



# FUJITSU Software ServerView

Windows Server Integration Pack V8.5 for MS SCOM



Copyright 2019 FUJITSU LIMITED

All hardware and software names used are trademarks of their respective manufacturers.

All rights, including rights of translation, reproduction by printing, copying or similar methods, in part or in whole, are reserved.

Offenders will be liable for damages.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Delivery subject to availability. Right of technical modification reserved.



---

# Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Purpose and target groups .....	1
1.2	Changes since the last edition .....	2
1.3	ServerView Suite link collection .....	2
1.4	Documentation for ServerView Suite .....	4
1.5	Notational Conventions .....	4
<b>2</b>	<b>Integration requirements .....</b>	<b>5</b>
2.1	Setting trap severities for ServerView Agents .....	6
2.2	Updating ServerView Agents.....	6
<b>3</b>	<b>Installation and uninstallation.....</b>	<b>7</b>
3.1	Installing ServerView Integration Pack.....	7
3.1.1	Installed files.....	7
3.1.2	Importing Management Packs.....	8
3.2	Update to a new version.....	9
3.3	Updating the ServerView Library Management Packs .....	9
3.4	Uninstalling ServerView Integration Pack .....	10
3.4.1	Removing the Management Packs.....	10
<b>4</b>	<b>Properties of the ServerView Windows Server Integration Pack .....</b>	<b>11</b>
4.1	Management Packs .....	11
4.2	PRIMERGY server computer groups .....	13
4.3	Discovering and monitoring PRIMERGY servers .....	14
4.3.1	Displayed properties of recognized PRIMERGY servers.....	14
4.3.2	Health state of a PRIMERGY server .....	15
4.3.3	Virtual machine is recognized as a PRIMERGY server.....	16
4.4	Discovering and monitoring server components .....	16
4.4.1	Discovering subsystems and components.....	17
4.4.1.1	Processors.....	17
4.4.1.2	Memory .....	18
4.4.1.3	Storage.....	19
4.4.1.4	Network Adapters .....	20
4.4.1.5	Management Controller.....	21
4.4.1.6	Fans (Cooling) .....	21
4.4.1.7	Temperature Sensors .....	22

---

4.4.1.8	Voltage Sensors .....	23
4.4.1.9	Power Supplies.....	23
4.4.1.10	Power Consumption .....	24
4.4.1.11	RAID Subsystem .....	25
4.4.1.12	RAID Logical Drives .....	26
4.4.1.13	RAID Physical Disks .....	26
4.4.1.14	Other Components .....	27
4.4.1.15	Communication Monitor .....	28
4.4.2	Updating the state of the subsystems .....	29
4.4.3	Monitoring components.....	29
4.4.4	Software Components .....	30
4.4.4.1	ServerView Agents .....	30
4.4.4.2	ServerView RAID.....	31
4.4.4.3	Windows Management Instrumentation (WMI) .....	31
4.4.5	Monitoring services.....	32
4.4.5.1	SCCI Management Software (ServerView Agents) .....	32
4.4.5.2	Windows Management Instrumentation (WMI) .....	32
4.4.5.3	ServerView RAID Manager .....	32
4.5	Performance Data Collection.....	33
4.5.1	Temperature Performance Data .....	33
4.5.2	Power Consumption Performance Data .....	34
4.6	Performance Data Collection for OMS.....	35
4.7	Views .....	35
4.7.1	Views defined by the Fujitsu ServerView Core Library MP .....	35
4.7.2	Views defined by the Fujitsu AddOnViews MP .....	37
4.7.3	Views defined by the Fujitsu PRIMERGY Windows Servers MP .....	39
4.7.4	Active Alerts View.....	40
4.7.5	Diagram View .....	41
4.7.6	Servers Health View .....	42
4.7.7	Health Monitoring Views.....	42
4.7.8	Alerts per Server View (from optional AddOnViews MP) .....	43
4.7.9	Components per Server View (from optional AddOnViews MP) .....	43
4.7.10	Views defined by the Performance Monitoring MP .....	44
4.8	Health Explorer.....	45
4.9	Fujitsu PRIMERGY Windows Server Tasks .....	46
4.9.1	Computer Management.....	46
4.9.2	Remote Desktop .....	46
4.9.3	Remote Desktop Console .....	46
4.9.4	Re-Initialize PRIMERGY Server Component Inventory.....	47
4.9.5	ServerView RAID Manager .....	47
4.9.6	ServerView Remote Management iRMC.....	47

---

4.9.7	ServerView Remote Management MMB .....	47
4.9.8	ServerView System Monitor.....	48
4.10	Events and alerts .....	48
4.10.1	Enabling and disabling alerts .....	49
4.11	Knowledge Base .....	49
<b>5</b>	<b>Working with the Performance Monitoring Management Pack .....</b>	<b>50</b>
5.1	Create additional Performance Monitoring Views .....	50
5.1.1	Create a Performance View based on specific rules .....	50
5.1.2	Create a Performance View based on specific performance objects and counters .	51
5.1.3	Create a Dashboard View containing a State and a Performance Widget .....	52
5.1.3.1	Define the dashboard layout .....	52
5.1.3.2	Configure the State Widget.....	52
5.1.3.3	Configuring the Performance Widget.....	53
5.1.4	24 Hour Performance Dashboard View.....	54
<b>6</b>	<b>Appendix.....</b>	<b>56</b>
6.1	Supported PRIMERGY servers .....	56
6.2	Entries in the Operations Manager's Event Log .....	56
6.3	Creating test entries in the Windows Event Log .....	56
6.4	Creating log files.....	57
6.4.1	Currentness of log files .....	58
6.5	Troubleshooting .....	58
6.5.1	Use ServerView System Monitor to examine a PRIMERGY Server .....	58
6.5.2	No event logging of the controller driver(s) .....	58
6.5.3	Enable / Disable Windows Installer Logging (Debug) .....	59
6.6	Hints and known issues .....	59





# 1 Introduction

The PRIMERGY ServerView Suite from Fujitsu offers numerous ServerView integration modules which enable PRIMERGY servers to be integrated easily into other enterprise management systems.

This manual describes the ServerView Windows Server Integration Pack, which enables Fujitsu PRIMERGY Windows Servers to be integrated into System Center Operations Manager (SCOM). All SCOM editions from SCOM 2012 up to SCOM 2016 are supported.

This ServerView Integration Pack allows PRIMERGY Windows Servers from Fujitsu to be monitored via SCOM. Monitoring PRIMERGY Windows Servers is implemented using script monitors for hardware and software components. The Health State of monitored components is displayed by means of icons.

If errors occur during monitoring of a PRIMERGY Windows Server, the ServerView Agents enter these into the Windows Event Log of the managed server. These events are evaluated and displayed on the SCOM Console. Rules can be applied which trigger an appropriate action when a fault is detected, e.g. a mail describing the fault might be sent to hardware support.

For detailed analysis the ServerView System Monitor can be started.

The current ServerView Windows Server Integration Pack for SCOM is provided on the latest PRIMERGY ServerView Suite DVD from Fujitsu or under:

[http://download.ts.fujitsu.com/prim\\_supportcd/SVSSoftware/](http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/)

## 1.1 Purpose and target groups

This manual is intended for system administrators, network administrators and service technicians who have a thorough knowledge of hardware and software. Likewise, a sound basic knowledge of the Microsoft System Center Operations Manager is required.

## 1.2 Changes since the last edition

The ServerView Windows Server Integration Pack includes the following changes:

- The Overall Health Collection State View has been removed.
- The Fujitsu ServerView Administration Pane (*Fujitsu.ServerView.IntegrationPackAdmin.mpb*) has been enhanced to support the Online Update of Fujitsu Management Packs. . See AdminPane documentation *sv-intpack-scom-adm-en.pdf* in folder *Common* for details.
- Management Packs for OMS Integration (*Fujitsu.ServerView.Monitoring.Cloud.mpb*, *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.mpb*, *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.Overrides.xml*) are now part of the Integration Pack. See OMS documentation *Whitepaper SCOM OMS integration-en.pdf* in folder *Common* for details.
- The Diagram view was enhanced to show the relationship between Physical Disks and Logical Drives.
- The OMS/Cloud Management Packs are now included in the Integration Pack.
- A task to open the MMB console has been introduced for Blade Servers.

## 1.3 ServerView Suite link collection

Via the link collection, Fujitsu provides their customers with numerous downloads and further information on the ServerView Suite and PRIMERGY servers

In "ServerView Suite" on the left side, links are offered on the following topics:

- Forum
- Service Desk
- Manuals
- Product information
- Security information
- Software downloads
- Training



The downloads include the following:

- Current software versions for the ServerView Suite and additional Readme files.
- Information files and update sets for system software components (BIOS, firmware, drivers, ServerView Agents and ServerView Update Agents) for updating the PRIMERGY servers via ServerView Update Manager or for locally updating individual servers via ServerView Update Manager Express.
- The current version of all documentation on the ServerView Suite.

All downloads from the Fujitsu web server are free of charge.

For PRIMERGY servers, links are offered on the following topics:

- Service Desk
- Manuals
- Product information
- Spare parts catalogue

### Access to the ServerView link collection

You can reach the link collection of the ServerView Suite in various ways:

1. Via ServerView Operations Manager.
  - ▶ Select Help – Links on the start page or on the menu bar.  
This opens the start page of the ServerView link collection.
2. Via the start page of the online documentation for the ServerView Suite on the Fujitsu manual server.



The start page of the online documentation can be reached via the following link: <http://manuals.ts.fujitsu.com>

- ▶ In the selection list on the left, select x86 servers.
- ▶ Click the menu item PRIMERGY ServerView Links.  
This opens the start page of the ServerView link collection.
3. Via the ServerView Suite DVD2
  - ▶ In the start window of the ServerView Suite DVD2, select the option Select ServerView Software Products.

- ▶ Click Start to open the page with the software products of the ServerView Suite.
- ▶ On the menu bar select Links to open the start page of the ServerView link collection.




## 1.4 Documentation for ServerView Suite

The documentation can be downloaded free of charge from the Internet. You will find the online documentation at <http://manuals.ts.fujitsu.com> under the link *x86 servers*.

For an overview of the documentation to be found under ServerView Suite as well as the filing structure, see the ServerView Suite sitemap (*ServerView Suite -Site Overview*).

## 1.5 Notational Conventions

The following notational conventions are used in this manual:

	<p><b>Warning</b></p> <p>This symbol is used to draw attention to risks which may represent a health hazard or which may lead to data loss or damage to the hardware</p>
	<p><b>Information</b></p> <p>This symbol highlights important information and tips.</p>
	<p>This symbol refers to a step that you must carry out in order to continue with the procedure.</p>
<i>italics</i>	<p>Commands, menu items, names of buttons, options, file names and path names are shown in italics in descriptive text.</p>
<variable>	<p>Angle brackets are used to enclose variables which are replaced by values.</p>

### Screen Output

Please note that the screen output shown in this manual may not correspond to the output from your system in every detail. System-related differences between the menu items available can also arise.

