NetIQ® AppManager® for Siemens ServerView

Management Guide

February 2012

Legal Notice

Contents

About this Book and the Library

The NetIQ AppManager for Siemens ServerView 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 for Siemens ServerView provides system administrators with a central, easy-to-use console to view critical server and application resources across the enterprise. With AppManager for Siemens ServerView, 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 Siemens ServerView library is available in Adobe Acrobat (PDF) format from the NetIQ Web site: www.netiq.com/support/am/extended/documentation/default.asp?version=AMDocumentation.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measureable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please 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
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, 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, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

1 Introducing AppManager for Siemens ServerView

AppManager for Siemens ServerView lets you monitor the operation and performance of Siemens ServerView through the same console you use to monitor your Windows and UNIX environments.

The Knowledge Scripts in the Siemens ServerView category raise events in the AppManager Operator Console or in the Control Center Console when problems arise. For example, the Knowledge Scripts raise events if the voltage level drops below or exceeds the normal operating threshold, or if a service is not running. These Knowledge Scripts collect information about Siemens servers, which you can for trend analysis and reporting. With AppManager for Siemens ServerView, you can monitor the following functions:

- Performance and availability of key Siemens ServerView components and major services, including service status, and the status of key performance counters
- Thermal status
- Power supply and voltage status of the computer
- PRIMERGY server-related services, including SNMP
- Logical disk and physical device status on MYLEX RAID Controllers
- Health of the network interface card
- Network interface card for packets received and transmitted with errors
- CPU performance
- SCSI and IDE physical device status
- Adaptec RAID controller status
- Memory module status
- Logical disk and physical device status on LSI MegaRAID controllers
- Fan and voltage status

2 Installing AppManager for Siemens ServerView

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

This 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.

2.1 System Requirements

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

AppManager for Siemens ServerView has the following system requirements:

Software/Hardware	Version
NetIQ AppManager installed on the AppManager repository (QDB) computers, and all agent and console computers	7.0, at minimum For enhanced support of Windows Server 2008, hotfix 71704 is recommended. For more information, see the AppManager Suite Hotfixes Web page
Microsoft Windows operating system on the agent computer	One of the following: ◆ 32-bit or 64-bit Windows Server 2003 R2 with SP2 ◆ 32-bit or 64-bit Windows Server 2008 with SP2 or Windows Server 2008 R2
AppManager for Microsoft Windows installed on the repository, agent, and console computers	7.5.208.0, at minimum
Siemens ServerView Agent on the agent computer	One of the following: ◆ Siemens ServerView Agent for Windows 2003, versions 4.3 through 4.9 ◆ Siemens ServerView Agent for Windows 2008, versions 4.6.1 through 4.9

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

2.2 Permissions for Running Knowledge Scripts

AppManager for Siemens ServerView requires that the NetIQ AppManager Client Resource Monitor (`netiqmc`) and the NetIQ AppManager Client Communication Manager (`netiqccm`) agent services have the following permissions:

- Ability to log on as a service.
- Membership in the Domain Admin Group.

By default, the setup program configures the agent to use the Windows Local System account.

To update the agent services:

1. Start the Services Administrative Tool from the Administrative Tools folder in the Control Panel.
2. Right-click the **NetIQ AppManager Client Communication Manager** (`netiqccm`) service in the list of services, and select **Properties**.
3. On the Logon tab, specify the appropriate account to use, then click **OK**.
4. Repeat steps 2 through 4 for the **NetIQ AppManager Client Resource Monitor** (`netiqmc`) service.
5. Restart both services.

2.3 Installing the Module

The setup program automatically identifies and updates all relevant AppManager components on a computer. Therefore, run the setup program only once on any computer. The pre-installation check also runs automatically when you launch the setup program.

You can install the module in one of the following ways:

- Run the module setup program, `AM70-Siemens-7.x.x.0.msi`, which you downloaded from the Web. Save the module setup files on the distribution computer, and then delete the older versions of the module setup files. For more information, see the *Installation Guide for AppManager.*
- Use Control Center to install the module on the remote computer where an agent is installed. Ensure you check in the installation package, which is the `.XML` file included with the module setup program. For more information about the `.XML` file, see the *AppManager for Siemens ServerView Readme*. For more information, see the *Control Center User Guide for AppManager*.

