

White paper

Integrating PRIMERGY Servers into HP Systems Insight Manager

This White Paper describes the integration of PRIMERGY Servers into an established HP server infrastructure using management tools of the PRIMERGY ServerView® Suite to build on.



Content	
Introduction	2
1 Management Summary	2
Why server management?	2
Why "integration"?	2
Highlights of ServerView® Integration	2
ServerView® Integration Components	2
2 Server Management Solutions	3
2.1 ServerView® integration into HP SIM at a glance:	3
3 Installing and Configuring the ServerView® Suite	4
3.1 Installing ServerView® SNMP Agents	4
3.2 Installing ServerView® Operations Manager	4
4 Loading ServerView® MIBs into HP SIM	5
5 Configuring HP SIM to recognize PRIMERGY Servers	5
5.1 Discovery	5
5.2 Adding a PRIMERGY system with W2K3 Operation System or no WBEM access	6
5.3 Detecting a PRIMERGY's management controller	7
6 Testing the Integration	8
6.1 Discovering PRIMERGY Systems	8
6.3 Calling ServerView® from HP SIM	8
6.4 Generating Test Traps	10
7 Configure Additional Management Software	11
7.1 Vulnerability and Patch Management (VPM)	11
7.2 Virtual Machine Manager (VMM)	11
7.3 Remote Task Execution via SSH	11
8 Limitations and Caveats	12
9 Uninstalling the ServerView® Integration	12
Appendix A: ServerView® MIBs	13
Enclosure and Environment Management	13
RAID Management	13

Introduction

This White Paper describes the integration of PRIMERGY Servers into an established HP server infrastructure using management tools of the ServerView® Suite (version 5.00 or higher) to build on. Fujitsu Technology Solutions delivers the tools to enable monitoring of PRIMERGY servers in heterogeneous server farms using HP Systems Insight Manager. System messages are passed on and displayed on the central management console using the alarm management facility in HP SIM; the messages are based on the various "Management Information Bases" (MIBs) supplied with ServerView®. ServerView® Suite is the management system of PRIMERGY servers from Fujitsu Technology Solutions. It administrates all PRIMERGY servers.

1 Management Summary

Why server management?

New applications and IT concepts as well as the increasing complexity of IT structures result in the need for a central server administration concept. Because of diminishing budgets the availability and manageability of IT systems are more important than ever before. Virtually hundred-percent availability of core business applications is often required, while the operation and management of servers should be as simple and reliable as possible.

As experience shows, about 80 % of the total cost of ownership of IT systems is incurred after procurement due to server and network administration and the need to uphold security standards and guarantee the provision of maintenance and service work. The PRIMERGY management concept covering the ServerView® management suite is a step toward trouble-free operation of IT systems. It helps to reduce the total cost of ownership for IT infrastructures dramatically.

Despite focusing on the management of PRIMERGY servers, the ServerView® Suite is also a solution open for integration. It provides extremely easy, favorable and reliable integration into almost any 3rd-party management systems on the basis of the SNMP standard.

Why "integration"?

Most vendor specific management solutions similar to ServerView® Suite offer extensive functions for server administration and server life cycle management. Many of the users of these solutions use this platform-specific management as "their" Central Server Management solution. They are familiar with the handling and functionality, and having invested a lot in establishing appropriate skills are not willing to invest too much in additional management tools.

As a consequence these users demand that PRIMERGY servers should be monitored and managed in an efficient way by means of integration into the known management system keeping the level of additional effort and platform-specific training as low as possible.

Highlights of ServerView® Integration

ServerView® integration into HP SIM provides:

- Discovery and recognition of PRIMERGY servers
- Management of PRIMERGY servers via one central HP SIM console (single point of administration)
- Reliable notification of PRIMERGY Events in the SIM Alarm Console - different colors indicate the severity of an event
- Ability to launch ServerView® Operations Manager or Remote System Monitor for in-depth analysis

With its integration of ServerView® Suite into HP SIM, Fujitsu Technology Solutions consistently supports only published interfaces and guidelines provided by HP.

