ServerView Suite Enterprise Edition V2.41

Installation Guide

Edition May 2009

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujtsu.com

Certified documentation according to DIN EN ISO 9001:2000

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2000.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Contents

1 Preface

The *ServerView Suite Enterprise Edition* combines different system management interfaces for various server families (PRIMEQUEST, PRIMERGY, PRIME-POWER, SPARC Enterprise Server) into one graphical user interface. This manual describes the installation and configuration of *ServerView Suite Enterprise Edition* (referred to in the following as *ServerView Suite* or *SVS EE* for short).

This product was previously known as *WebSysAdmin* (WSA for short). The abbreviation WSA still appears frequently in the path and file names.

1.1 Target groups

This manual is intended for system administrators and customer support staff. Sound operating system and hardware knowledge is required.

1.2 Notational conventions

The following notational conventions are used in this manual:

italics
: Denote names of commands, system calls, functions, files, procedures, programs etc., as well as menu options and input/output fields from figures in the main body of text.

Name (extension)
: Commands, system calls, functions, files, interfaces, etc. are provided with an extension in brackets if manual pages (descriptions) are available for them. The extension indicates the chapter in which the manual page is described.

  You can show the manual pages on the screen by means of the *man* command [see *man*(1)]. See the manual page for *man* itself for information about using this command. To do this, enter *man man*.

`fixed-pitch font`
: Indicates system output, such as error messages, notes, file excerpts and program examples.

`fixed-pitch semi-bold font`
: Denotes user input in examples.

► Indicates activities to be carried out by the user.

Highlights additional information that should be noted to assist understanding of the surrounding text passages.

2 Overview

2.1 Architecture

The *ServerView Suite* architecture can be divided into three areas, as illustrated from left to right in the figure below:

1. administration desktop (PC client / front end)
2. management server (MS)
3. managed nodes

All of these three layers have particular requirements and must be managed. All the management activities required are described in the sections below.

2.2 Management activities

The following management activities are required:

- creating the required software and hardware conditions
- installation and uninstallation
- configuration

In accordance with the *ServerView Suite* architecture, particular software and hardware requirements must be borne in mind for the following:

- the administration desktop
- the management server (MS)
- the managed nodes

Likewise, the following three areas must be distinguished when *ServerView Suite* is installed or uninstalled:

- installation and uninstallation on the administration desktop
- installation and uninstallation on the management server (MS)
- installation and uninstallation on the managed nodes: PRIMEPOWER (PW), PRIMERGY (PY), SPARC Enterprise Server (SPARC ES) and PRIMEQUEST (PQ part.)

The configuration must be adapted on the management server and the managed nodes for:

- SNMP communication
- communication with the MMB of PRIMEQUEST
- communication with XSCF and the partitions of a SPARC Enterprise Server

The figure below illustrates the entire architecture with all the network connections:

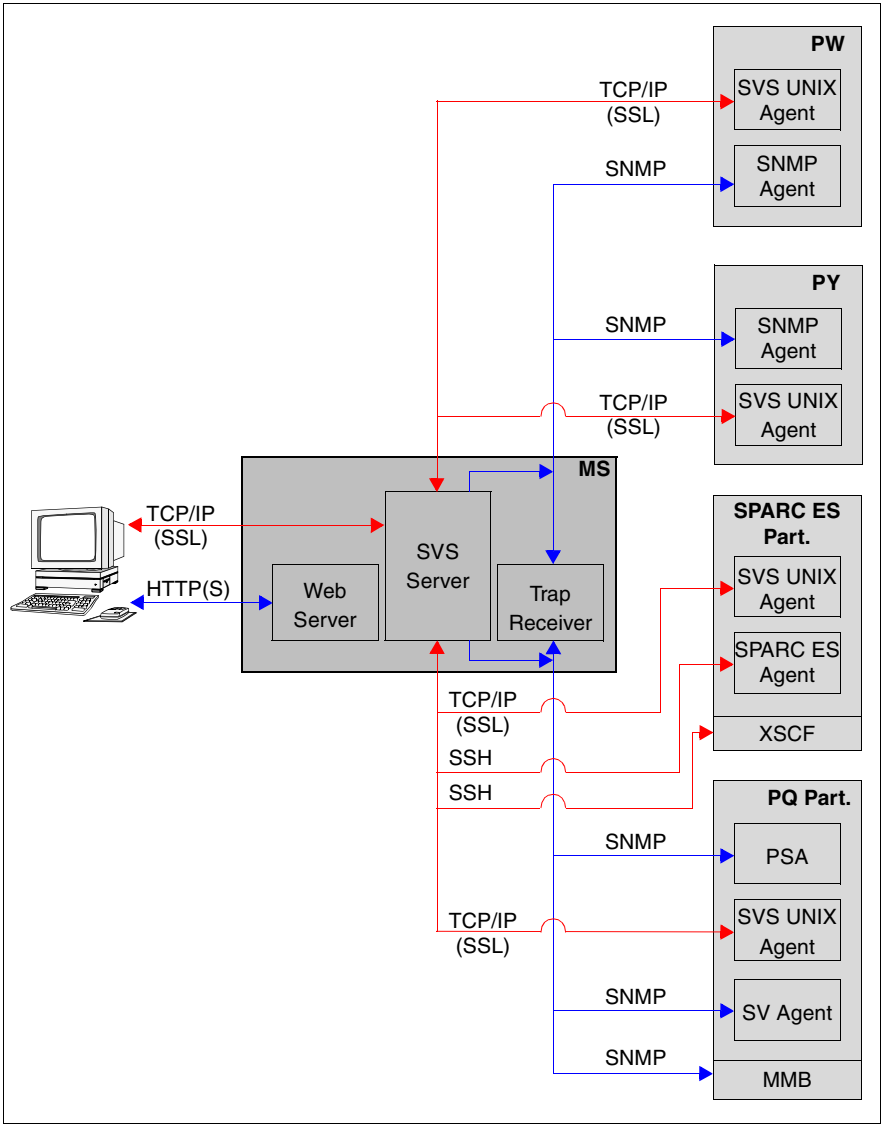

Figure 1: ServerView Suite architecture

3 Management server

3.1 Requirements

The manager part of *ServerView Suite* can be installed on every Linux system which fulfills the following requirements:

- x86 system (PRIMERGY recommended) with at least
  - 1 GB memory (2 GB recommended)
  - 2 GHz CPU
  - 500 MB available disk space
  - 17" display with XVGA resolution
- Operating system must be
  - SLES9 SP3 (x86 variant only)
  - SLES10 SP1 (x86 variant only)
  - SLES10 SP2 (x86, Intel64 or AMD64 variant)
  - RHEL 5.1 (x86 variant only)
  - RHEL 5.2 (x86, Intel64 or AMD64 variant)
  - RHEL 5.3 (x86, Intel64 or AMD64 variant)
- The following packages must be installed:
  - *apache2* (SLES) or *httpd* (RHEL)
  - *at*
  - *net-snmp* version 5.1.3.1-0.6 or higher (SLES)
  - *net-snmp* version 5.1.2-11.EL4.6 or higher (RHEL)
  - *net-snmp-utils* (RHEL)
  - *openssl*
  - *perl*
  - *zlib*
  - *inetd* or *xinetd*
  - *unixODBC* version 2.2.11 or higher
  - *unixODBC-devel* (RHEL)
  - *expect*
  - *compat-2004* (SLES9)
  - *compat-2006.1.25-11.2* and *compat-libstdc++-5.0.7-22.2* (SLES10)
  - *compat-libstdc++-296* and *compat-libstdc++-33-3.2.3-47.3* or higher (RHEL)
  - *openssh* (SLES) or *openssh-clients* (RHEL)
  - *libX11* (RHEL 5.1 or higher)

– *libXp* (RHEL 5.1 or higher)
– *bash*

Special requirements for Intel64/AMD64 variants:

– *unixODBC* is required in both variants x86(i386) and Intel64/AMD64(x86_64)
– *unixODBC-devel* is required in x86(i386) variant only (RHEL)
– *net-snmp-libs* is required in both variants x86(i386) and Intel64/AMD64(x86_64) (RHEL)
– Upgrade Kernel 2.6.16.60-0.23 (Linux kernel 20080515) or higher: Due to a problem in *netstat* command all currently installed kernel packages have to be replaced (SLES10 SP2 Intel64/AMD64(x86_64)).