To install the module:

1. Run the module setup program on all repository computers to install the Knowledge Scripts and reports. For repositories running in a clustered environment, run the setup program on the node that currently owns the cluster resource.
2. Install the module on the Siemens ServerView computer you want to monitor. Use one of the following methods:
   - Run the module setup program.
   - Use Control Center to deploy the installation package.
3. Run the module setup program on all console computers to install the Help.
4. If you have not already discovered Siemens ServerView resources, run the Discovery_Siemens Knowledge Script on all agent computers where you installed the module.

After the installation has completed, you can find a record of problems encountered in the `Siemens_Install.log` file, located in the `\NetIQ\Temp\NetIQ_Debug\<`*ServerName*`>` folder.

2.4 Silently Installing the Module

To silently (without user intervention) install a module, create an initialization file (`.ini`) for this module that includes the required property names and values to use during the installation.

To create and use an initialization file for a silent installation:

1. Create a new text file and change the filename extension from `.txt` to `.ini`.
2. To specify the community string required to access hardware resources, include the following text in the `.ini` file:

   `MO_CommunityString=`*`string name`*

   where *string name* is the name of the community string, such as `public`.
3. Save and close the `.ini` file.
4. Run the following command from the folder in which you saved the module installer:

   `msiexec.exe /i "AM70-Siemens-7.`*`x.x`*`.0.msi" /qn MO_CONFIGOUTINI="`*`full path to the initialization file`*`"`

   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-Siemens-7.`*`x.x`*`.0.msi.log"`

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

2.5 Upgrading Knowledge Script Jobs

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

- Use the AMAdmin_UpgradeJobs Knowledge Script.
- Use the Properties Propagation feature.

2.5.1 Running AMAdmin_UpgradeJobs

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

Upgrading jobs to use the most recent script version allows the jobs to take advantage of the latest script logic while maintaining existing parameter values for the job.

For more information, see the Help for the AMAdmin_UpgradeJobs Knowledge Script.

2.5.2 Propagating Knowledge Script Changes

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

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

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

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

Propagating Changes to Ad Hoc Jobs

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

To propagate changes to ad hoc Knowledge Script jobs:

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

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

Propagating Changes to Knowledge Script Groups

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

After you propagate script changes to Knowledge Script Group members, you can propagate the updated Knowledge Script Group members to associated running jobs. For more information, see "Propagating Changes to Ad Hoc Jobs" on page 14.

To propagate Knowledge Script changes to Knowledge Script Groups:

1. In the Knowledge Script view, select the Knowledge Script Group for which you want to propagate changes.
2. On the KS menu, select **Properties propagation** > **Ad Hoc Jobs**.
3. ***If you want to exclude a Knowledge Script member from properties propagation,*** deselect that member from the list in the Properties Propagation dialog box.

4 Select the components of the Knowledge Script that you want to propagate to associated Knowledge Script Groups:

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

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

3 Siemens ServerView Knowledge Scripts

The Siemens category provides the following Knowledge Scripts for monitoring Siemens PRIMERGY servers running ServerView. To access more information about any Knowledge Script, select the Knowledge Script and press **F1** in the Knowledge Script view of Control Center. Or in the Operator Console, click any Knowledge Script in the Knowledge Script pane and press **F1**.

Knowledge Script	What It Does
AdaptecLogicalDriveStatus	Monitors the status of logical drives on an Adaptec RAID controller.
AdaptecPhysicalDiskStatus	Monitors the status of physical disks on an Adaptec RAID controller.
AdaptecRAIDControllerStatus	Monitors the status of Adaptec RAID controllers and any attached hard drives.
ArrayLogicalDriveStatus	Monitors the status of a logical drive on a MYLEX RAID controller.
ArrayPhysicalDiskHardErrors	Monitors the number of hardware errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskMiscErrors	Monitors the number of miscellaneous errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskParityErrors	Monitors the number of parity errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskSoftErrors	Monitors the number of software errors on a disk connected to a MYLEX RAID controller.
ArrayPhysicalDiskStatus	Monitors the status of a disk connected to a MYLEX RAID controller.
CPU	Monitors the status of one or more CPUs.
Fan	Monitors the status of individual fans.
HealthCheck	Monitors ServerView-related services.
IDEPhysicalDevice	Monitors discovered IDE physical devices, such as disk or CD-ROM devices.
LSILogicalDriveHealth	Monitors the physical device status, errors, and S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) status.
LSIPhysicalDeviceHealth	Monitors physical disk status.
MemoryModule (page 34)	Monitors the status of memory modules on the system board.
NICError	Monitors the network interface card for transmission errors.
NICFail	Checks the status of the network interface card.