ServerView® Integration Components

The following components comprise the ServerView® Integration. All components are located on the ServerView® Suite DVD follow Software Products - ServerView -> Integration Solutions -> ServerView HP SIM Integration (ServerView® Suite DVD online:

http://download.ts.fujitsu.com/prim_supportcd/start.html):

- This ServerView® Integration Whitepaper
- Fujitsu Technology Solutions' MIBs
- The ServerView® HP Systems Insight Manager Integration Kit (SVToSim.zip):
 - The MIB tools svtosim-loadmibs.cmd, svtosim-domibs.cmd, svtosim-getinfo.vbs, svtosim-unloadmibs.cmd
 - Rules and tools for the HP Systems Insight Manager import tool (svtosim-single.cmd, svtosim-single-remove.cmd)
 - Scripts to enable or disable the HP SIM Integration of Fujitsu Technology Solutions' management controller (iRMC-simintegration-enable.xml, iRMC-simintegration-disable.xml)

2 Server Management Solutions

PRIMERGY ServerView® Suite is an easy-to-use, comprehensive set of management programs for monitoring and managing PRIMERGY systems. A powerful alarm management facility that can also be configured individually over the Internet ensures rapid and secure forwarding of system messages to administrators or service providers. ServerView® uses standardized protocols and interfaces. Administrators are provided with a quick and reliable overview of the operating status of the systems, utilization trends and possible sources of errors. The individually configurable alarm management facility ensures that predefined administrators or service providers can respond rapidly.

The ServerView® Suite management software consists of the ServerView® Operations Manager, the front-end for the Management Station (manager / monitoring station), and the ServerView® SNMP Agents for the servers to be monitored.

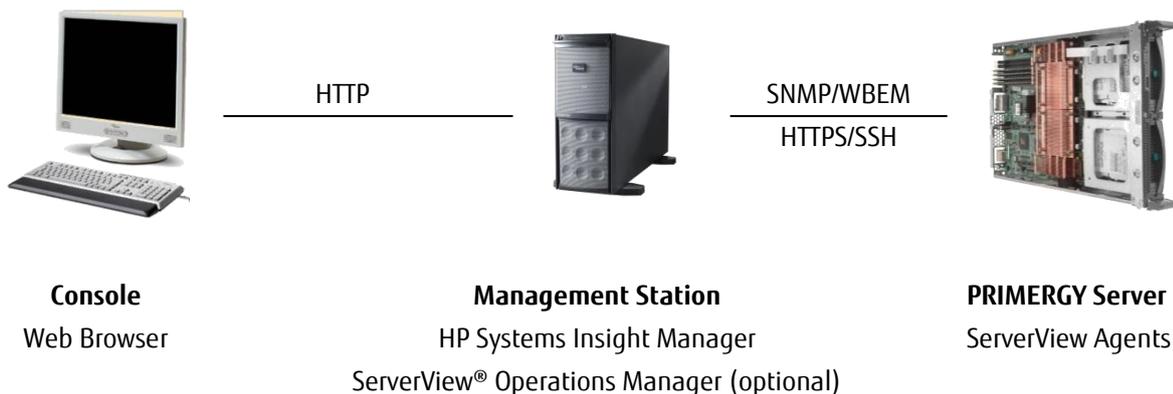
HP Systems Insight Manager is the set of management tools for monitoring and managing HP Servers.

This paper describes how to integrate PRIMERGY servers into an HP Server environment managed by HP Systems Insight Manager.

2.1 ServerView® integration into HP SIM at a glance:

- Install ServerView® SNMP Agents on the PRIMERGY server so it can communicate with HP SIM
- Optional: Install ServerView® Operations Manager on a management station of your choice for in-depth analysis of PRIMERGY servers and test trap generation
- Load ServerView® MIBs into HP SIM so it can properly understand the events generated by the ServerView® Agents
- Configure HP SIM to recognize PRIMERGY servers
- Test the integration
- Configure additional management software

The architecture of the integration solution will be as follows:



ServerView® Agents are installed on the PRIMERGY server to be monitored. They provide information about the system's health status and generate SNMP traps should a problem be detected.

The actual monitoring software (i.e. both HP Systems Insight Manager and the ServerView® Operations Manager) reside on the management station. Note that it would also be possible to install the ServerView® Operations Manager on a separate management station.

Finally, the user accesses the management station using a standard web browser.

3 Installing and Configuring the ServerView® Suite

3.1 Installing ServerView® SNMP Agents

The ServerView® Agents can be installed together with the Windows OS using the ServerView® Installation Manager or after OS installation using the ServerView® Suite Software CD.

Installation of the ServerView® Agents is described in chapter 6 of the ServerView® Suite installation manual, which can be found on the ServerBooks CD (included in the ServerView® Installation Manager package). An online version of the related installation manual is also available in the Internet: <http://manuals.ts.fujitsu.com/serverbooks/>

In the lefthand-side navigation bar choose 'Industry Standard Servers' - 'Software' then select 'PRIMERGY ServerView Suite' and 'ServerView Suite Installation Manuals' in the two selection bars in the main frame.

After the ServerView® Agents have been installed on the managed server the next step is to configure the SNMP service to match your HP SIM configuration:

1. Configure SNMP traps to be sent to the management station where HP SIM is installed
2. Configure SNMP access so that the HP SIM is able to access the server using SNMP (read-only is sufficient)

How this is accomplished depends on the operating system. For details please refer to the related ServerView® Operations Manager installation guide on the ServerBooks CD.