Please note that the *atd* service, the web service (*apache2* (SLES) or *httpd* (RHEL)) and either the *inetd* or *xinetd* service must be activated. You can activate these services at CLI level using the *chkconfig* command (see *man chkconfig*) or by means of the installed system management application:

– On SLES use *YaST2*
Select menu options *System* → *Runlevel Editor*
– On RHEL use *Serviceconf*

- Ensure that the */etc/hosts* file contains an entry with the public IP address of the management server and its host name.

  Moreover it is necessary that the IP address 127.0.0.1 for *localhost* is contained in */etc/hosts*. This is needed for the access to the PostgreSQL server.

  Example for these two lines in */etc/hosts*:

```
<IP address>  <full qualified host name>  <short host name>
127.0.0.1     localhost.localdomain       localhost
```

- Ensure that the time zone and system time are set to the local time of the location at which the service is operated (see *man hwclock*).

- On RHEL 5.1 or higher, SELinux must be deactivated. You will achieve this by changing the corresponding line (*SELINUX=*) in */etc/sysconfig/selinux* as follows:

```
SELINUX=disabled
```

  After this, the system has to be rebooted. For further information on SELinux look at *http://www.ittvis.com/services/techtip.asp?ttid=3092*

- On SLES10 SP1 and RHEL 5.1 or higher, SNMP-trap receiving is deactivated by default. You can activate trap receiving by adding the following line to */usr/share/snmp/snmptrapd.conf*:

  ```
  disableAuthorization yes
  ```

  If you have already installed *ServerView Suite*, the *trpsrvd* service must be restarted after you modify *snmptrapd.conf*:

  ```
  # /etc/init.d/WsaSnmp stop
  # /etc/init.d/trpsrvd stop
  # /etc/init.d/trpsrvd start
  # /etc/init.d/WsaSnmp start
  ```

  For further information on trap receiving look at *http://net-snmp.sourceforge.net/docs/man/snmptrapd.conf.html*

- Before execution of the installer script, please check the following issues:
  - The language setting must not be set to "C" or "", because the installation of the Postgre data base does not support this. In this case, the installation will fail at some point. Please set the language to an appropriate value (e.g. "en_US.UTF-8").
  - When both the operating system and ServerView Suite need to be updated, the OS update must be performed first.

Before you are allowed to perform an update installation, all SVS EE sessions on the administration desktops must be closed (this is checked by the *installer* script).

An update installation automatically supports all SVS EE versions V1.0 or higher.

3.2 Installation

ServerView Suite is installed by executing the *installer* script in the *ServerView_Suite_Enterprise_Edition* directory.

To do this, proceed as follows:

- Mount the ISO image in an existing directory, e.g. in */media*:

  ```
  # mount -o loop <absolute_pathname_of_the_ISO_file> /media
  ```

- Go to the directory of the product to be installed:

  ```
  # cd /media/ServerView_Suite_Enterprise_Edition
  ```

- Start installation using the following command:

  ```
  # ./installer
  ```

  A text like the one below will appear:

  ```
  +++ Installation of ServerView Suite Enterprise Edition started.
  ```

  Follow the instructions displayed.

  If any problem occurred during the installation of the *ServerViewStarter* package, please enter the package's directory *ServerView Suite Enterprise Edition/all* and call the *InstallServerView -upgrade* command.

- When installation has been completed, quit the mounting directory and unmount it, e.g.:

  ```
  # cd /
  # umount /media
  ```

3.3 Uninstallation

If the management server is to be uninstalled, you are recommended to remove the domain before doing so. Please start the GUI and delete all nodes from the domain. Then remove the management server itself.

ServerView Suite is uninstalled by invoking */opt/SMAW/deinstaller.ServerView_Suite_Enterprise_Edition*.

Before you are allowed to uninstall the software, all SVS EE sessions on the administration desktops must be closed (this is checked by the *deinstaller* script).