Knowledge Script	What It Does
OverallCondition	Monitors the overall condition of discovered subsystems, for example, mass storage, system board, power supply, and environment.
PowerSupply	Monitors the status of one or more internal power supply units.
SCSIPhysicalDevice (page 39)	Monitors discovered SCSI physical devices, such as disk or CD-ROM devices.
Temperature	Monitors the server's thermal environment and the status of the server's temperature sensors.
Voltage	Monitors the voltage levels found on the system board.
Discovery_Siemens	Discovers Siemens ServerView configuration and resources.

3.1 AdaptecLogicalDriveStatus

Use this Knowledge Script to monitor the status of logical drives on an Adaptec RAID controller. This Knowledge Script raises an event if the logical drive is degraded, building, rebuilding, or has failed.

This Knowledge Script also raises an event if the status of the drive is `other`, which includes invalid, verifying, formatting, formatCertifying, notCreated, verifyingFixing, abortActivity, and reserved.

In addition, the Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.1.1 Resource Objects

Adaptec Logical Drive folder or Adaptec Logical Drive icon.

3.1.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.1.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the logical drive is operating properly ◆ **50** if the logical drive is degraded, building, or rebuilding (this value is also returned to indicate a status of `other`) ◆ **0** if the logical drive has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...logical drive failed**. The default is 5 (red event indicator). ◆ **...logical drive degraded**. The default is 15 (yellow event indicator). ◆ **...logical drive building or rebuilding**. The default is 20 (yellow event indicator). ◆ **...logical drive at other status**. The default is 20 (yellow event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.2 AdaptecPhysicalDiskStatus

Use this Knowledge Script to monitor the status of physical disks on an Adaptec RAID controller. This Knowledge Script raises an event if the disk is building, rebuilding, has issued a warning, or has failed.

The Knowledge Script also raises an event if the status of the disk is `other`, which includes invalid, verifying, formatting, formatCertifying, notCreated, verifyingFixing, abortActivity, and reserved.

In addition, the Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.2.1 Resource Objects

Adaptec Physical Disk folder or Adaptec Physical Disk icon.

3.2.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.2.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the physical disk is operating properly ◆ **50** if the physical disk has issued a warning, is building, or rebuilding (this value is also returned to indicate a status of `other`) ◆ **0** if the physical disk has failed or is missing The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...physical disk failed or missing**. The default is 5 (red event indicator). ◆ **...physical disk degraded or warning**. The default is 15 (yellow event indicator). ◆ **...physical disk building or rebuilding**. The default is 20 (yellow event indicator). ◆ **...physical disk at other status**. The default is 20 (yellow event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.3 AdaptecRAIDControllerStatus

Use this Knowledge Script to monitor the status of Adaptec RAID controllers and any attached hard drives. This Knowledge Script raises an event if the controller or an attached hard drive has failed or issued an error.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.3.1 Resource Objects

Adaptec RAID Controller folder or Adaptec RAID Controller icon.

3.3.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.3.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the controller and attached drives are operating properly ◆ **50** if the controller or an attached drive has issued an error ◆ **0** if the controller or an attached drive has failed, is invalid, or is not supported The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...RAID Controller failed**. The default is 5 (red event indicator). ◆ **...RAID Controller error**. The default is 15 (yellow event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.4 ArrayLogicalDriveStatus

Use this Knowledge Script to monitor the status of a logical drive on a MYLEX RAID controller. A *logical drive* is a combination of partitions on physical disks. If the logical drive status is dead or unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.4.1 Resource Objects

Array Logical Drive folder or Array Logical Drive icon.

3.4.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.4.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the logical drive is operating properly ◆ **50** if the logical drive status is unknown ◆ **0** if the logical drive is dead The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...logical drive critical**. The default is 5 (red event indicator). ◆ **...logical drive offline or status unknown**. The default is 25 (blue event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.5 ArrayPhysicalDiskHardErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of hardware errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent hardware errors, replace the defective disk.