To configure SNMP access is optional for Windows servers as HP-SIM also uses WBEM to access its managed servers. Configuring SNMP access is required for Linux servers.

The current SNMP community used by HP SIM can be determined in the following way:

1. Click Options -> Protocol Settings -> Global Protocol Settings. The Global Protocol Settings window will appear
2. Scroll down to the Default SNMP settings section
3. Click on Global Credentials
4. Click OK to accept the settings.

In addition to SNMP-based discovery, HP SIM also uses WBEM for system discovery when Web-Based Enterprise Management (WBEM) services are enabled and configured. In order to make use of the information provided by WMI, the following steps are necessary:

1. Navigate to Options -> Protocol Settings -> Global Protocol Settings, tick the 'Enable WBEM' box and click on 'Global Credentials'. The 'Global Credentials' window will appear.
2. Enter as many default user names and passwords as needed. For Windows-based systems, the user name should include the domain name, for example domainname\username.
3. In order to minimize search time, frequently used root and administrator passwords should be listed first.
4. Click OK to accept the settings

3.2 Installing ServerView® Operations Manager

ServerView® Operations Manager can be used as an element manager to provide you with more information about a PRIMERGY server than HP SIM has to offer. Therefore, it should be installed on a management station within your network. A good choice would be the same system that HP SIM is installed on.

If the OS is installed, ServerView® Operations Manager can be installed with user guidance from the ServerView® Suite DVD (online version: http://download.ts.fujitsu.com/prim_supportcd/start.html)

Installation of ServerView® Operations Manager is described in chapter 5 of the installation manual, which can be found on the ServerBooks CD. An online version of the related installation manual is also available: <http://manuals.ts.fujitsu.com/serverbooks/>

In the lefthand-side navigation bar choose 'Industry Standard Servers' - 'Software' then select 'PRIMERGY ServerView Suite' and 'ServerView Suite Installation Manuals' in the two selection bars in the main frame.

Note:

ServerView® Operations Manager V6.20 should not be used for HP-SIM integration, as there is a problem with the SVOM call that HP-SIM generates for the Custom Management Page. Please use either a newer or an older version of ServerView® Operations Manager.

4 Loading ServerView® MIBs into HP SIM

The ServerView® MIB files that describe what events may be generated by PRIMERGY servers can be found on the 'Software CD' in the Software\ServerView\MIBs directory. These MIBs are integrated into HP SIM by performing the following steps:

1. Unzip ServerView® integration toolkit into a directory of your choice.
2. Unzip SNMPMIBs.zip into a directory into a subfolder SNMPMIBs of that directory.
3. Open a command window (cmd.exe)
4. Using the cd command, change to the ServerView® integration toolkit directory.
5. Enter the svtosim-loadmibs.cmd command. Relevant ServerView® MIBs are now copied into the HP-SIM MIBs folder where they are compiled and integrated into HP SIM. This process takes some time.

HP SIM is now able to understand SNMP traps generated by ServerView®.

Note:

If the user account this process is conducted with does not have Administrator rights within HP-SIM, compiling and integrating the MIBs will fail. In this case add a user account and password to the svtosim-loadmibs command, e.g.

```
svtosim-loadmibs.cmd -user "Domain\User" -pwd "Password"
```

5 Configuring HP SIM to recognize PRIMERGY Servers

5.1 Discovery

When a new system is detected via a ping sweep or when receiving an SNMP trap, it is added to the HP SIM database. The System Type Manager then performs a sequence of queries to the new device to determine its identity. The steps below configure HP SIM to look for specific information within the ServerView® MIBs to tell the System Type Manager that the device found is a PRIMERGY server.

The ServerView® integration toolkit offers a batch file (svtosim-single.cmd) to configure the Device Type Manager to recognize PRIMERGY servers. It also configures the Custom Management Page with HP-SIM for PRIMERGY servers to point to either ServerView® Operations Manager Single System View or to the Remote System Monitor of the ServerView® Agents of the server.

Notes:

- Using the Remote System Monitor requires ServerView® Agents V7.01 or later on the monitored server
- The Custom Management Page will be set for all PRIMERGY servers. For any server with ServerView® Agents lower than V7.01 there will be no Custom Management Page available.
- PRIMERGY server discovery requires HP's WMIMapper. Make sure to have the latest version installed with HP-SIM.

Follow these steps:

1. If you already have a working ServerView® HP-SIM Integration Kit, uninstall it as described in section 9
2. On the ServerView® Software CD, browse to the '\Software\Integration_Solutions\HP_SIM' directory
3. Unzip SVtoSIM.zip into a directory of your choice.
4. By default the integration provided by svtosim-single.cmd will use ServerView® Operations Manager Single System View as Custom Management Page. The integration script assumes that ServerView® Operations Manager and HP SIM are installed on the management station where the user's web browser is started and the SNMP community string is 'public'.