3.4 Configuration

The password of the domain administrator *wdmadm* is preset! It is recommended that this password should be changed on all systems (see *5.1.2 Changing the password of the domain administrator "wdmadm"* in the current *ServerView Suite EE System Administration within a Domain* user manual), or - even better - that SSL encryption should be used. Details of SSL configuration are provided in section "SSL for TCP/IP connections" on page 45.

ServerView Suite communicates with the managed nodes using TCP/IP and SNMP. Ports are assigned on the management server and the managed nodes for this purpose.

Information on SNMP configuration is provided in the section "SNMP configuration on the management server" on page 36.

The standard configuration of the fixed ports and the ranges for the dynamic ports can be changed. Details are provided in the chapter "Port configuration" on page 55.

Details of configuring SPARC Enterprise Systems are provided in the chapter "Configuring SPARC ES" on page 77.

If you want to use the SVS EE to establish a secure management domain based on SSL, you must create a user ID for each SVS EE user on the management server and install their private and public keys. Details are provided in the chapter "Protecting communication paths" on page 45.

3.4.1 Hardware Monitoring

For PRIMEQUEST servers, hardware monitoring works without any SVS parts on the monitored nodes and for all operating systems.

For PRIMERGY, PRIMEPOWER and SPARC Enterprise Servers, the appropriate ServerView Agent part is mandatory.

3.4.2 Administration Functions

The current SVS EE software version supports the following administration functions, too:

- User administration and group administration
- cron job administration for the user *root*
- Display, checking and deletion of software packages
- Evaluation and configuration of logbooks
- Process management (displaying / killing of processes)
- File System and NFS administration (Solaris only)

The system administration functions need the product ServerView Suite Enterprise Edition Agent installed on each node which is to be administered. At present this is supported for Linux and Solaris only.

3.4.3 Life Cycle Management

Life Cycle Management incorporates Asset and Performance Management for PRIMERGY and PRIMEQUEST servers. To be able to use these functions, the appropriate ServerView Agents have to be installed on the monitored nodes.

Please note that due to internal update mechanisms on PRIMEQUEST servers, under some circumstances it may take nearly 30 minutes until new data is available after configuration changes. Additionally, the results of a DP action (Dynamic Partitioning) are only visible in the Performance Manager's GUI after the operating system has been restarted.

3.5 Troubleshooting

- In case of the problem "Open UDP connection to server failed! Please check your server configuration. Try again?" please check the *inetd* or *xinetd* configuration.

  Please note that the *atd* service, the web service (*apache2* (SLES) or *httpd* (RHEL)) and either the *inetd* or *xinetd* service must be activated. You can activate these services at CLI level using the *chkconfig* command (see *man chkconfig*) or by means of the installed system management application:

  - On SLES use *YaST2*
    Select menu options *System* → *Runlevel Editor*
  - On RHEL use *Serviceconf*

- In case of the problem "Cannot create PRIMEQUEST Server", the probable cause is an incorrect setting between PRIMEQUEST *MMB Web-UI* and Management Server. Recommended operation:
  - Check SNMP/IPMI setting of PRIMEQUEST *MMB Web-UI* again.
  - Check the access authorizations in SVS EE GUI against the settings on the MMB.

  If it is not possible to solve this problem, please save the log files to the working directory */tmp/work* using the following commands:

```
# /bin/mkdir /tmp/work
# cd /
# /opt/FJSVpqsc/sbin/pqsc_snap -d /tmp/work
# /bin/tar zcvf /tmp/work/SMAW_trace.tar.gz \
opt/SMAW/tmp/WSATrace
```

  Send the log files */tmp/work/*tar.gz* to Fujitsu´s / Fujitsu Technology Solutions´ support.

- Very rarely it may occur that a ServerView package cannot be uninstalled. You can use the following command to check whether any other packages are dependent on the one you wish to uninstall:

```
# rpm -q --whatrequires <package>
```

  If there are dependent packages, uninstall these first with the following command:

```
# rpm -e <package>
```

  Or, if you get error messages, uninstall the packages with the following command:

```
# rpm -e --noscripts <package>
```

  Packages installed are:

  - *SMAWPbase*
  - *SMAWPpgsq*
  - *ServerViewDB*
  - *ServerViewCommon*
  - *AlarmService*
  - *ServerView_S2*

Remove these packages in the reverse order, starting by *ServerView_S2*.