3.5.1 Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

3.5.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.5.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of hardware errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for hardware errors	Enter a threshold for the maximum number of hardware errors in a monitoring interval. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...threshold exceeded**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.6 ArrayPhysicalDiskMiscErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of miscellaneous errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent miscellaneous errors, replace the defective disk.

3.6.1 Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

3.6.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.6.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of miscellaneous errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for miscellaneous errors	Enter a threshold for the maximum number of miscellaneous errors in a monitoring interval. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...threshold exceeded**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.7 ArrayPhysicalDiskParityErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. At certain RAID levels, data blocks are protected by redundant data (so-called parity blocks). This Knowledge Script shows a count of the errors detected during this procedure.

If the number of parity errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences frequent parity errors, check cabling and termination. This error may be caused by:

- Improper parity generation and checking
- Cable failure
- Improper cable length
- Improper or missing cable termination
- Interference from another device

3.7.1 Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

3.7.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.7.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of parity errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for parity errors	Specify the maximum number of parity errors that can occur during a monitoring interval before an event is raised. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...threshold exceeded**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.8 ArrayPhysicalDiskSoftErrors

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If the number of software errors exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a disk experiences a software error, run Siemens consistency check. If the disk experiences frequent software errors, replace the defective disk.

3.8.1 Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

3.8.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.8.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of software errors encountered by a physical disk. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for software errors	Specify the maximum number of software errors that can occur during a monitoring interval before an event is raised. The default is 5.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...threshold exceeded**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.9 ArrayPhysicalDiskStatus

Use this Knowledge Script to monitor the status of the physical disks connected to a MYLEX RAID controller. If a disk is dead or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.9.1 Resource Objects

Array Physical Disk folder or individual Array Physical Disk icon.

3.9.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.9.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the physical disk is operating properly ◆ **50** if the physical disk status is rebuilding ◆ **30** if the physical disk status is unknown ◆ **0** if the physical disk is dead The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...physical disk dead** (the disk status is `dead`, the disk does not exist, the disk exists but is not powered on, the disk was deactivated by the controller due to an error). The default is 5 (red event indicator). ◆ **...physical disk rebuilding**. The default is 18 (yellow event indicator). ◆ **...physical disk status unknown**. The default is 25 (yellow event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.10 CPU

Use this Knowledge Script to monitor the status of one or more CPUs. If a CPU fails or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.10.1 Resource Objects

CPU Folder or individual CPU icons.

3.10.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.10.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.

Parameter	How to Set It
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the CPU status is OK ◆ **30** if the CPU status is unknown ◆ **0** if the CPU is in any other state The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...CPU failed**. The default is 5 (red event indicator). ◆ **...prefailure warnings**. The default is15 (yellow event indicator). ◆ **...CPU status unknown**. The default is 25 (blue event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.11 Fan

Use this Knowledge Script to monitor the status of individual fans. If a fan is not operating properly or if its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.11.1 Resource Objects

Fan Folder or individual Fan icons.

3.11.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.11.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the fan status and speed. The default is n.

Parameter	How to Set It
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...fan has failed**. The default is 5 (red event indicator). ◆ **...fan failure predicted**. The default is15 (yellow event indicator). ◆ **...redundant fan failed**. The default is 15 (yellow event indicator). ◆ **...fan status is unknown**. The default is 25 (blue event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.12 HealthCheck

Use this Knowledge Script to monitor all ServerView-related services. If a ServerView-related service is not running, this Knowledge Script raises an event, performs the action you specify in the Actions tab of the Knowledge Script, and automatically restarts the service.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

In order for SNMP errors to generate an event, you need to run this Knowledge Script in the TreeView on an object at the Siemens Server level or above.

3.12.1 Resource Objects

Siemens Server or any Siemens Service icon.

3.12.2 Default Schedule

The default interval for this Knowledge Script is **Every 5 minutes**.

3.12.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Auto-start service?	Set to **y** to automatically restart stopped services. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the status of ServerView-related services. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.