To adapt the kit to the real configuration the following case-sensitive command line options are available:

- a. Using `-mon svom` or `-mon sysmon` defines whether ServerView® Operations Manager Single System View or the Remote System Monitor of the ServerView® Agents is to be used for the Custom Management Page.
 - b. When ServerView® Operations Manager is to be used for the Custom Management Page, option `-svomserver SERVER` changes the location where ServerView® Operations Manager is installed.
 - c. When ServerView® Operations Manager is to be used for the Custom Management Page, option `-svomcomm COMMUNITY` changes the SNMP community string.
5. Open a command window (cmd.exe)
 6. Change to the ServerView® integration toolkit directory where you unzipped svtosim-single.cmd
 7. Call svtosim-single.cmd using the command line options as required by your environment.

Note:

The following ports are used by ServerView®:

Port Number	Usage
3170	Secure HTTPS access for SV Operations Manager
3172	Secure HTTPS access for Remote System Monitor.

Now that the new PRIMERGY server device types have been added to the HP SIM database (with two entries per PRIMERGY server, one for a potential Windows-based system and one for a potential Linux-based system) HP SIM can properly discover and identify PRIMERGY servers.

Notes:

- If the user account this step is conducted with does not have Administrator rights within HP-SIM, integrating the rules will fail. In this case add a user account and password to the svtosim-single command, e.g.
svtosim-single.cmd -user "Domain\User" -pwd "Password"
- Using WBEM services for discovery with W2K8 or later enables very simplified discovery rules for PRIMERGY Servers. This version of the HP Integration Toolkit only supports PRIMERGY servers with W2K8 or later or Linux.

5.2 Adding a PRIMERGY system with W2K3 Operation System or no WBEM access

Using svtosim-single.cmd as guideline set up a batch file containing the rules for both Windows and Linux for the new server. Add HP-SIM administrator account details if necessary:

```
mxstm [--user "<user>" --pass="<password>"] -a -n "<newPrimergyModel>" -p snmp -x type=Server -x priority=1 -x osname="Microsoft Windows" -x sysoid=1.3.6.1.4.1.311.1.1.3.1.2 -x sysoidrule=3 -x oid=1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 -x oidval="<newPrimergyValue>" -x oidrule=1 -x url=127.0.0.1:3169/ServerView/ServerView.html? IPAddress=$IPADDRESS &Community=<community>
mxstm [--user "<user>" --pass="<password>"] -a -n "<newPrimergyModel>" -p snmp -x type=Server -x priority=1 -x osname="Linux" -x sysoid=1.3.6.1.4.1.8072.3.2.10 -x sysoidrule=3 -x oid=1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 -x oidval="<newPrimergyValue>" -x oidrule=1 -x url=127.0.0.1:3169/ServerView/ServerView.html? IPAddress=$IPADDRESS &Community=<community>
```

where

- <newPrimergyModel> is the name of the PRIMERGY which will be shown in the 'All server' list and identifies the corresponding rule in 'Manage System Types',
- <newPrimergyValue> is the name of the PRIMERGY system exactly as delivered by any SNMP tool to OID .1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4.
- <community> is a SNMP community string for read access.
- If using the SystemMonitor is desired, change the url parameter to [https://\\$IPADDRESS:3172/ssm/desktop/](https://$IPADDRESS:3172/ssm/desktop/)

Note:

Please note that the ServerView® Operations Manager URL is case-sensitive, the SystemMonitor URL is not.

For more information on the mxstm command, please consult the HP-SIM CLI Guide. To get the PRIMERGY's name use for example snmputil:

```
snmputil getnext <host> <community> .1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4
```

where <host> is either the hostname or the IP address of the new PRIMERGY and <community> is a SNMP community string for read access.

To create the rule to identify a new PRIMERGY system directly in HP-SIM use menu 'Options' - 'Manage System Types'. After the list of rules is displayed click 'New'. On the form for new rule carry out the following steps:

1. copy the OID 1.3.6.1.4.1.231.2.10.2.2.5.10.3.1.4 into the field 'MIB variable object identifier' and click 'Retrieve from system'. The OID will appear in the new field below 'Retrieve from system'. Supply the community string and the PRIMERGY's hostname or IP and click 'Get Response'. The name (value of OID) will be displayed below after 'Response value'. Copy it and paste into the field 'Object value';
2. fill-in the field 'System object identifier' with OID 1.3.6.1.4.1.311.1.1.3.1.2 for Windows or with OID 1.3.6.1.4.1.8072.3.2.10 for Linux;
3. select 'Server' in the combobox 'System type';
4. fill in the field 'Product model' with an identification name of this rule (it will be shown in the 'All server' list);

