or exclusion criteria* parameter. You can also click **Browse** and navigate to the file.
	Use the local path to the file rather than the UNC path. For example, use `D:\<path to file>` rather than `\\<server>\D$\<path to file>`.
	To list the devices in the file, do one of the following:
	- Use commas with no spaces to separate the devices. For example: `PhysicalDisk01`,`PhysicalDisk02`,`PhysicalDisk03`
	- List the disks on separate lines. For example:
	`PhysicalDisk01`
	`PhysicalDisk02`
	`PhysicalDisk03`
	All regular expressions are supported. For examples, see "Include or exclude array physical disks" on page 49.

Case-sensitive inclusion or exclusion	Select **Yes** to use case-sensitive pattern matching to include or exclude resources from monitoring based on the selected criteria. The default is unselected.

4 Troubleshooting AppManager for Hardware

This chapter describe how to troubleshoot AppManager for Hardware.

AppManager agent and SAN device are not responding

If the CIM server is not responding to any query from the Knowledge Script, the Knowledge Script hangs and no data or events are reported.

To resolve the issue, restart the CIM server service on the SMI-S Provider machine.