## 2 Integration requirements

The requirements specified below must be satisfied for integration.

### Management station

- Windows Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019.  
See the requirements for the relevant SCOM version
- SQL Server 2008 / 2012 / 2014 / 2016 / 2019.  
See the requirements for the relevant SCOM version
- Microsoft System Center Operations Manager 2012 / 2012 SP1/ 2012 R2 / 2016 / 2019
- SCOM 2012 SP1 UR6 or SCOM 2012 R2 UR2 for additional dashboard views



On SCOM 2012 SP1 with UR6  
Microsoft.SystemCenter.Visualization.Component.Library version 7.0.9538.1109  
is required.

On SCOM 2012 R2 with UR2  
Microsoft.SystemCenter.Visualization.Component.Library version  
7.1.10226.1015 is required.

### Managed PRIMERGY servers

- Windows Server 2008 R2 or Windows Server 2012 [R2] or Windows Server 2016 or Windows Server 2019
- Windows Management Instrumentation (WMI)
- PowerShell >= V2.0
- ServerView Agents and CIM Providers >= V7.00.06
- ServerView RAID >= V6.0.3 for RAID monitoring
- Management controller iRMC (integrated Remote Management Controller) (for power consumption monitoring)
- Installed SCOM agent

## 2.1 Setting trap severities for ServerView Agents

To permit ServerView events to be displayed in SCOM, they must be written to the Windows Event Log. For this purpose the required trap severities must be enabled for the ServerView Agents.

Using the start menu function *Start - [All] Programs - Fujitsu - ServerView Suite - Agents - Agents Configuration* open the dialog box below, and in the Trap Forwarding tab enable the required trap severities under *Report to system event log*.

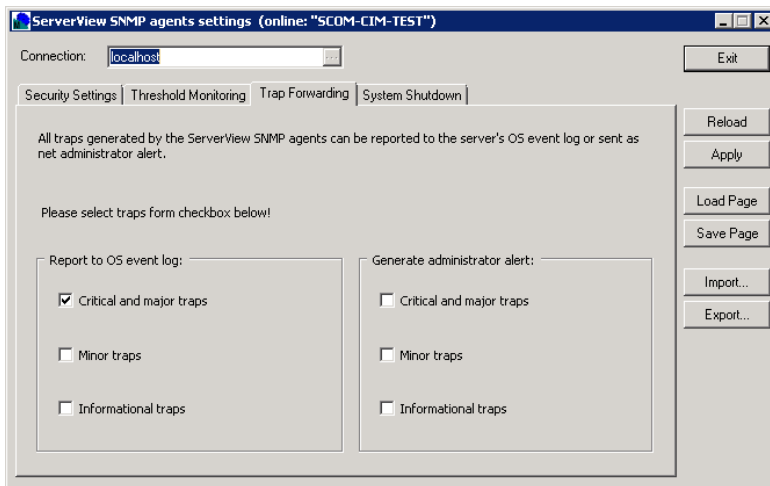



Figure 1 – ServerView SNMP Settings

## 2.2 Updating ServerView Agents

When updating the ServerView Agents set the relevant PRIMERGY server in Maintenance Mode during this action.

-  Failure to set target servers where ServerView Agents are to be updated in maintenance mode may lead to an incomplete installation of ServerView Agents. This may impact the monitoring capabilities of the ServerView Agents and the ServerView Windows Server Integration Pack.

## 3 Installation and uninstallation

### 3.1 Installing ServerView Integration Pack

The installation program SVSICOM-Win.exe is located on the ServerView Suite DVD at <DVDroot>\SVSSoftware\Software\Integration\_Solutions\SCOM

or as a download on the website at

[http://download.ts.fujitsu.com/prim\\_supportcd/SVSSoftware/](http://download.ts.fujitsu.com/prim_supportcd/SVSSoftware/)

The installation program first runs some basic checks then starts the Installation Wizard. Follow the instructions displayed during the installation process.

#### 3.1.1 Installed files

The default installation path on the management station is:

— %ProgramFiles%\Fujitsu\ServerView Suite\SCOM Integration

The following files are copied into the installation directories:

Folder	Files
SVSICOM-Win sub folder	<ul style="list-style-type: none"> <li>• <i>eula_en.pdf</i></li> <li>• <i>eula_ja.pdf</i></li> <li>• <i>sv-intpack-scom-win-en.pdf</i></li> </ul>
Management Packs sub folder	<ul style="list-style-type: none"> <li>• <i>Fujitsu.ServerView.Library.mpb</i></li> <li>• <i>Fujitsu.ServerView.Image.Library.mpb</i></li> <li>• <i>Fujitsu.ServerView.AddOnViews.mpb (optional)</i></li> <li>• <i>Fujitsu.ServerView.IntegrationPackAdmin.mpb (optional)</i></li> <li>• <i>Fujitsu.ServerView.Monitoring.Cloud.mpb (optional)</i></li> <li>• <i>Fujitsu.Servers.PRIMERGY.WindowsSeed.mpb</i></li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.mpb</i></li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.mpb (optional)</i></li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.Overrides.xml (optional)</i></li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.PerfMon.mpb (optional)</i></li> </ul>

	<ul style="list-style-type: none"> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Overrides.xml</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.AddOnViews.mpb</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.DDM.Alerts.mpb</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.FC.Alerts.mpb</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.NIC.Alerts.mpb</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.RAIDMIB.Alerts.mpb</i> (optional)</li> <li>• <i>Fujitsu.Servers.PRIMERGY.Windows.SC2MIB.Alerts.mpb</i> (optional)</li> </ul>
<i>Common sub folder</i>	<ul style="list-style-type: none"> <li>• <i>sv-intpack-scom-adm-en.pdf</i></li> <li>• <i>Whitepaper SCOM OMS integration-en.pdf</i></li> </ul>



After Installation start the SCOM console with the command  
 Microsoft.EnterpriseManagement.Monitoring.Console.exe /clearcache.



In case other Fujitsu Integration Packs are also installed on the SCOM, the folder *Management Packs* may contain both the old *ServerView Core Library* (*Fujitsu.ServerView.Library.mp*) and the new *ServerView Core Library* (*Fujitsu.ServerView.Library.mpb*) after installation.

Please note that to install the new *ServerView Core Library* (*Fujitsu.ServerView.Library.mpb*) it is imperative not to also select the old *ServerView Core Library* (*Fujitsu.ServerView.Library.mp*) for import into SCOM. If both Libraries are selected, SCOM will refuse to import any of them.

## 3.1.2 Importing Management Packs

Management packs installed by the ServerView Windows Server Integration Pack are located in the folder 'Management Packs' within the installation folder. This folder holds all management packs from ServerView Integration Packs for System Center Operations Manager not only from the ServerView Windows Server Integration Pack.

PRIMERGY Management Packs are imported in the usual way from the SCOM Console.

Not all Management Packs of the ServerView Windows Server Integration Pack must be imported, some Management Packs are optional. See chapter [3.1.1 Installed files](#) for details. All Management Packs can be installed at one time.

Close the SCOM Console once after importing management packs.



## 3.2 Update to a new version

Update installation is not supported by the ServerView Windows Server Integration Pack. The process is an uninstallation of the old version followed by the installation of the new version.



The Management Packs of the ServerView Windows Server Integration Pack themselves are usually update-compatible. New management packs can be imported on top of the old management packs.

You can do this either manually or use the Fujitsu ServerView Administration Page. See *sv-intpack-scom-adm-en.pdf* for its usage.

Use Windows' un-installation feature to un-install the old ServerView Windows Server Integration Pack.

Follow chapter [3.1 Installing ServerView Integration Pack](#) to install the new ServerView Windows Server Integration Pack.

## 3.3 Updating the ServerView Library Management Packs

The ServerView Library Management Pack and the ServerView Image Library Management Pack are used and referenced by all Fujitsu ServerView Integration Packs for System Center Operations Manager.



If a ServerView Integration Pack contains a newer version of one of the ServerView Library Management Packs this new version can usually be imported into SCOM without impact to any other Fujitsu ServerView Integration Management Packs.

In the rare case that a new version of one of the ServerView Library Management Packs is not compatible with the old version, it is necessary to uninstall all Fujitsu Management Packs including their Override Management Packs and reinstall all Fujitsu Management Packs from the folder 'Management Packs' together with the updated ServerView Library and ServerView Image Library Management Packs.

You can do this either manually or use the Fujitsu ServerView Administration Page. See *sv-intpack-scom-adm-en.pdf* for its usage.

## 3.4 Uninstalling ServerView Integration Pack

If the ServerView Windows Server Integration Pack is to be removed completely from the management station, it is necessary to first remove the management packs from SCOM (see [3.4.1 Removing the Management Packs](#)).

For an update-installation removing the old installer package is sufficient.

### 3.4.1 Removing the Management Packs

To remove the management packs follow these steps:

- Remove the corresponding override management packs if any from SCOM. To keep existing override settings, e.g. to re-use in a new version, the override management packs should be exported and saved.
- Remove the PRIMERGY Windows Server Management Packs from SCOM.

Or use the Fujitsu ServerView Administration Page. See *sv-intpack-scom-adm-en.pdf* for its usage.



If other ServerView Integration Packs for System Center Operations Manager have been installed, the ServerView Library Management Packs cannot be uninstalled.

To remove the Management Packs you need SCOM administrator rights. The old ServerView Windows Server Integration Pack should be removed from all SCOM Remote Consoles.

## 4 Properties of the ServerView Windows Server Integration Pack

### 4.1 Management Packs

The *Fujitsu ServerView Core Library* Management Pack contains the basic definitions to manage Fujitsu systems in a consolidated manner in SCOM. This Management Pack is distributed with all Fujitsu SCOM Integration Packs.

The file name of this package is *Fujitsu.ServerView.Library.mpb*.

The *Fujitsu ServerView Image Library* Management Pack contains images common to all Fujitsu SCOM Management Packs. This Management Pack is distributed with all Fujitsu SCOM Integration Packs.

The file name of this package is *Fujitsu.ServerView.Image.Library.mpb*.

The optional *Fujitsu ServerView AddOn Views* Management Pack contains definitions for additional interactive Views for detailed component health investigations.

This Management Pack requires SCOM 2012 SP1 UR6 or SCOM 2012 R2 UR2.

The file name of this package is *Fujitsu.ServerView.AddOnViews.mpb*.



On SCOM 2012 SP1 with UR6 Microsoft.SystemCenter.Visualization.Component.Library version 7.0.9538.1109 is required.

On SCOM 2012 R2 with UR2 Microsoft.SystemCenter.Visualization.Component.Library version 7.1.10226.1015 is required.

The optional *Fujitsu ServerView Administration Page* Management Pack contains an Addition to SCOM's Administration Pane which is designed to help with managing Fujitsu ServerView Integration Packs. For more information see *sv-intpack-scom-adm-en.pdf*.

The file name of this package is *Fujitsu.ServerView.IntegrationPackAdmin.mpb*.