- fill in the field 'Custom management page' with
 'https://<SvomServer>:3170/serverView/serverview.html?IPAddress=\$ipaddress&Community=<community>' where <SvomServer> is the server where SVOM is installed and <community> is a SNMP community string for read access.
 or, if using the SystemMonitor is desired, fill in 'Custom management page' with
 'https://\$IPADDRESS:3172/ssm/desktop/'

5.3 Detecting a PRIMERGY's management controller

Management controllers in PRIMERGY Servers (iRMC S2, iRMC S3, iRMC S4) are per default set up to answer HP SIM's request to identify as management controllers. After both the PRIMERGY server and its management controller have been integrated into HP SIM the management controller is associated to the server automatically.

Note:

iRMC S4 can only be detected as a Management Controller with newer versions of HP-SIM. Use at least V7.4.

Once the management controller has been detected and associated it is connected to the server in both the server list and the system's page. Please note that the iRMC is always recognized as 'Lights-Out 100'.

Server list:

HS Summary: 0 Critical 0 Major 0 Minor 4 Normal 0 Disabled 0 Unknown Total: 4									
System Name	System Type	System Address	Product Name	OS Name					
172.17.51.102 in Server rx300s5-pst	Management Processor	172.17.51.102	Lights-Out 100 Remote ...	Embedded					
hpsim-pst Hosted by tx300s4-pst	Server	172.17.55.249		Microsoft Windows Serv...					
rx300s5-pst	Server	172.17.51.2	PRIMERGY RX300 S5	Microsoft(R) Windows(R)...					
tx300s4-pst	Server	172.17.50.22	PRIMERGY TX300 S4	Microsoft Windows Serv...					

Figure 1: ServerList with associated management controller

System page:

rx300s5-pst (PRIMERGY RX300 S5)
 Go back to [All Systems](#)

System | **Tools & Links** | Events | Essentials | Quick Launch...

System Status

- Health Status
- Management Processor Status
- Aggregate Event Status

More Information

- Properties
- Lights-Out 100 Remote Management

Identification

Address	172.17.51.2
Preferred System Name	rx300s5-pst
Network Name	rx300s5-pst.servware.abg.fsc.net
Serial Number	YKJB000068
Product Number	861721
UUID	00000000-0000-0000-0000-001999464F8C

Product Description

Asset Information

Management Processor

Name	172.17.51.102
Address	172.17.51.102
Management Processor Homepage	Lights-Out 100 Remote Management
Model	Lights-Out 100 Remote Management

Figure 2: System Page with associated management controller

If the automatic detection and association of PRIMERGY's management controllers is not desired, it can be disabled via the iRMC webinterface. Log into the iRMC, select 'Server Management' in the navigation bar on the left side and un-check the 'HP SIM Integration Disabled' box in the 'HP System Insight Manager (HP SIM) Integration Options' section.

To re-enable the management controller's HP SIM integration feature, just check the box.

Disabling the management controller's HP SIM integration feature can also be achieved automatically if the server's OS is Windows. Copy "iRMC-simintegration-disable.xml" into the folder %ProgramFiles%\Fujitsu\ServerView Suite\Agents\Server

ControlIncoming, this causes the file to be processed automatically. After being processed it will be renamed to "iRMC-simintegration-disable.out". To re-enable the management controller's HP SIM integration feature, use "iRMC-simintegration-enable.xml".

On Linux the feature can be controlled via the command line. To enable it type "eecdcp -c oc=E002 oe=1968 oi=0 cab=0 0x'01'" or type "eecdcp -c oc=E002 oe=1968 oi=0 cab=0 0x'00'" to disable the feature.

6 Testing the Integration

6.1 Discovering PRIMERGY Systems

Once the Device Type Manager settings described above have been implemented, any PRIMERGY system now known by HP System Insight Manager will be detected automatically by the usual discovery sweeps.

Please note that in order for the integration to work properly all PRIMERGY systems have to be re-identified e.g. by removing them from the system list and discovering them anew.