Parameter	How to Set It
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...service down; restart failed**. The default is 5 (red event indicator). ◆ **...service down; restart succeeded**. The default is 25 (blue event indicator). ◆ **...service down; don't restart**. The default is 18 (yellow event indicator). ◆ **...SNMP down**. The default is 5 (red event indicator).

3.13 IDEPhysicalDevice

Use this Knowledge Script to monitor discovered IDE physical devices such as, disk or CD-ROM devices. If a device fails, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.13.1 Resource Objects

IDE folder or individual IDE drives.

3.13.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.13.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set it
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns 100 if the IDE device is operating properly or 0 if the IDE device is dead. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...IDE device failure**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.14 LSILogicalDriveHealth

Use this Knowledge Script to monitor logical drive status on LSI MegaRAID controllers. If the logical drive status is Rebuilding, Failed, Degraded, or Unknown, an event is raised.

3.14.1 Resource Objects

LSI Logical Drive folder or individual Logical Drive icon

3.14.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.14.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set it
General Settings	
Community string	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Job failure event notification	
Event severity for SNMP or ServerView service down	Set the severity level from 1 to 40 to indicate the importance on an event in which the SNMP or ServerView service is down. The default is 10.
Event Notification	
Status Settings	
Raise event when status of logical drive is Failed?	Select Yes to raise an event when the status of the logical drive is Failed. The default is Yes.
Event severity when status of logical drive is Failed	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Failed. The default is 5.
Raise event when status of logical drive is Degraded or Rebuilding	Select Yes to raise an event when the status of the logical drive is Degraded or Rebuilding. The default is Yes.
Event severity when status of logical drive is Degraded or Rebuilding	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Degraded or Rebuilding. The default is 18.
Raise event when status of logical drive is Unknown	Select Yes to raise an event when the status of the logical drive is Unknown. The default is unselected.
Event severity when status of logical drive is Unknown	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the logical drive is Unknown. The default is 35.
Data Collection	

Parameter	How to Set it
Collect data for logical drive status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the operational status of the logical drive at each monitoring interval. The default is unselected.

3.15 LSIPhysicalDeviceHealth

Use this Knowledge Script to monitor physical device status, device errors, and S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) status on LSI Mega RAID controllers. If the physical device status is Rebuilding, Failed, or Unknown or if the number of errors exceed the threshold you set, an event is raised. An event is also raised if failure is predicted for a physical device or the S.M.A.R.T status is not known.

3.15.1 Resource Objects

Disk Array folder or LSI Physical Disk folder or individual Physical disk icon

3.15.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.15.3 Setting Parameter Values

Set the following parameters as needed

Parameter	How to Set it
General Settings	
community string name	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Job failure event notification	
Event severity for SNMP or ServerView service down	Set the severity level from 1 to 40 to indicate the importance on an event in which SNMP or the ServerView service is down. The default is 10.
Event Notification	
Status Settings	
Raise event when status of physical device is Rebuilding?	Select Yes to raise an event when the status of the physical device is Rebuilding. The default is Yes.
Event severity when status of physical device is Rebuilding	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Rebuilding. The default is 15.
Raise event when status of physical device is Failed?	Select Yes to raise an event when the status of the physical device is Failed. The default is Yes.

Parameter	How to Set it
Event severity when status of physical device is Failed	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Failed. The default is 5.
Raise event when status of physical device is Unknown	Select Yes to raise an event when the status of the physical device is Unknown. The default is unselected.
Event severity when status of physical device is Unknown	Set the severity level from 1 to 40 to indicate the importance of an event in which the status of the physical device is Unknown. The default is 35.
S.M.A.R.T. Status Settings	
Raise event when failure is predicted for physical device?	Select Yes to raise an event when failure is predicted for the physical device. The default is Yes.
Event severity when failure is predicted for physical device	Set the severity level from 1 to 40 to indicate the importance of an event in which failure is predicted for the physical device. The default is 15.
Raise event when S.M.A.R.T. Status of physical device is not available?	Select Yes to raise an event when the S.M.A.R.T. status for the physical device is not available. The default is unselected.
Event severity when S.M.A.R.T. Status of physical device is Not Available.	Set the severity level from 1 to 40 to indicate the importance of an event in which the S.M.A.R.T status of the physical device is Not Available. The default is 5.
Error Settings	
Raise event when physical device errors exceed threshold?	Select Yes to raise an event if the number of physical device errors exceeds the threshold you set. The default is Yes.
Threshold for device errors	Specify the maximum number of errors that can occur for a physical device before an event is raised. The default is 5.
Event severity when device errors exceed threshold	Set the severity level from 1 to 40 to indicate the importance of an event in which physical device errors exceed the threshold you set. The default is 15.
Data Collection	
Collect data for physical device status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the operational status of the device at each monitoring interval. The default is unselected.
Collect data for physical device errors?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the number of errors of the device at each monitoring interval. The default is unselected.
Collect data for physical device S.M.A.R.T. status?	Set to **Yes** to collect data for charts and reports. If set to Yes, this Knowledge Script records the S.M.A.R.T. status of the device at each monitoring interval. The default is unselected.