The optional *Fujitsu ServerView Server - Collect Health State to OMS* Management Pack collects health information of Fujitsu ServerView Servers to a Microsoft Operations Management Suite (OMS) workspace. For more information see *Whitepaper SCOM OMS integration-en.pdf*.

The file name of this package is *Fujitsu.ServerView.Monitoring.Cloud.mpb*.

The *Fujitsu PRIMERGY Windows Servers Seed* Management Pack contains the initial Fujitsu PRIMERGY Windows Server Discovery.

The file name of this package is *Fujitsu.Servers.PRIMERGY.WindowsSeed.mpb*.

The *Fujitsu PRIMERGY Windows Servers* Management Pack contains the definitions for discovery and monitoring of Fujitsu PRIMERGY servers running Windows operating systems.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.mpb*.

The optional *Fujitsu PRIMERGY Windows Server Performance Monitoring* Management Pack adds performance collection rules for Temperature and Power Consumption related sensors of PRIMERGY servers.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.mpb*.

The optional *Fujitsu PRIMERGY Windows Server Performance Monitoring Overrides* Management Pack adds overrides for the performance collection rules from the *Fujitsu PRIMERGY Windows Server Performance Monitoring* Management Pack to enable some Performance Counters (Ambient Temperature and System Power Consumption). It can be edited to enable or disable Performance Collection Rules as desired.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Overrides.xml*.



Please note that without importing the *Fujitsu PRIMERGY Windows Server Performance Monitoring Overrides* Management Pack all Performance Collection rules are disabled by default.

The optional *Fujitsu PRIMERGY Windows Servers AddOn Views* Management Pack contains definitions for additional interactive Views for detailed component health investigations.

This Management Pack requires SCOM 2012 SP1 UR6 or SCOM 2012 R2 UR2.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.AddOnViews.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers DuplexDataManager Alerts* Management Pack contains rules to catch error and warning events from the Duplex Data Manager.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.DDM.Alerts.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers FibreChannel Alerts* Management Pack contains rules to catch error and warning events from supported FibreChannel controllers in PRIMERGY servers.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.FC.Alerts.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers NIC Alerts* Management Pack contains rules to catch error and warning events from supported Network Interface Controllers in PRIMERGY servers.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.FC.Alerts.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers RAID.MIB Alerts* Management Pack contains rules to catch error and warning alerts from the ServerView RAID.mib.

This Management Pack is not necessary to ensure full monitoring of PRIMERGY Windows server's RAID environment but is provided for customers who do not only want to see status changes for the server's RAID environment but want to receive all RAID events as individual alerts.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.RAIDMIB.Alerts.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers SC2.MIB Alerts* Management Pack contains rules to catch error and warning alerts from the ServerView hardware MIB SC2.mib and other hardware MIBs (HD.mib, NTCLUSTER.mib, THRESHOLD.mib).

This Management Pack is not necessary to ensure full monitoring of PRIMERGY Windows servers but is provided for customers who do not only want to see status changes for hardware but want to receive all hardware events as individual alerts.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.SC2MIB.Alerts.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers OMS Performance Data Collection* Management Pack adds additional rules to collect performance data of Fujitsu PRIMERGY Windows Servers to a Microsoft Operations Management Suite (OMS) workspace.

The file name of this package is *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.mpb*.

The optional *Fujitsu PRIMERGY Windows Servers OMS Performance Data Collection Overrides* Management Pack adds overrides for the performance collection rules from the *Fujitsu PRIMERGY Windows Servers OMS Performance Data Collection* Management Pack to enable Performance Counters. It can be edited to enable or disable Performance Collection Rules as desired.

The name of this package is *Fujitsu.Servers.PRIMERGY.Windows.PerfMon.Cloud.Overrides.xml*.



Please note that without importing the *Fujitsu PRIMERGY Windows Servers OMS Performance Data Collection Overrides* Management Pack all Performance Collection for OMS rules are disabled by default.

## 4.2 PRIMERGY server computer groups

Detected PRIMERGY servers are categorized in groups:

- BX models (e.g. BX2560)
- CX models (e.g. CX2550)
- RX models (e.g. RX2510, RX4770)

- SX models (e.g. SX150, SX350)
- TX models (e.g. TX1330, TX2560)
- PRIMEQUEST Partitions (e.g. PQ3800)
- PRIMERGY models which do not fit in any of the above groups



Econel models are assigned to the TX model group (Econel Floorstand) or to the RX model group.

For a description of the presentation of the servers and the PRIMERGY server computer groups, see section [4.7 Views](#).

## 4.3 Discovering and monitoring PRIMERGY servers

PRIMERGY servers and their components can be discovered and monitored only if they have been included in SCOM management (installed SCOM Agent on the servers to be monitored).

The initial (seed) discovery checks the target server's registry for manufacturer (Fujitsu... or FUJITSU... or FSC ) and system type (PRIMERGY or PRIMEQUEST) and checks the target system's PowerShell version ( $\geq$  V2.0).

Any Fujitsu servers that fit the requirements are discovered and collected in the Seed Discovery class. Any Fujitsu servers whose PowerShell version does not fit is collected in the Obsolete Discovery class and will not be discovered or will subsequently be removed from monitored Fujitsu servers in SCOM.

The supported servers are discovered in detail and monitored using scripts and on the basis of the data supplied by WMI and ServerView CIM providers.

### 4.3.1 Displayed properties of recognized PRIMERGY servers

The following properties of a managed server are displayed:

- *Display Name*: host name of the server
- *Network Name*: fully qualified DNS name of the server

- *IP Address*: IP address(es) of the server
- *Model*: complete model name of the server
- *Serial Number*: serial number of the server
- *Operating System*: detailed version of the OS
- *Manufacturer*: system manufacturer
- *Chassis Model*: chassis name
- *Cabinets*: IDs of main and attached cabinets
- *System Firmware*: version of the system firmware
- *Physical Memory*: available memory
- *Disk Size*: total capacity of the partitions configured as logical disks
- *Monitoring Agents*: name and version of the ServerView Agents
- *RAID Manager*: name and version of the ServerView RAID Manager
- *BMC Address*: IPv4 address of the iRMC (if available)
- *BMC DNS name*: fully qualified DNS name of the iRMC (if available and if DNS enabled on iRMC)

The properties of a server which are discovered are displayed in the *Detail View* below a *Status* or a *Diagram* view.

## 4.3.2 Health state of a PRIMERGY server

The health state of a PRIMERGY server is determined by the state of its hardware and software components. The component with the most severe error determines the final health state of the PRIMERGY server. This means component redundancy is not supported.

This state is also passed on to the model group and the PRIMERGY server group (roll-up monitor).

### 4.3.3 Virtual machine is recognized as a PRIMERGY server

Virtual machines are not designed to be used for monitoring with the PRIMERGY Windows Server Management Pack.

If a virtual machine is detected as a PRIMERGY server and included in the monitoring activities (e.g. because a physical PRIMERGY server was converted to a virtual machine), this happens because the values used to detect the PRIMERGY server are still stored in the registry.