HS	MP	SW	ES	System Name	System Type	System Address	Product Name	OS Name
✓				172.17.51.237	Enclosure	172.17.51.237	PRIMERGY BX900 MMB	
✓				bx400s1em_044	Enclosure	172.17.49.237	PRIMERGY BX400 MMB	
✓		?		hpsim-pst	Server	172.17.55.249	Virtual Machine	Microsoft Windows Serv...
✓	✓		✗	rx300s5-stk	Server	172.17.51.2	PRIMERGY RX300 S5	Red Hat Enterprise Lin...
✓				rx300s5-stk-irmc in Server rx300s5-stk	Management Processor	172.17.51.102	Lights-Out 100 Remote ...	Embedded
✓	✓			tx200s7-pst	Server	172.17.49.1	PRIMERGY TX200 S7	Microsoft Windows Serv...
?				tx200s7-pst_New Virtual Machine Hosted by tx200s7-pst	Server			
✗			✗	tx200s7-pst_SCCM2012R2_SiteServer Hosted by tx200s7-pst	Server	10.40.0.1		Windows Server 2012 St...
✓				tx200s7-pst-irmc in Server tx200s7-pst	Management Processor	172.17.49.101	Lights-Out 100 Remote ...	Embedded
?	✓		✗	tx300s4-pst	Server	172.17.50.22	PRIMERGY TX300 S4	Microsoft Windows Serv...
?				tx300s4-pst_PXE Target Hosted by tx300s4-pst	Server			
?				tx300s4-pst_SCCM2012R2_SiteServer Hosted by tx300s4-pst	Server			
✓			✓	tx300s4-pst-irmc in Server tx300s4-pst	Management Processor	172.17.50.122	Lights-Out 100 Remote ...	Embedded
✓	✓		?	tx300s8-stk	Server	172.17.54.15	PRIMERGY TX300 S8	SUSE Linux Enterprise ...
✓				tx300s8-stk-irmc in Server tx300s8-stk	Management Processor	172.17.54.115	Lights-Out 100 Remote ...	Embedded

Figure 3: PRIMERGY Servers within the HP SIM Server List

6.3 Calling ServerView® from HP SIM

In order to obtain more detailed information about your PRIMERGY server, it is possible to start the ServerView® Operations Manager or the SystemMoitor for a single server from the HP SIM console. In order to do so, perform the following steps:

1. In the All Systems page, click on the name or IP address of the server you want to examine.
1. The System Page will open.
2. Click on the Tools & Links tab (see Figure 5)
3. Select the link called 'Custom management page'. A ServerView® Operations Manager or a Remote System Monitor window providing details about the selected PRIMERGY server will appear (see Figures 6 and 7).

rx300s5-pst (PRIMERGY RX300 S5)

[Go back to All Systems](#)

System Tools & Links Events Essentials Quick Launch...

System Web Application Pages: rx300s5-pst

[Custom management page](#)
[Default WebServer](#)

HP Systems Insight Manager Pages

[System Protocol Settings](#)
[Data Collection Report](#)
[System Credentials](#)
[Edit System Properties](#)
[Suspend/Resume Monitoring](#)

iLO links

[Telnet to the server's iLO](#)