3.16 MemoryModule

Use this Knowledge Script to monitor the status of memory modules on the system board. If a memory module fails or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If a memory module experiences frequent errors, locate and replace the defective memory module.

3.16.1 Resource Objects

Memory Module icon.

3.16.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.16.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the memory module is operating properly ◆ **50** if the memory module status is unknown ◆ **0** if the memory module has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...memory module failed**. The default is 5 (red event indicator). ◆ **...status unknown**. The default is 25 (blue event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.17 NICError

Use this Knowledge Script to monitor network interface transmission errors. Both input and output errors are reported and evaluated against the thresholds you specify. If the number of network interface errors per minute exceeds the threshold, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.17.1 Resource Objects

Network Interface Card (NIC) folder or individual NIC icons.

3.17.2 Default Schedule

The default interval for this Knowledge Script is **Every 30 minutes**.

3.17.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the number of input and output errors per minute at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Maximum threshold for input errors per minute	Specify the maximum number of input errors that can occur per minute before an event is raised. The default is 2 errors per minute.
Maximum threshold for output errors per minute	Enter a threshold for the maximum number of output errors per minute. The default is 4 errors per minute.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...SNMP or ServerView service down**. The default is 9 (red event indicator). ◆ **...input error threshold exceeded**. The default is 10 (red event indicator). ◆ **...output error threshold exceeded**. The default is 10 (red event indicator).

3.18 NICFail

Use this Knowledge Script to monitor the status of the network interface. This Knowledge Script checks whether the network interface subsystem is down when the administrator has indicated it should be in the "up" state. If the network interface subsystem is down, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.18.1 Resource Objects

Network Interface Card (NIC) folder or individual NIC icons.

3.18.2 Default Schedule

The default interval for this Knowledge Script is **Every 5 minutes**.

3.18.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the operational status of the network interface subsystem at each monitoring interval. The default is n.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...network interface subsystem is down**. The default is 6 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 9 (red event indicator).

3.19 OverallCondition

Use this Knowledge Script to monitor the overall condition of the discovered subsystems on the server such as, mass storage, system board, power supply, and environment. If a subsystem is not operating properly, this Knowledge Script raises an event.

NOTE: You cannot customize the parameters to specify what subsystems need to be monitored by this Knowledge Script.

When this Knowledge Script raises an event, the event message does not indicate the subsystem having a problem. It displays a generic message that some of the subsystems are not working properly.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

If the overall condition of a device degrades, use the Siemens-related Knowledge Scripts to identify the source of the problem. To monitor Siemens ServerView services, see HealthCheck.

3.19.1 Resource Objects

Siemens Server.

3.19.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.19.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data. If set to y, this Knowledge Script returns: ◆ **100** if the overall condition is normal ◆ **50** if the overall condition has degraded ◆ **0** if the server encountered an error The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...device error or failed**. The default is 5 (red event indicator). ◆ **...unknown subsystem status**. The default is 10 (red event indicator). ◆ **...device degraded**. The default is 15 (yellow event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.20 PowerSupply

Use this Knowledge Script to monitor the status of one or more internal power supply units. If a power supply unit is not operational or its status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.20.1 Resource Objects

Power Supply folder or individual Power Supply icons.