To remove the virtual machine from SCOM monitoring, place the virtual machine into Maintenance Mode and delete the following entry in the registry together with its entire content:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-Win\PYServerData
```

## 4.4 Discovering and monitoring server components

The server components are discovered and monitored with scripts on the basis of data retrieved via the ServerView Agents' CIM providers (WMI), via the ServerView RAID Agent and occasionally via other ServerView Agent APIs.

Only components which exist are discovered and monitored. If, for example, no fans can be detected (e.g. in a blade server where fans are managed by the chassis), the fan subsystem is not displayed in the Diagram View. Component groups which do not contain components with a usable state at discovery time are not displayed, either.

Instances of the same type are combined in groups (collections) and displayed together (e.g. all CPUs of a server belong to the processors group). In the case of an error the faulty component is displayed with *Critical* or *Warning* state and its health can be examined in the Health Explorer. The instance with the severest error determines the overall state of the group.

By default events with the severity *Critical* generate an alert and events with the severity *Warning* do not generate an alert. This default setting can be overridden.

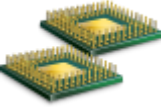
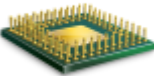


## 4.4.1 Discovering subsystems and components

The subsystems and components of a PRIMERGY server which are listed below can be discovered and monitored.


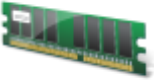
### 4.4.1.1 Processors

Processors which physically exist are discovered and grouped in the *Processors* collection. Their data is displayed and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: Network name: BMC Address: BMC DNS name: Component ID: Monitoring Agents: RAID Manager:	Processors <Name of the server> Number of Processors: <number> <Network name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> Processors ServerView Agents V<version> ServerView RAID V<version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Processor Information:	<Processor name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V<version> ServerView RAID V<version> <Processor name> <CPU Type / Number of cores>



### 4.4.1.2 Memory

Memory modules which are connected are discovered and grouped in the *Memory* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: Network name: BMC Address: BMC DNS name: Component ID: Monitoring Agents: RAID Manager:	Memory <Name of the server> <Number of detected Memory Modules> <Total Memory>; <Types and Numbers of Modules> <Network name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> Memory ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Capacity: Manufacturer: Part Number: Serial Number	<Module name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Module name> <Module capacity> <Module Manufacturer> <Module Part Number> <Module Serial Number>



### 4.4.1.3 Storage

Available volumes are discovered and grouped in the *Storage* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: Network name: BMC Address: BMC DNS name: Component ID: Monitoring Agents: RAID Manager:	Storage <Name of the server> <Number of detected Storage Disks> <Total Disk Space>; <Sizes and Numbers of Disks> <Network name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> Storage ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Size: Firmware Revision: Model Name: Serial Number Interface Type:	<Disk name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Disk name> <Disk size> <Disk Firmware Revision> <Disk Model Name> <Disk Serial Number> <Disk Interface Type>

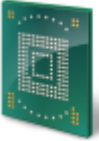
#### 4.4.1.4 Network Adapters

Available Network Adapters are discovered and grouped in the *Network (Ethernet)* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Networks (Ethernet) <Name of the server> <Number of detected Network Devices> <IPv4 address of the iRMC> <FQDN of the iRMC> Networks (Ethernet) ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: MAC Address: Connection ID: Service Name:	<Network Device name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Network Device name> <Network Device hardware address> <Network Device connection ID in OS> <Network Device driver name>


### 4.4.1.5 Management Controller


The iRMC (integrated Remote Management Controller) is discovered, its data is displayed and its health state is monitored.

Component Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Management Controller <i>&lt;Name of the server&gt;</i> <i>&lt;iRMC Name&gt;</i> <i>&lt;iRMC Firmware Version&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> Management Controller ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i>

### 4.4.1.6 Fans (Cooling)



Connected fan modules of PRIMERGY servers and their connected extension modules are discovered and grouped in the *Fans (Cooling)* collection. Their data is displayed and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Fans (Cooling) <i>&lt;Name of the server&gt;</i> <i>&lt;Number of detected Fan Devices&gt;</i> <i>&lt;Number of not populated Fans&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> Fans (Cooling) ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i>

Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	<Fan name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Fan name>



### 4.4.1.7 Temperature Sensors

Temperature sensors which physically exist are discovered and grouped in the *Temperatures* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Temperatures <Name of the server> <Number of detected Temperature Sensors> <Number of not populated Temperature Sensors > <IPv4 address of the iRMC> <FQDN of the iRMC> TemperatureSensors ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name : Monitoring Agents: RAID Manager: Device:	<Temperature Sensor name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Temperature Sensor name>


### 4.4.1.8 Voltage Sensors


Voltage sensors which physically exist are discovered and grouped in the *Voltages* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Voltages <Name of the server> <Number of detected Voltage Sensors> <Number of not populated Voltage Sensors > <IPv4 address of the iRMC> <FQDN of the iRMC> VoltageSensors ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	<Voltage Sensor name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Voltage Sensor name>

### 4.4.1.9 Power Supplies


Power supply modules which physically exist are discovered and grouped in the *Power Supplies* collection. Their data is displayed, and their health state is monitored.

Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Power Supplies <Name of the server> <Number of detected Power Supplies> <Number of not populated Power Supplies > <IPv4 address of the iRMC> <FQDN of the iRMC> Power Supplies ServerView Agents V <version> ServerView RAID V <version>

Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	<Power Supply name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Power Supply name>

#### 4.4.1.10 Power Consumption




Power Consumption is monitored if the iRMC supports power consumption monitoring and if the iRMC Power Control Mode is set to Power Limit. If the iRMC Power Control Mode is set to any other mode, Power Consumption monitoring always shows OK.

Component Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Power Consumption <Name of the server> Power Level <Power Consumption Sensor Name> <IPv4 address of the iRMC> <FQDN of the iRMC> PowerConsumption ServerView Agents V <version> ServerView RAID V <version>





### 4.4.1.11 RAID Subsystem

If ServerView RAID is installed and configured the *RAID Subsystem* collection is discovered. It contains Adapters, Logical Drives and Physical Disks. Their data is displayed, and their health state is monitored.

Raid Subsystem	Information	
	Display Name: Server Name: Devices: Device Information:  BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	RAID Subsystem <Name of the server> <Number of detected RAID Controllers> <Number and Type of Logical Drives>; <Number and Size of Physical Disks>; <IPv4 address of the iRMC> <FQDN of the iRMC> RAID Subsystem ServerView Agents V <version> ServerView RAID V <version>
Component Icons		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Type: Vendor: Serial Number: Firmware Version: Driver Details:	<Raid Controller name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Raid Controller name> <Raid Controller Type> <Raid Controller Vendor> <Raid Controller Serial Number> <Raid Controller Firmware Version> <Raid Controller Driver Details>
	Display Name: Server Name: BMC Address: BMC DNS name: Device: Monitoring Agents: RAID Manager:	SV RAID Overall State <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> SV RAID Overall State


### 4.4.1.12 RAID Logical Drives


The status of the logical RAID drives from ServerView RAID is discovered and monitored via the ServerView Agents.

Subsystem Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	RAID Logical Drives <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version>
Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Type	<Logical Drive name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> < Logical Drive ID> <RAID Type>

### 4.4.1.13 RAID Physical Disks

The status of the physical RAID disks from ServerView RAID is discovered and monitored via the ServerView Agents.

Subsystem Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	RAID Physical Disks <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version>

Component Icon		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device: Size: Firmware Revision: Model Name: Serial Number: Vendor Name:	<Physical Disk name> <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> <Physical Disk ID> <Physical Disk Size> <Physical Disk Firmware Revision> <Physical Disk Model Name> <Physical Disk Serial Number> <Physical Disk Vendor Name:>


#### 4.4.1.14 Other Components



This subsystem is used to display and monitor any hardware and non-hardware components which not fit into any of the above subsystems.

One of these is the overall state of a PRIMERGY server as reported by ServerView Agents which was cleared of all the know problems. This may reveal server problems which result from components the Management Pack cannot monitor.

The state of the Other Components subsystem is also influenced by the Communication Monitor (see [4.4.1.15 Communication Monitor](#) ).

Use the ServerView System Monitor task to check for details.


Subsystem Icon	Information	
	Display Name: Server Name: Devices: Device Information: BMC Address: BMC DNS name: ComponentID: Monitoring Agents: RAID Manager:	Other Components <Name of the server> <Number of detected components> <IPv4 address of the iRMC> <FQDN of the iRMC> OtherComponents ServerView Agents V <version> ServerView RAID V <version>

Component Icons		
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	BIOS Selftest <i>&lt;Name of the server&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i> BIOS Selftest
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	ServerView Overall State <i>&lt;Name of the server&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i> ServerView Overall State