Figure 5: System Page

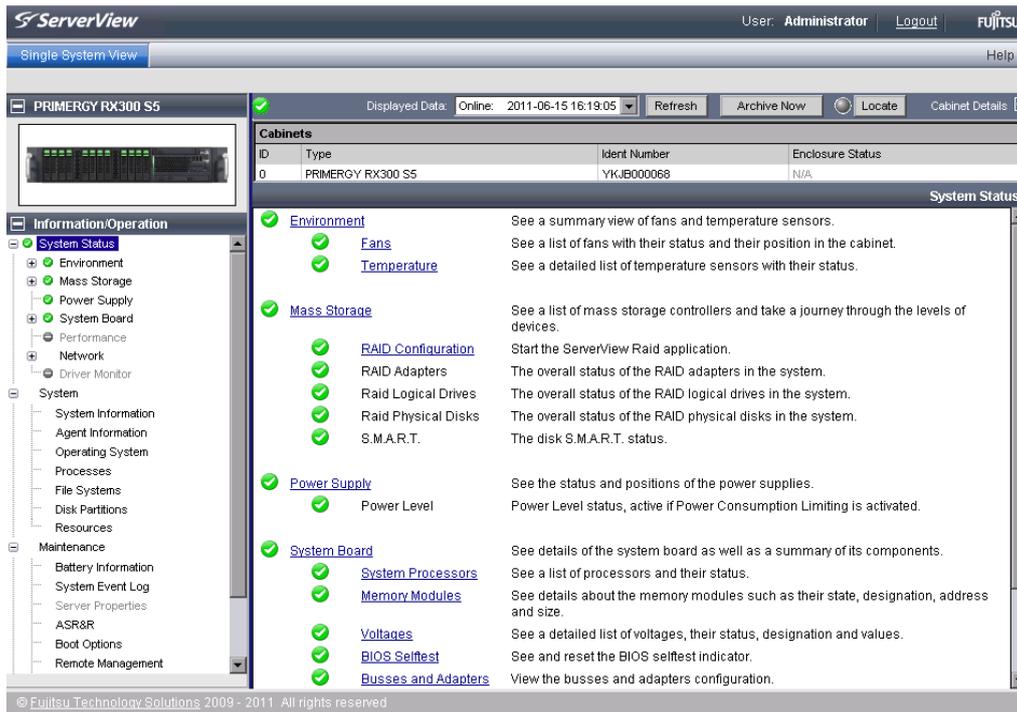


Figure 6: ServerView® Operations Manager window

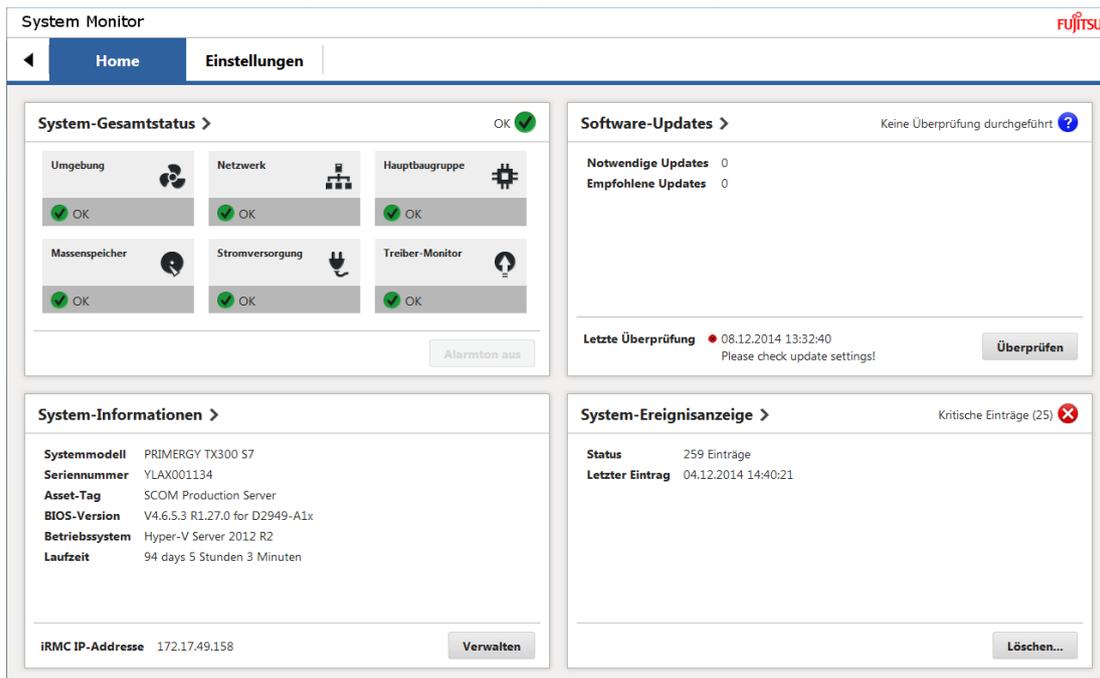


Figure 7: Remote System Monitor

6.4 Generating Test Traps

Of all the information in the MIB files, the traps or error indications sent by the ServerView® Agents are of primary interest to an administrator. Events may cause different reactions according to their severity, with “informational” traps being just for the information of the administrator, and “critical” events, for example, requiring instant attention.

In order to test that events are passed correctly from the managed server to HP SIM, a test trap can be generated by performing the following steps:

1. Start the ServerView® front-end. After the initial screen it will display the server list (see Figure 7).
2. Right-click on the server you want to test and select “Test connectivity”
3. In HP SIM, select All Events from the left-hand frame and note the events that have been generated.

7 Configure Additional Management Software

In addition to the integration mechanisms described above there are some HP SIM software components that also work for PRIMERGY servers. These components include

- Vulnerability and Patch Management (VPM)
- Virtual Machine Manager (VMM)
- Remote Task Execution via SSH

The following sections describe how this can be accomplished.

7.1 Vulnerability and Patch Management (VPM)

The integration of VPM helps to identify and resolve security vulnerabilities. In order to install and configure VPM for PRIMERGY servers the following steps are necessary:

1. Install VPM on the same server as HP SIM
2. Select the managed node
3. Deploy the VPM Agent by selecting Deploy -> Vulnerability and Patch Management -> VPM Patch Agent
4. Deploy license key for VPM by selecting Deploy -> License Manager -> Deploy Keys
5. Re-Identify the managed system. This produces an icon in the VPM column.
6. Select Tools -> System Information -> System Page, then select 'Vulnerability Status'.
This can also be achieved by selecting the icon in the VPM column.
7. Select 'Scan for Vulnerability' and complete the wizard

7.2 Virtual Machine Manager (VMM)

The Virtual Machine Management Pack provides central management and control of VMWare and Microsoft virtual machines and provides physical host to virtual machine association.