3.20.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.20.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns: ◆ **100** if the power supply is operating properly ◆ **30** if the power supply status is unknown ◆ **0** if the power supply has failed The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...power supply failed**. The default is 5 (red event indicator). ◆ **...power supply status unknown**. The default is 25 (blue event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.21 SCSIPhysicalDevice

Use this Knowledge Script to monitor discovered SCSI physical devices such as, disk or CD-ROM devices. If a device fails, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.21.1 Resource Objects

SCSI folder or individual SCSI icons.

3.21.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.21.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script returns 100 if the SCSI device is operating properly or 0 if the SCSI device has failed. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...SCSI physical device failure**. The default is 5 (red event indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.22 Temperature

Use this Knowledge Script to monitor the thermal environment and the status of the thermal sensors of the server. If a sensor is operating out of normal temperature range, or if the thermal status is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

3.22.1 Resource Objects

Temperature folder or individual Temperature icons.

3.22.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.22.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the temperature (in degrees Celsius) at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...temperature abnormal or sensor failed**. The default is 15 (yellow event indicator). ◆ **...temperature critical**. The default is 5 (red event indicator). ◆ **...temperature status unknown**. The default is 25 (blue indicator). ◆ **...SNMP or Siemens ServerView service down**. The default is 10 (red event indicator).

3.23 Voltage

Use this Knowledge Script to monitor the voltage level for a Siemens server. This Knowledge Script monitors the status of the voltage sensors on the system board. If a sensor detects that the voltage level has dropped below or exceeded the normal operating threshold, or the voltage level is unknown, this Knowledge Script raises an event.

In addition, this Knowledge Script raises an event if SNMP is not operating or there is a problem retrieving a MIB (Management Information Base) variable value.

The server system defines the voltage levels for normal operation internally.

3.23.1 Resource Objects

Voltage folder or individual Voltage icons.

3.23.2 Default Schedule

The default interval for this Knowledge Script is **Every 10 minutes**.

3.23.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Event?	Set to **y** to raise events. The default is y.
Collect data?	Set to **y** to collect data for charts and reports. If set to y, this Knowledge Script records the voltage level for each voltage sensor at each monitoring interval. The default is n.
Community	Specify the community string name. If you do not enter a value, the script uses the community string name supplied by Security Manager. If no entry for the community string name exists in Security Manager, the script uses the default value `public`.
Event severity level for...	Set the event severity level, from 1 to 40, to indicate the importance of: ◆ **...voltage is too high or low**. The default is 5 (red event indicator). ◆ **...voltage status unknown**. The default is 25 (blue indicator). ◆ **...SNMP or ServerView service down**. The default is 10 (red event indicator).

3.24 Discovery_Siemens

Use this Knowledge Script to discover the resource and configuration information. This Knowledge Script requires SNMP to be running on the computer you are discovering. If a required service is not found or is not running, the Discovery job fails with a "Not a Siemens Server" event.

Because SNMP is not installed on Siemens servers by default, you may need to install it and restart the server before you can run this Knowledge Script successfully.

3.24.1 Resource Objects

Siemens ServerView servers.

3.24.2 Default Schedule

The default schedule for this Knowledge Script is **Run once**.

3.24.3 Setting Parameter Values

Set the following parameters as needed:

Parameter	How to Set It
Raise event if discovery succeeds?	This Knowledge Script always raises an event when the job fails for any reason. In addition, you can set this parameter to **y** to raise an event when the job succeeds. The default is n.

Parameter	How to Set It
SNMP community string name	Enter the SNMP community string name to use. The default is the community string name entered in the AppManager for Siemens ServerView Security Manager or public if no community string name has been entered.
Event severity when discovery...	Set the event severity level, from 1 to 40, to reflect the importance when the job: ◆ **...succeeds**. If you set this Knowledge Script to raise an event when the job succeeds, set the event severity level for a successful discovery. The default is 25 (blue event indicator). ◆ **...fails**. The default is 5 (red event indicator). ◆ **...partially succeeds**. Set the event severity level for a discovery that returns some data but also generates warning messages. The default is 10 (red event indicator). ◆ **...is not applicable**. This type of failure usually occurs when the target computer does not have Siemens ServerView installed. The default is 15 (yellow event indicator). **NOTE**: If required services, such as SNMP, are not running on the computer you are discovering, you may see a severity 15 event (Not a Siemens Server). If you see this type of event, see the detail message for more information about what caused the discovery to fail.