#### 4.4.1.15 Communication Monitor

The Other Components Subsystem also comprises a communication monitor which monitors the communication between the scripts run by SCOM and the ServerView Agents (CIM Providers).

Problems here indicate that hardware monitoring is impaired. Restart 'ServerView Server Control' service and use the ServerView System Monitor task to check for details.

Component Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	Communication Monitor <i>&lt;Name of the server&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i> Communication Monitor

## 4.4.2 Updating the state of the subsystems

By default, the configuration of the components of a PRIMERGY server is discovered automatically every 4 hours.

Set the server in maintenance mode for a brief period. Once the maintenance mode has elapsed, SCOM automatically discovers the components again. Alternatively change the component discovery interval to force an update by performing a (temporary) override for all 'Discovery Rule for Windows Server Health Collection'.

## 4.4.3 Monitoring components

Components are monitored by means of a single script which is called at a regular interval (default 200 seconds; settable). Each component is monitored by its own monitor using the same script at the same interval.

This enables SCOM to cook down the monitoring process to a single script call and collect all component health states using only one process and call.



Script calls place a considerable load on SCOM.

If the monitoring intervals of single components are changed to different values this breaks down SCOMs CookDown feature and results in script calls in various intervals.


Keep this in mind when considering changing the monitoring intervals.

All component states are displayed in the Health Explorer (see [4.8 Health Explorer](#) ).

If the monitoring function reports the *Critical* state for a component, a corresponding alert is generated. *Warning* alerts are per default disabled. When the component returns to the *OK* state, the alert is resolved and is no longer displayed in the *Active Alerts* view (see [4.7.4 Active Alerts View](#)).



## 4.4.4 Software Components

The services of a PRIMERGY server which are listed below are discovered and monitored within the Software Components subsystem.

Component Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	Software Components <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version>



### 4.4.4.1 ServerView Agents

The ServerView Agents' *Server Control service* is Fujitsu's central service to monitor PRIMERGY hardware components.

Component Icon	Information	
	Display Name: Version: Server Name: Devices: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	ServerView Agents <ServerView Agents Version> <Server Name> Service 'SrvCtrl.exe' <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version>
Version Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	ServerView Agents Version <Name of the server> <IPv4 address of the iRMC> <FQDN of the iRMC> ServerView Agents V <version> ServerView RAID V <version> ServerView Agents Version


### 4.4.4.2 ServerView RAID

ServerView RAID manages and monitors all RAID controllers of PRIMERGY servers.

Component Icon	Information	
	Display Name: Version: Server Name: Devices: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	ServerView RAID <i>&lt;ServerView Agents Version&gt;</i> <i>&lt;Server Name&gt;</i> Service'amService.exe' <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i>
Version Icon	Information	
	Display Name: Server Name: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager: Device:	SV RAID Version <i>&lt;Name of the server&gt;</i> <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i> SV RAID Version

### 4.4.4.3 Windows Management Instrumentation (WMI)

While WMI is not a Fujitsu service, it is essential for ServerView Agents to report on PRIMERGY Hardware. For this reason WMI is also monitored by the Management Pack.

Component Icon	Information	
	Display Name: Version: Server Name: Devices: BMC Address: BMC DNS name: Monitoring Agents: RAID Manager:	Windows Management Instrumentation <i>&lt;WMI Version&gt;</i> <i>&lt;Server Name&gt;</i> None <i>&lt;IPv4 address of the iRMC&gt;</i> <i>&lt;FQDN of the iRMC&gt;</i> ServerView Agents V <i>&lt;version&gt;</i> ServerView RAID V <i>&lt;version&gt;</i>

## 4.4.5 Monitoring services

Services are monitored by individual monitors per service. The health state of the services is displayed in the Health Explorer.

### 4.4.5.1 SCCI Management Software (ServerView Agents)

The state of this software component is determined by the following service:

- ServerView Server Control (Service Name: SvrCtrl.exe)

If the monitoring function reports the *Critical* state, a corresponding alert is generated.



If the ServerView Agents are in *Critical* state, monitoring the server is no longer possible.

When the component returns to the *OK* state, the alert is resolved and no longer displayed in the *Active Alerts* view (see [4.7.4 Active Alerts View](#)).

### 4.4.5.2 Windows Management Instrumentation (WMI)

The state of this software component is determined by the Windows Management Instrumentation Service (Service Name: *wimgmt*). If this service is not running, the state of the WMI component is set to *Critical*.

If the monitoring function reports the *Critical* state, a corresponding alert is generated.



If the WMI service is in *Critical* state, monitoring the server is severely limited.

When the component returns to the *OK* state, the alert is resolved and no longer displayed in the *Active Alerts* view (see [4.7.4 Active Alerts View](#)).

### 4.4.5.3 ServerView RAID Manager

The state of this software component is determined by the ServerView RAID Manager Service (Service Name: *amService*). If this service is not running, the state of the ServerView RAID component is set to *Critical*.

If the monitoring function reports the *Critical* state, a corresponding alert is generated.





If the ServerView RAID Manager Service is in *Critical* state, monitoring the RAID subsystem is limited.

When the component returns to the *OK* state, the alert is resolved and no longer displayed in the *Active Alerts* view (see [4.7.4 Active Alerts View](#)).

## 4.5 Performance Data Collection

The *Fujitsu PRIMERGY Server Performance Monitoring* Management Pack adds various data collection rules to SCOM which are by default disabled. To enable the most interesting performance collection rules (Ambient Temperature and System Power Consumption) the *Fujitsu PRIMERGY Server Performance Monitoring Overrides* Management Pack must be installed. It can be edited to enable or disable Performance Collection Rules as desired.



Please note that without importing the *Fujitsu PRIMERGY Windows Server Performance Monitoring Overrides* Management Pack all Performance Collection rules are disabled by default.

The rules collect performance data by means of PowerShell Scripts. The collected performance data are then visualized and filtered using standard SCOM Performance Views supplied with the Management Pack.

While the sensors themselves are evaluated by the main management pack's health state monitors, collecting and storing current sensor readings can be useful for long time trend analysis and similar scenarios, e.g. finding peak or weekly re-occurring workload areas within a data center and help induce proactive actions such as cooling adjustments. Another scenario might be finding temperature hot spot locations within the data center by comparing performance data from multiple servers in different locations of the data center.

### 4.5.1 Temperature Performance Data

The *Fujitsu PRIMERGY Server Performance Monitoring* Management Pack imports the following temperature collection rules:

- *Fujitsu Windows Server 'Ambient' Temperature Performance Data Collection Rule*  
This rule collects data from the server's 'Ambient' or 'Air Inlet' temperature sensor.

- *Fujitsu Windows Server 'Processor' Temperature Performance Data Collection Rule*  
This rule collects data from all available 'Processor' temperature sensors of the server.
- *Fujitsu Windows Server 'Memory' Temperature Performance Data Collection Rule*  
This rule collects data from all available 'Memory' temperature sensors of the server.
- *Fujitsu Windows Server 'Power Supply' Temperature Performance Data Collection Rule*  
This rule collects data from all available 'Power Supply' temperature sensors of the server.
- *Fujitsu Windows Server 'System Board' Temperature Performance Data Collection Rule*  
This rule collects data from all available temperature sensors on the server's 'system board'.
- *Fujitsu Windows Server 'Other' Temperature Performance Data Collection Rule*  
This rule collects data from all other available temperature sensors of the server.

## 4.5.2 Power Consumption Performance Data

The *Fujitsu Servers PRIMERGY Server Performance Monitoring* Management Pack imports the following power consumption collection rules:

- *Fujitsu Windows Server 'Total' Power Consumption Performance Data Collection Rule*  
This rule collects data from the main power consumption sensors of the server.
- *Fujitsu Windows Server 'System Chassis' Power Consumption Performance Data Collection Rule for Multi Node Systems*  
This rule collects data from the main power consumption sensors of the chassis the server is housed in. The rule applies to BX and CX servers.
- *Fujitsu Windows Server 'Processor' Power Consumption Performance Data Collection Rule*  
This rule collects data from the available 'Processor' power consumption sensors of the server.
- *Fujitsu Windows Server 'Power Supply' Power Consumption Performance Data Collection Rule*  
This rule collects data from the available 'Power Supply' power consumption sensors of the server.
- *Fujitsu Windows Server 'Other' Power Consumption Performance Data Collection Rule*  
This rule collects data from the all other available power consumption sensors of the server.

## 4.6 Performance Data Collection for OMS

The *Fujitsu PRIMERGY Windows Servers OMS Performance Data Collection* adds various data collection rules for OMS to SCOM which are by default disabled. It requires the *Fujitsu ServerView Server - Collect Health State to OMS* Management Pack to be installed.

To enable any performance collection rules the *Fujitsu PRIMERGY Windows Servers Performance Monitoring Overrides* Management Pack must be installed. It can be edited to enable or disable Performance Collection Rules as desired.

For more information about forwarding data to an OMS work space see *Whitepaper SCOM OMS integration-en.pdf*.

## 4.7 Views

The health state in all views is displayed by the usual health state icons of the Operations Manager.

### 4.7.1 Views defined by the Fujitsu ServerView Core Library MP

When integrating the *Fujitsu ServerView Core Library* Management Pack a *Fujitsu ServerView Systems* node is created in the *Monitoring* pane of the SCOM Console. The following views are displayed in this node:

- Active Alerts
- Servers Diagram
- Systems State

State	Name	Model	Serial Number	Operating System
Critical	TX30058-STK	PRIMERGY TX300 S8	YLN0000017	SUSE Linux Enterprise Server 12 SP0 V3.12.28-4-default
Warning	H49007-BX92452	PRIMERGY BX924 S2	BX92452267	Microsoft Windows Server 2012 Standard
Warning	essi51sw4b200s5	PRIMERGY TX200 S5	YKKG.....	VMware ESXi 5.1.0 build-838463