For setting up VMM in HP SIM, the following steps are necessary:

1. Select the managed node
2. Deploy the VMM Agent by selecting Deploy -> Deploy Drivers, Firmware and Agent -> Install VMM Agent -> Windows
3. Check whether HP SIM detected the system's serial number. If not supply the serial number manually (via 'Edit System properties') otherwise the license will not become active.
4. Deploy License Key for VMM by selecting the VMM server keys. Select Deploy -> License Manager -> Deploy Keys
5. Re-Identify the managed system. A green checkmark icon appears.
6. Select Tools -> System Information -> System Page, the select 'Virtual Machines'.
This can also be done by clicking the icon in the VMM column.

7.3 Remote Task Execution via SSH

Installing and configuring SSH allows running tasks and scheduled jobs from HP SIM on PRIMERGY servers, e.g. use OpenSSH. After OpenSSH is installed, a copy of the SSH-generated public key can be copied from HP SIM to the managed server. To do this from the GUI, the following steps are necessary:

1. Select the managed node
2. Select Configure -> Configure and Repair Agents
3. Enter the sign in credentials for an administrator of the managed system
4. Uncheck 'Configure SNMP' since this function only works with HP servers
5. Uncheck 'Trust relationship', 'Set administrator password for Insight Management Agents version 7.1 or earlier' and 'Create subscriptions for WBEM events'
6. Select 'Configure secure shell (SSH) access, then select 'Host based authentication'.
7. Click 'Run Now'

8 Limitations and Caveats

With iRMC controllers with older firmware versions the automatic detection and association of the management controller to its server is not implemented. Required minimum iRMC firmware versions are:

- iRMC S1: no fix available
- iRMC S2: 5.59A
- iRMC S3: 6.27A
- iRMC S4: any. HP-SIM version at least V7.4.

As there are no applicable HP version control agents for PRIMERGY servers, the Management Processor and Software status will always be 'unknown' or blank. HP SIM cannot display a graphical picture of blade enclosures for PRIMERGY servers or associate the servers with rack or enclosure information.

Sometimes PRIMERGY servers are integrated as 'Unknown device'. This is probably due to unsuccessful SNMP/WMI requests. Make sure SNMP and WMI requests are applied with correct authentication. If the global SNMP and WMI credentials cannot be applied to a particular server, server-specific credentials can be set up via the system protocol settings on the system's 'Tools & Links' page within HP SIM.

Some PRIMERGY servers are not recognized as 'Server'. This is a limitation of HP SIM, which sometimes fails to properly recognize servers. The System Type of a server can be manually rectified using the server's 'Tools & Links' page within HP SIM and select 'Edit System Properties'.

Using WBEM services for discovery with W2K8 or later enables very simplified discovery rules for PRIMERGY Servers. This version of the HP Integration Toolkit only supports PRIMERGY servers with W2K8 or later or Linux.

ServerView® Operations Manager V6.20 should not be used for HP-SIM integration, as there is a problem with the SVOM call that HP-SIM generates for the Custom Management Page. Please use either a newer or an older version of ServerView® Operations Manager.

Remote System Monitor can only be used when ServerView® Agents V7.01 or later are installed on the monitored PRIMERGY servers. If this is not the case, use ServerView® Operations Manager instead.

9 Uninstalling the ServerView® Integration

The ServerView® integration is uninstalled via a batchfile (svtosim-single-remove.cmd) delivered with the kit.

In order to uninstall the ServerView® integration the following steps have to be performed:

1. Open a command window (cmd.exe)
2. Using the cd command, change the working directory to the folder where the Integration is located.
3. Call svtosim-single-remove.cmd
4. To un-install the MIB Integration call svtosim-unloadmibs.cmd.

Note:

If the user account this step is conducted with does not have Administrator rights within HP-SIM, uninstalling the ServerView® Integration will fail. In this case add a user account and password to the svtosim-unloadmibs command, e.g.

```
svtosim-single-remove.cmd -user "Server\Administrator" -pwd "Password"  
svtosim-unloadmibs.cmd -user "Server\Administrator" -pwd "Password"
```

Appendix A: ServerView® MIBs

Enclosure and Environment Management

MIB File	Comment
S31.MIB	Provides information about the PRIMERGY Blade Server chassis
SC.mib SC2.mib	Collectively provide detailed information about a PRIMERGY server's state of health
Status.mib	Provides summary status information for various subsystems
Threshold.mib	Provides information needed for ServerView® performance management
egeneraV1.mib	Provides information about PRIMERGY BladeFrame systems
domagt.mib	Provides information about domains managed by PrimePower ServerView®

RAID Management

MIB File	Comment
RAID.mib	Provides information about generic RAID subsystems.