Warning	SCOM2016	PRIMERGY VM	4358-1827-3627-8659-42...	Microsoft Windows Server 2016 Standard
Warning	FTS4	PRIMEQUEST 1800L	1480932004	Embedded Linux
Warning	BX40051em_044_System_044	BX40051	System_044	Embedded Linux
Healthy	iRMC01CA5C-iRMC.servwar...	PRIMERGY RX2540 M1	YLT000098	N/A
Healthy	TX14052-STK2	PRIMERGY TX14052	YLPX001011	VMware ESXi 6.0.0 build-2494585
Healthy	RX10058-STK	PRIMERGY RX100 S8	YLN0000051	Red Hat Enterprise Linux Server 6.6 V2.6.32-504.el6.x86_64
Healthy	FK-iRMC-RX4770M4.svsnet...	PRIMERGY RX4770 M4	YMAK000000	N/A
Healthy	H49053-TX20057	PRIMERGY TX200 S7	YLFK001124	VMware ESXi 5.5.0 build-3343343
Healthy	iRMC40BD13.servware.abgf...	PRIMERGY RX2520 M1	YLSK0004699	Windows Server 2016 Standard
Healthy	PRIMEQUESTTFT57	PRIMEQUEST 2800E	1541329002	Embedded Linux

Figure 2 – Views defined by the Fujitsu ServerView Core Library MP

- These views display all objects which are assigned to the class the particular view targets. Which systems this class comprises depends on the further Fujitsu Management Packs that have been installed, e.g. the Fujitsu PRIMERGY Windows Servers Management Pack.
- The views installed by the Fujitsu ServerView Core Library Management Pack comprise all systems that are targeted by Management Packs that depend on the Fujitsu ServerView Core Library Management Pack and aim for an easy overview of all Fujitsu systems.

Additionally a *Fujitsu ServerView Management* node is created in the *Administration* pane of the SCOM console. This node is designed to hold all administration features any *Fujitsu ServerView Management Pack* may introduce, e.g. the admin page introduced by the *Fujitsu ServerView Administration Page* management pack.

## Fujitsu ServerView Integration Packs

This page provides a list of all installed and available Fujitsu Software Serve those located locally on the SCOM Console host after Integration Pack insta

Available Integration Packs and Libraries:

**Integration Packs**

- Fujitsu PRIMEQUEST
- Fujitsu PRIMERGY BladeSystem
- Fujitsu PRIMERGY ESXi
- Fujitsu PRIMERGY Linux
- Fujitsu PRIMERGY OutOfBand
- Fujitsu PRIMERGY PRO
- Fujitsu PRIMERGY Windows

**Common Libraries**

Figure 3 – Administration node defined by the Fujitsu ServerView Core Library MP

For more information about the *Fujitsu ServerView Administration Page* management pack see [sv-intpack-scom-adm-en.pdf](#).

## 4.7.2 Views defined by the Fujitsu AddOnViews MP

The AddOnViews Management Pack requires SCOM 2012 SP1 with UR6 or SCOM 2012 R2 with UR2 installed.



On SCOM 2012 SP1 with UR6 Microsoft.SystemCenter.Visualization.Component.Library version 7.0.9538.1109 is required.

On SCOM 2012 R2 with UR2 Microsoft.SystemCenter.Visualization.Component.Library version 7.1.10226.1015 is required.

When integrating the *Fujitsu ServerView AddOn Views* Management Pack the *Fujitsu ServerView Systems* node is enhanced with the following dashboard views:

- Alerts per Server
- Components per Server

The screenshot shows the 'Alerts per Server' dashboard. The top section, 'Fujitsu ServerView Servers', is a table with columns: State, Alerts, Name, Model, Processors, Memory, Fans, Temperatures, Voltages, Power Supplies, Other, RAID, and Path. The table lists several servers, with the 'BX92052-PST' server highlighted in blue. This server has a yellow warning icon in the 'Alerts' column and a red 'X' icon in the 'State' column. The middle section, 'Alerts per selected Server(s) (2)', shows a list of alerts for the selected server. It includes a 'Raid Physical Disk' alert (Severity: Critical) and a 'Communication Monitor' alert (Severity: Warning). The bottom section, 'Detail View', provides information for the selected server: Display Name (BX92052-PST), Path (BX92052-PST.servware.abg.fsc.net|BX92052-PST), Health (Warning), Object Display Name (BX92052-PST), and Model (PRIMERGY BX920 S2).

State	Alerts	Name	Model	Processors	Memory	Fans	Temperatures	Voltages	Power Supplies	Other	RAID	Path
✓		TX14052-STK2	PRIMERGY TX14052	✓	✓	✓	✓	✓	✓	✓		SCOM-CIM-T
✓		PGTR3	PRIMERGY TX120	✓	✓	✓	✓	✓	✓	✓	✓	pgtr3.servwa
⚠	✖	BX92052-PST	PRIMERGY BX920 S2	✓	✓	✓	✓	✓	✓	✓	⚠	BX92052-P5
✓		H50235-MX13052L	PRIMERGY MX130 S2	✓	✓	✓	✓	✓	✓	✓		H50235-MX1
⚠		TX30054-STK2	PRIMERGY TX300 S4	✓	✓	✓	✓	✓	✓	✓	✓	SCOM-CIM-T

Severity	Source	Maintenance Mode	Name
✖	Raid Physical Disk: 0/2		BX92052-PST.servware.abg.fsc.net: The 'RAID Physical Disks' collection of a Fujitsu PRIMERGY Windows Server is in failed state.
⚠	Communication Monitor		BX92052-PST.servware.abg.fsc.net: The Communication Monitor of a Fujitsu PRIMERGY Windows Server is in warning state.

Detail View

Display Name: BX92052-PST  
 Path: BX92052-PST.servware.abg.fsc.net|BX92052-PST  
 Health: ⚠ Warning  
 Object Display Name: BX92052-PST  
 Model: PRIMERGY BX920 S2

Figure 4 – Alerts per Server View

The *Alerts per Server* dashboard view displays alerts for selected servers. The view is comprised of three windows.

Servers are displayed in the top 'Fujitsu ServerView Servers' window. When a server is selected in the 'Servers' View, its alerts are displayed in the middle 'Alerts per selected Servers' window.

The Detail view below in the bottom window displays the details of the selected object (Server or alert)

Components per Server

Fujitsu ServerView Servers

State	Alerts	Name	Model	Processors	Memory	Fans	Temperatures	Voltages	Power Supplies	Other	RAID	Path	
⚠	✖	BX92052-PST	PRIMERGY BX920 S2	✔	✔		✔	✔			⚠	⚠	BX92052-PST
✔		H50235-MX13052L	PRIMERGY MX130 S2	✔	✔	✔	✔	✔			✔		H50235-MX1
⚠		TX30054-STK2	PRIMERGY TX300 S4	✔	✔	✔	✔	✔			✔		SCOM-CIM-T

Component of selected Server(s)

State	Display Name	Server	Devices
✔	Storage	BX92052-PST.servware.abg.fsc.net	Storage Dis
⚠	RAID Subsystem	BX92052-PST.servware.abg.fsc.net	Raid Contr
✔	Power Consumption	BX92052-PST.servware.abo.fsc.net	Power Lev

Sub-Components of selected Component(s)

State	Display Name	Server	Path
⚠	Raid Controller 0	BX92052-PST.servware.abg.fsc.net	BX92052-PST.s
✔	Raid Controller 1	BX92052-PST.servware.abg.fsc.net	BX92052-PST.s
✔	SV Raid Version	BX92052-PST.servware.abo.fsc.net	BX92052-PST.s

Alerts (1)

Severity	Source	Maintenance Mode	Name
✖	Raid Physical Disk	0/2	BX92052-PST.servware.abg.fsc.net: The 'RAID Physical Disks' collection of a Fujitsu PRIMERGY Windows Server is in failed state

Detail View

Display Name	RAID Subsystem
Path	BX92052-PST.servware.abg.fsc.net\Fujitsu.Health\Collections\RAID Subsystem
Health	⚠ Warning

Figure 5 – Components per Server View

The *Components per Server* dashboard view displays components groups, components and alerts for selected servers. The view is comprised of 5 individual windows.

Servers are displayed in the top 'Fujitsu ServerView Servers' window. When a server is selected in the 'Servers' View, its alerts are displayed in the bottom 'Alerts' window and its component groups are displayed in the middle left 'Component Groups per selected Servers' window.

When a component group is selected in the middle left 'Components Group View', the middle right 'Sub-Components of selected Components' window shows all components and the bottom 'Alerts' view shows all alerts for the selected group.

The Detail view below in the very bottom window always displays the details of the selected object (server or group or component or alert).



## 4.7.4 Active Alerts View

The *Active Alerts* view displays all alerts which are assigned to the Fujitsu PRIMERGY Windows Server class. Only alerts which have the resolution state *Not Closed* are displayed.

The following causes can trigger an alert:

- If a component monitor is in the Critical state and a corresponding alert is displayed for this component.  
This alert is "auto-resolving": As soon as the cause has been resolved, the alert is no longer displayed in the view.
- An event for which a rule is defined in the Management Pack is entered in the Windows Event Log of a monitored server. These alerts remain in the display until they are explicitly closed.
- An error for which a rule is defined in the Management Pack occurs in a script. These alerts remain in the display until they are explicitly closed.

By default alerts are only generated for events which have been entered in the Windows Event Log (Application, Operations Manager or System) with the severity *Critical (Error)*. Events with the severity *Warning* can also be displayed if they are enabled by the user.

Source	Name	Resolution Sta...	Created	Age	Repeat Co
Severity: Critical (1)					
PRIMERGY Overall State	The Overall Health State of a PRIMERGY is in failed state.	New	1/21/2015 3:06:45 PM	2 Hours, 21 M...	0

Figure 7 – Active Alerts View

Alerts which are placed in the resolution state *Closed* no longer appear in the *Active Alerts* view.

For some alerts Alarm Suppression is enabled. In this case, the alert is only reported once. Any next alert of this type causes the *Repeat Count* to be increased. To display the *Repeat Count* column use the *personalize view* setting.



## 4.7.5 Diagram View

A *Diagram* view is the graphical presentation of the Fujitsu systems infrastructure. The connection of Fujitsu systems to PRIMERGY servers to model groups and the connection of the components to the PRIMERGY servers are presented here.

When systems are included in a group, this is indicated by a non-empty circle near the computer symbol. This group can be expanded further to display the existing systems:

The state of the hardware and software components of a server is also shown in the *Servers Diagram* view. The components are displayed graphically together with the assigned server.

Components which are in a healthy state are included in the healthy group beneath the associated server.

If more than one component is in the *Warning* or *Critical* state, these are collected in the corresponding groups and also presented (simultaneously) beneath the PRIMERGY server.

The discovered instances of a component are grouped into health collections. Properties of the selected component or group are displayed in the *Detail View* below the component representation.

The following properties are displayed for each group of components:

- *Display Name:* Name of the component
- *Server Name:* Name of the system to which the component belongs
- *Devices:* Information of amount of discovered device instances
- *Device Information:* Additional information for the group if available
- *BMC Address:* IPv4 address of the integrated Remote Management Controller
- *BMC DNS name:* Fully Qualified Domain Name, if available and DNS enabled on iRMC

The following properties are displayed for each component:

- *Display Name:* Name of the component
- *Server Name:* Name of the system to which the component belongs
- *Devices:* Information of discovered device instances
- *Device Information:* Additional information for the devices if available
- *BMC Address:* IPv4 address of the integrated Remote Management Controller
- *BMC DNS name:* Fully Qualified Domain Name, if available and DNS enabled on iRMC
- *Additional properties:* if information is available

## 4.7.6 Servers Health View

The *Servers Health* view displays the state of all servers which are assigned to the class the view targets.

State	Name	Model	Processors	Memory	Fans	Temperature	Voltages	Power Supplies	Networks	Raid Component	Software Component	Other Component	Monitoring Agents
Critical	TX30054-PST	PRIMERGY TX300 54	Healthy	Healthy	Healthy	Warning	Healthy	Healthy	Healthy	Healthy	Healthy	Critical	ServerView Agents / 7.01.06
Warning	SCOM-CIM-TE...	PRIMERGY VM	Healthy	Healthy								Warning	ServerView Agents / 6.00.04
Warning	BX92052-PST	PRIMERGY BX920 52	Healthy	Healthy		Healthy	Healthy		Healthy	Healthy	Healthy	Warning	ServerView Agents / 7.20.08
Healthy	PGTR3	PRIMERGY TX120	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	ServerView Agents / 6.00.04
Healthy	H50235-MX130...	PRIMERGY MX130 52	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	ServerView Agents / 7.20.20
Healthy	H54001-CX257...	PRIMERGY CX2570 ...	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	ServerView Agents / 7.20.16

Figure 8 – Servers Health View

The properties of the selected PRIMERGY server are displayed in the Details View below this view.

## 4.7.7 Health Monitoring Views

The *Health Monitoring* views display the health state and corresponding alerts of the hardware component class the view targets. The Detail view below State and Alerts view display the details of the selected object (hardware component or alert).

**Raid Controller Health**

Raid Controller State (4)

State	Display Name	Server Name	Type	Vendor	Serial Number	Firmware Version	Driver Details
Warning	Raid Controller 0	BX92052-PST.senware.abg.fsc.net	SAS	Fujitsu Technol...		01.27.00.00	lsi_sas_v1.32.00...
Healthy	Raid Controller 0	pgtr3.senware.abg.fsc.net	SAS				
Healthy	Raid Controller 1	BX92052-PST.senware.abg.fsc.net	SAS	Fujitsu Technol...		01.27.00.00	lsi_sas_v1.32.00...

Raid Controller Alerts (1)

Source	Name	Resolution State	Created	Age
<b>Severity: Critical (1)</b>				
Raid Physical Disk 0/2	BX92052-PST.senware.abg.fsc.net: The 'RAID Physical D...	New	17.05.2016 09:04:53	6 Days, 5 Hours, 28 Minut...

**Alert Details**

<p><b>BX92052-PST.senware.abg.fsc.net: The 'RAID Physical Disks' collection of a Fujitsu PRIMERGY Windows Server is in failed state.</b></p> <p>Source: <b>Raid Physical Disk 0/2</b></p> <p>Full Path Name: <b>BX92052-PST.senware.abg.fsc.net\Fujitsu.HealthCollections\RAID Subsystem\RAID Controller 0\RAID Physical Disks 0\RAID Physical Disk 0/2</b></p> <p>Alert Monitor: <b>Fujitsu PRIMERGY Windows Server RAID Physical Disk Health Monitor</b></p> <p>Created: 17.05.2016 09:04:53</p>	<p><b>Alert Description</b></p> <p>BX92052-PST.senware.abg.fsc.net: An instance of 'RAID Physical Disks' is in Critical o Check the running status of the ServerView Agents Service ('ServerView Server Contr</p>
--	---

Figure 9 – Raid Controller Monitoring Health View

## 4.7.8 Alerts per Server View (from optional AddOnViews MP)

The AddOnViews Management Pack requires SCOM 2012 SP1 with UR6 or SCOM 2012 R2 with UR2 installed.

The *Alerts per Server* dashboard view displays alerts for selected servers. The view is comprised of three windows.

Servers are displayed in the top 'Fujitsu PRIMERGY Windows Servers' window. When a server is selected in the 'Servers' View, its alerts are displayed in the middle 'Alerts per selected Server' window. The Detail view below in the bottom window displays the details of the selected object (Server or alert).

Alerts per Servers

Fujitsu PRIMERGY Windows Servers

State	Alerts	Name	Model	Processors	Memory	Fans	Temperatures	Voltages	Power Supplies	Storage	Networks	Raid Components	Other C
⊗	⊗	TX30054-PST	PRIMERGY TX300 54	⊙	⊙	⊙	⚠	⊙	⊙	⊙	⊙	⊙	
⊙		PGTR3	PRIMERGY TX120	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	
⚠	⊗	BX92052-PST	PRIMERGY BX920 52	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⚠	
⊙		H50235-MX13052L	PRIMERGY MX130 52	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	
⚠	⊗	SCOM-CIM-TEST	PRIMERGY VM	⊙	⊙					⊙			

Alerts per selected Server(s) (2)

Filter

Severity	Source	Maintenance Mode	Name	Age
⊗	Raid Physical Disk 0/2		BX92052-PST.servware.abg.fsc.net: The 'RAID Physical Disks' collection of a Fujitsu PRIMERGY Windows Server is in failed state.	6 Days, 05 Hours
⚠	Communication Monitor		BX92052-PST.servware.abg.fsc.net: The Communication Monitor of a Fujitsu PRIMERGY Windows Server is in warning state.	11 Days, 05 Hours

Detail View

Display Name	BX92052-PST
Path	BX92052-PST.servware.abg.fsc.net\BX92052-PST
Health	⚠ Warning

Figure 10 – Alerts per Windows Server View

## 4.7.9 Components per Server View (from optional AddOnViews MP)

The AddOnViews Management Pack requires SCOM 2012 SP1 with UR6 or SCOM 2012 R2 with UR2 installed.

The *Components per Server* dashboard view displays components groups, components and alerts for selected servers. The view is comprised of 5 individual windows.

Servers are displayed in the top 'Fujitsu PRIMERGY Windows Servers' window. When a server is selected in the 'Servers' View, its alerts are displayed in the bottom 'Alerts' window and its

component groups are displayed in the middle left 'Component Groups per selected Server(s)' window.

When a component group is selected in the middle left 'Components Group View', the middle right 'Components per selected Group(s)' windows shows all components and the bottom 'Alerts' view shows all alerts for the selected group.

The Detail view below in the bottom windows always displays the details of the selected object (server or group or component or alert).

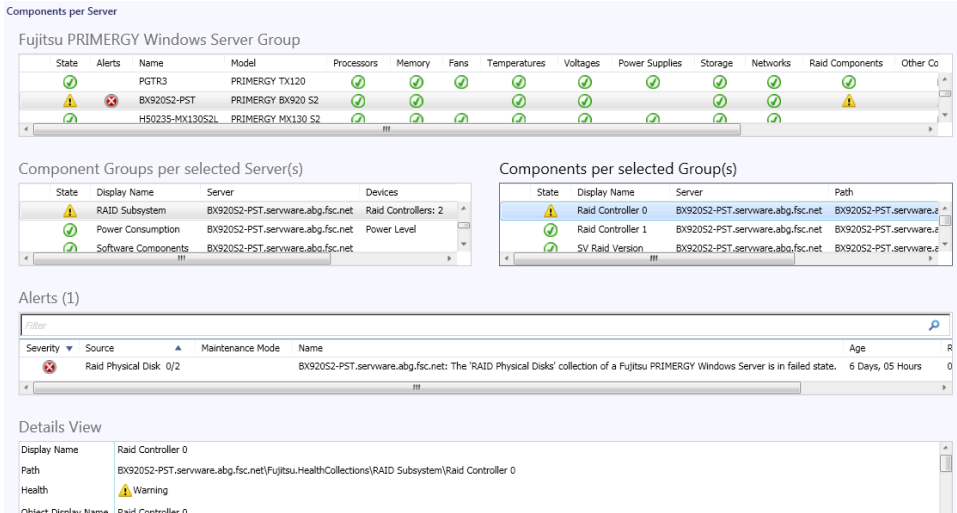


Figure 11 – Components per Windows Server View

## 4.7.10 Views defined by the Performance Monitoring MP

When integrating the *Fujitsu PRIMERGY Windows Server Performance Monitoring* Management Pack a *Performance* node is created in the *Windows Server* pane of the *Fujitsu Systems* node in the SCOM Console. The following views are displayed in this node:

- Ambient Temperature (°C)
- Processor Temperature (°C) and Power Consumption (Watt)
- System and Chassis Power Consumption (Watt)

Each of these views filters the available performance data for the specified data type and displays these in a diagram view. Data to be displayed must be selected in the Legend section of the view.

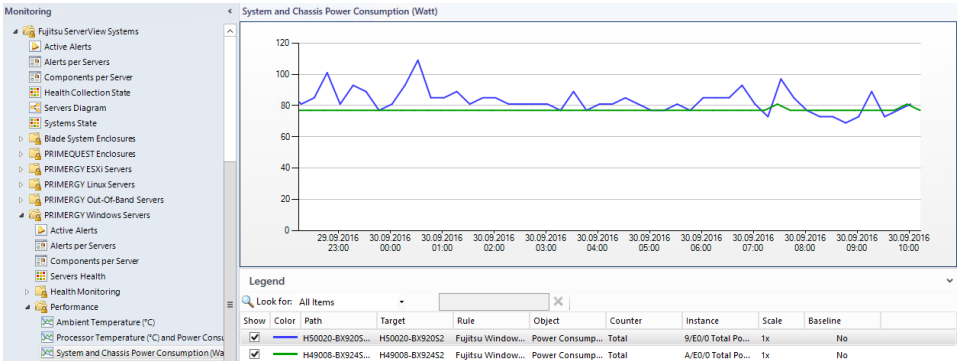


Figure 12 – System and Chassis Power Consumption (Watt)

## 4.8 Health Explorer

The Health Explorer can be started from various views. It shows the components and dependencies in a tree structure. When components are in the *Warning* or *Critical* state, the corresponding subdirectories are automatically expanded in the display.

Two different displays are possible in the right-hand window of the Health Explorer: *Knowledge* and *State Change Events*. Information on what the monitor displays and which actions (resolutions) are possible and recommended is provided under the *Knowledge* tab.

All state transitions (*OK* <-> *Degraded* <-> *Error*) of the component selected from the navigation window on the left are displayed under the *State Change Events* tab.

### Component

Name of the component.

### HealthState

Health State of the component.

### Reason

Reason of the degraded Health State if available.

## 4.9 Fujitsu PRIMERGY Windows Server Tasks

Tasks are actions which can be displayed and executed in different views. They are displayed in the *Actions* window when a PRIMERGY server is highlighted or when PRIMERGY hardware components are selected.

Tasks of the PRIMERGY servers and server components

- Computer Management
- Remote Desktop
- Remote Desktop Console
- Delete PRIMERGY Server Component Inventory
- ServerView RAID Manager
- ServerView Remote Management iRMC
- ServerView Remote Management MMB (Blade Servers only)
- ServerView System Monitor

### 4.9.1 Computer Management

This task is used to start the Microsoft Management Console (MMC application) and permits access to the data of the highlighted PRIMERGY server.

### 4.9.2 Remote Desktop

This task is used to start the Remote Desktop in order to log in on the PRIMERGY server.

### 4.9.3 Remote Desktop Console

This task is used to start the Remote Desktop in console mode in order to log in on the PRIMERGY server.

## 4.9.4 Re-Initialize PRIMERGY Server Component Inventory

The *Fujitsu PRIMERGY Windows Servers* Management Pack keeps track of the amount of components that have been discovered for a server in the server's registry at

HKEY\_LOCAL\_MACHINE\SOFTWARE\Fujitsu\ServerView Suite\SCOM Integration\SVISCOM-Win\PYServerData.

If new components are added to a server, the component inventory is increased and an informational alert is raised. If components are missing, a monitor raises an alert.

This task resets the server components inventory data. The next monitoring cycle generates new inventory data without raising any alerts. Use this task if components have been removed from a server.

## 4.9.5 ServerView RAID Manager

This task is used to call the web console of the ServerView RAID Manager. The task is displayed for all PRIMERGY servers even if ServerView RAID Manager is not installed on the server.

## 4.9.6 ServerView Remote Management iRMC

This task is used to call the console of the integrated Remote Management Controller (iRMC). If a DNS name has been found for the iRMC, the DNS name is called. Otherwise the IPv4 address of the iRMC is used.

## 4.9.7 ServerView Remote Management MMB

This task is only available for blade servers.

It is used to call the console of the Management Board (MMB) of the corresponding BX400 or BX900 chassis.

## 4.9.8 ServerView System Monitor

This task is used to start the web-based ServerView System Monitor, which can be used to examine PRIMERGY Servers in detail.

## 4.10 Events and alerts



This section applies only to alerts for which rules are defined in the Management Pack(s). Other reasons why an alert can be triggered are described in section [4.7.4 Active Alerts View](#).

Alerts remain visible in the *Active Alerts* view until they are explicitly closed (assigned the resolution state *Closed*).

Alerts are independent of monitors and have no influence on the health state of the server. They are used only to display an event.

The following event groups are integrated in the main Management Pack:

- Event Log entries of the scripts in the Management Pack



All alerts have alert suppression enabled.

The following alerts have been moved to separate Management Packs for customers who want to receive even these alerts even though the component health states are fully covered by individual health state monitors.

- SC2.MIB
- RAID.MIB
- HD.MIB
- NTCluster.MIB
- THRESHOLD.MIB
- Duplex Data Manager (DDM.MIB)
- QLogic Fibre Channel Adapters
- Emulex Fibre Channel Adapters (BE2NET, BE2ISCSI)
- Broadcom Network Adapters



- Intel Network Adapters (E1000, E100B, IE10G, ANS Miniport)

Only events with the severity *Warning* or *Critical* are integrated with all *Warning* alerts disabled by default.

### 4.10.1 Enabling and disabling alerts

By default all the events with the severity *Critical* generate an alert, and all the events with the severity *Warning* generate no alert.

To change the default settings override them in the Authoring section of the SCOM Console. The overrides must then be stored in a custom Management Pack which is writable.

## 4.11 Knowledge Base

A Knowledge Base is provided for the events and alerts. Depending on the alert various possible resolutions / actions after error are displayed.

## 5 Working with the Performance Monitoring Management Pack

### 5.1 Create additional Performance Monitoring Views

Make sure the Performance Data collection rules additional views are to be created for are enabled via overrides.



All performance collection rules are disabled by default.

#### 5.1.1 Create a Performance View based on specific rules

- ▶ In the 'My Workspace' Pane or in an unsealed management pack in the 'Monitoring' Pane create a 'Performance View' via 'Right Click' - 'New' - 'Performance View'.
- ▶ Give it a descriptive name, e.g. 'Power Supply Power Consumption'.
- ▶ On the 'Criteria' tab select an existing server group, e.g. 'Windows Servers Group', or create a new group containing only the servers of interest.
- ▶ Select the Checkbox 'collected by specific rules', and click the blue underlined 'specific' in the criteria selection pane.
- ▶ Select one or multiple rules, confirm all selections with 'OK'
- ▶ When the view is displayed, select one or more performance counter instances of interest.



View settings can be changes later via 'Right Click' - 'Properties'.

## 5.1.2 Create a Performance View based on specific performance objects and counters

- ▶ In the 'My Workspace' Pane or an unsealed Management Pack in the 'Monitoring' Pane create a 'Performance View' via 'Right Click' - 'New' - 'Performance View'.
- ▶ Give it a descriptive name, e.g. 'Rack Server Processor Power Consumption'.
- ▶ On the 'Criteria' tab select an existing server group, e.g. 'Windows RX Servers Group', or create a new group containing only the servers of interest.
- ▶ Select the Checkbox 'with a specific object name', and click the underlined 'specific' in the criteria selection pane. The following Object names are supported:
  - Power Consumption
  - Temperature
- ▶ Select the Checkbox 'with a specific counter name', and click the underlined 'specific' in the criteria selection pane.
  - For Power Consumption Sensors the following Counter Names are supported:
    - Total
    - System Chassis
    - Processor
    - Power Supply
    - Other
  - For Temperature Sensors the following Counter Names are supported:
    - Ambient
    - Processor
    - Memory
    - Power Supply
    - System Board
    - Other

## 5.1.3 Create a Dashboard View containing a State and a Performance Widget

The following steps show how to create a dashboard view containing a state widget for the Out-Of-Band Servers as well as a Performance Widget showing the Systems Power Consumption.

### 5.1.3.1 Define the dashboard layout

- ▶ In the 'My Workspace' Pane or an unsealed Management Pack in the 'Monitoring' Pane create a 'Dashboard View' via 'Right Click' - 'New' - 'Dashboard View'.
- ▶ From the templates select 'Grid Layout' from the right column.
- ▶ Add a descriptive name, e.g. 'Server State and Power Consumption'.
- ▶ Select the dashboard layout, e.g. a '2 Cells' layout with horizontal tiles.
- ▶ Confirm settings and create the View layout

### 5.1.3.2 Configure the State Widget

- ▶ Open the newly created view, e.g. 'Server State and Power Consumption'.
- ▶ Select the cell where you want to place the state widget, e.g. the upper tile.
- ▶ From the templates select the State Widget.
- ▶ Give the state widget a descriptive name.
- ▶ Select 'Windows Servers Group' as Object and 'Fujitsu PRIMERGY Windows Server' as Class Scope.  
Note: You can add multiple groups containing Windows Servers if needed.
  - Select the Class by clicking on 'Add'.  
Note: This defines which properties can be displayed as columns later on.
  - Select the Group in the lower part of the wizard  
Note: This defines which objects are shown in the state view.
- ▶ Specify display criteria.
- ▶ Select the columns to display and they are to be sorted.
- ▶ Confirm the settings and create the state widget

### 5.1.3.3 Configuring the Performance Widget

- ▶ Open the newly created view, e.g. 'Server State and Power Consumption'.
- ▶ Select the cell where you want to place the performance widget, e.g. the lower tile.
- ▶ From the templates select the Performance Widget.
- ▶ Give the performance widget a descriptive name, e.g. 'Windows Server Power Consumption'.
- ▶ Select 'Windows Servers Group' as Object in the 'Specify Scope and Counters' page
- ▶ Click '...' to start the group selection.
- ▶ In the 'Specify Scope and Counters' page click 'Add' to start the performance counter selection.
  - Select 'Power Consumption' as Performance Object
  - Select 'Total' as Performance Counter
  - Scroll down the list of available instances and select the 'All' entry, then click 'Add'.
  - Verify the selection and click 'OK'.
- ▶ In the 'Specify Scope and Counters' page click 'Next'.
- ▶ Select a time range for the performance data.
- ▶ Select the columns you want to display in the legend area of the widget. You can rearrange the order as needed.
- ▶ Confirm Settings and Click 'Create'

The final Dashboard View with State and Performance Widget:

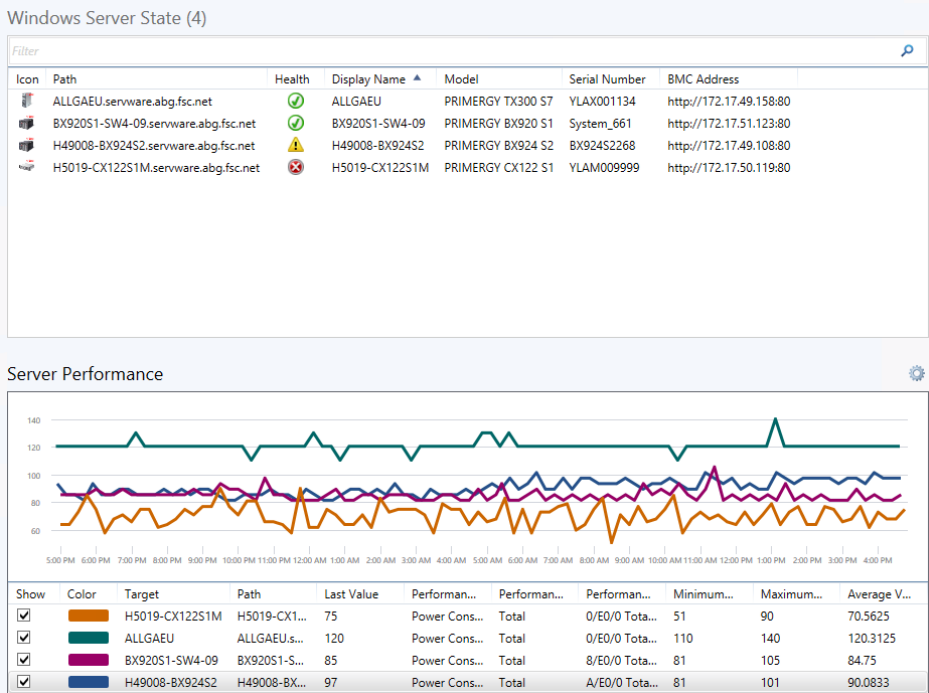


Figure 13 – Dashboard View containing a State and a Performance Widget

## 5.1.4 24 Hour Performance Dashboard View

In order to illustrate the possibilities of dashboard views the following screenshot is shown. This view contains a status widget which allows quick filtering the list of Windows servers and 2 contextual performance widgets showing the list of Power Consumption and Temperature values over the last 24 hours for the selected server(s). This allows a quick overview or comparison of different server values without the need for manually creating a separate view containing only the selected performance counter instances for the specific comparison.



While Microsoft currently provides a contextual health and alert widget, unfortunately a contextual performance widget is not available. There are some workarounds on SCOM related Internet blogs available which address this topic, but some technical limitations from the underlying standard SCOM performance widget still exist (e.g. sorting preferences and selected performance instances are not saved and reset to default when the re-entering the view).



Due to the existing limitations of SCOM the 24 hour performance dashboard view is not distributed with the Windows Performance Monitoring Management Pack. An evaluation copy which will be provided 'as-is' can be requested by sending a mail to <mailto:PRIMERGY-PM@ts.fujitsu.com?Subject=Windows Performance Monitoring Add-On Management Pack>.

Starting points for the technical interested are (but not limited to):

[https://blogs.msdn.microsoft.com/wei\\_out\\_there\\_with\\_system\\_center/2015/09/11/opsmgr-sample-contextual-performance-widget-template/](https://blogs.msdn.microsoft.com/wei_out_there_with_system_center/2015/09/11/opsmgr-sample-contextual-performance-widget-template/)

<https://gallery.technet.microsoft.com/Sample-Management-Pack-d03d2cf3>

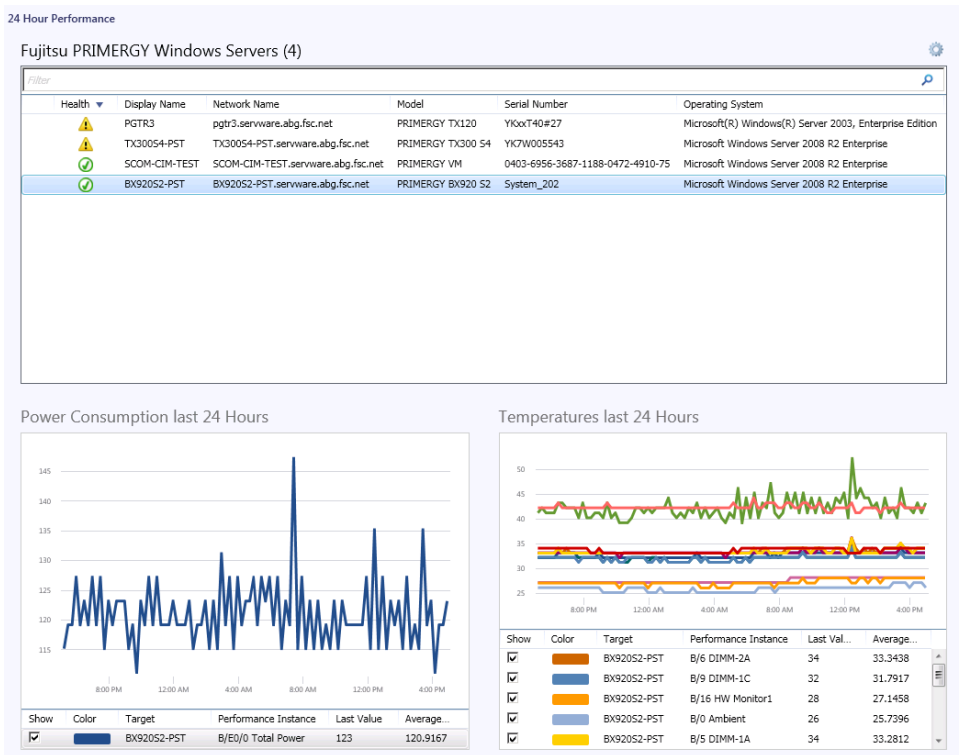


Figure 14 – 24 Hour Performance Dashboard View

## 6 Appendix

### 6.1 Supported PRIMERGY servers

The ServerView Windows Server Integration Pack does not itself support PRIMERGY servers but relies on ServerView Agents and CIM Provider installed on the server to provide server hardware data. PRIMERGY support therefore depends on the ServerView Agents installed on the monitored system.

Please refer to the ServerView Agents' release notes for detailed information on PRIMERGY support.

### 6.2 Entries in the Operations Manager's Event Log

The scripts for discovering and monitoring the PRIMERGY servers and their components write messages to the Operations Manager's Event Log when an error occurs.

These entries can be found on the monitored servers under the name *Health Service Script*, while the message text specifies which cscript generated the message.

Rules defined in the Management Pack check the event log for the above mentioned entries, which, if present, are displayed in the *Active Alerts* view.



Entries for errors are switched on; entries for warnings are switched off.

### 6.3 Creating test entries in the Windows Event Log

To check whether an alert is enabled, disabled, or recognized, you can create test entries for these events in the Event Log of the relevant server using PowerShell.



## 6.4 Creating log files

Log files can be created for error analysis. The log files are stored in the subdirectory *SVISCOM\SVISCOM-Win* of the directory entered in the system environment variable *TEMP*. Usually this is the *C:\Windows\TEMP* directory (where *C:* represents the system partition in this example).

Logging options are defined in the file *SVISCOMLog.ini* in this folder. If the file does not exist or was created by an older version of the Management Pack, a copy of the file with the name *SVISCOMLog.in\_* is generated on each server discovery in the *%TEMP%\SVISCOM\SVISCOM-Win* folder.



Note that changes to the logging options will only be added to the *SVISCOMLog.in\_* file. *SVISCOMLog.ini* from an older version of the ServerView Windows Server Integration Pack may need to be updated accordingly.

*SVISCOMLog.in\_* contains debug options for all discovery and monitoring features of the management pack. See *SVISCOMLog.in\_* on any target system for details.

In the case of error analysis using log files proceed as follows.

- ▶ Rename *SVISCOMLog.in\_* on the target server to *SVISCOMLog.ini*. If *SVISCOMLog.ini* already exists, check that all options of *SVISCOMLog.in\_* also exist in *SVISCOMLog.ini*.
- ▶ Check the debug options (documented in detail within the *SVISCOMLog.in\_* file) for each feature to be monitored and set to the desired value.

The following log files are created as required:

- *PRIMERGYServerDiscoveryTrace\_<servername>.log*
- *PRIMERGYComponentsMonitorTrace\_<servername>\_ALL.log*
- *PRIMERGYServerFCEvents\_<servername>.log*
- *ResetPYServerData\_<servername>.log*

These files must be sent to Fujitsu Support for further analysis.

If you wish to disable the creation of log files again, delete or rename *SVISCOMLog.ini* or change the logging options within the file.

## 6.4.1 Currentness of log files

When Fujitsu Management Packs are imported log files are generated promptly only if the initialization file is already available.

If the management pack already is imported log files are generated depending on the execution interval of the discovery or monitoring scripts.

Up to 4 hours are necessary for all log files to be generated.



The server discovery is executed by default every 4 hours.

After the component discovery was successful, monitoring is run every 3 minutes.

### Alternatively:

To create a current set of discovery log files, put the server in maintenance mode for a short time and let SCOM exit the maintenance mode. SCOM executes the server and component discovery automatically after maintenance mode has ended.

## 6.5 Troubleshooting

### 6.5.1 Use ServerView System Monitor to examine a PRIMERGY Server

If a PRIMERGY server seems to have a problem (e.g. the PRIMERGY Overall State is bad) and the cause of this problem cannot be determined via SCOM, it may help to use the System Monitor for closer examination.

Highlight the server and use the ServerView System Monitor task to start System Monitor.

### 6.5.2 No event logging of the controller driver(s)

Not all controller drivers create events in the Windows Event Log by default. For detailed information on activating the event logging, see the manual or readme file of the controller drivers.

### **6.5.3 Enable / Disable Windows Installer Logging (Debug)**

In case there are problems with the installation procedure refer to the following Microsoft knowledge base article (<http://support.microsoft.com/kb/223300>) that describes how to enable and disable logging.

## **6.6 Hints and known issues**

-