If *SMAWPbase* is required by some other package do not deinstall it. Also check, whether a package *ServerViewStarter* is installed. If so remove it.

- Very rarely an installation/uninstallation process might not run to completion. To purge the system from Life Cycle Modules, first uninstall all dependent packages and then the packages themselves.

  You must then delete the following directories:

  – *WebServerDocumentRoot>/ServerView*
  – *<WebServerScripts>/ServerView*
  – */opt/SMAWPlus/pgsql*
  – */usr/bin/setServerViewEnviron**
  – */usr/bin/setSVParams**
  – */usr/bin/UninstallServerView**

- If you recognize a strange behavior of the GUI (especially when selecting *Alarm Service* → *Server Settings* → *Filter Server*) the reason may be that the plugin architecure has changed to next generation plugin since JRE 1.6.0_10. In this case please click *Advance* tab in Java Control Panel and uncheck the check box *Enable the next-generation Java Plug-in*.

To solve other problems, please refer to the current *ServerView Suite EE System Administration within a Domain* user manual. Especially for problems with Java Web Start refer to section *3.2.3 Starting the product using Java Web Start*.

4 Administration desktop

The administration desktop can be configured on a Windows or Linux system. The administration desktop on Linux must also be the management server.

Manuals and some of the software to be installed can be downloaded from the management server using a Web browser (from the URL <*host*>:8883).

Figure 2: Download page on the management server

4.1 Requirements

4.1.1 Administration desktop with Windows

An x86 system with at least the following parameters is required:

- 512 MB memory
- Pentium® III or higher
- 200 MB available disk space
- 17" display with XVGA resolution (recommended)
- Windows XP

A Java Runtime Environment (JRE) must be installed. JRE Version 1.5.0_09 or higher is required. A JRE which is currently supported can be downloaded from the management server's download page (URL: http://<*host*>:8883).

Because some SVS EE user interfaces are Web-based, one of the following Web browsers is needed:

- Internet Explorer 6 or 7
- Mozilla Firefox 2.0

4.1.2 Administration desktop with Linux

The Linux administration desktop can only be configured on a Linux management server, i.e. the administration desktop must satisfy the requirements mentioned in the section "Requirements" on page 11.

Because some SVS EE user interfaces are Web-based, as Web browser Mozilla Firefox 2.0 with a JRE plug-in ≥1.5.0_09 must be installed.

Installation packages *libX11-1.0.3-8.0.1.el5* and *libXp-1.0.0-8.1.el5* must be available to allow the *svsee* script to be executed.

4.2 Installation

4.2.1 Installation on Windows systems

On a Windows system the user interface of SVS EE can be started locally as a Java application or as a Java Web Start application via a browser. You are recommended to use the local Java application.

4.2.1.1 Local Java application

If you want to work with ServerView Suite as a local application under Windows, you must download it from an SVS EE management server. To download it, enter the following in the browser's URL line:

`http://<host>:8883`

e.g.: `http://discover-scm.pdb.fts.net:8883`

This takes you to the ServerView Suite download page where you can select the product. After you have downloaded the product, you can install it like any Windows application.

The application is installed under Programs in the Start menu. From there you can start *ServerView Suite* locally on your PC.

The default setting of the installation path is as follows:

C:\<program_directory>\Fujitsu\WebSysAdmin

If the JAVA Runtime Environment (JRE) on the administration desktop was updated after ServerView Suite was installed, the ServerView Suite configuration must be adjusted accordingly. Proceed as follows:

– reinstall ServerView Suite (recommended procedure)

or

– use an editor to update the JRE path name in *<installation_directory>\wsa.bat*

4.2.1.2 Java Web Start application

If you want to work with ServerView Suite as a Java Web Start application under Windows, installation on the administration desktop is not required.

Call:

Enter one of the following URLs in the Web browser:

- http://<host>:8881
- http://<host>:8882
- http://<host>:8883

You obtain read/write access via port 8881, and read-only access via port 8882 (see also the chapter “Port configuration” on page 55).

If you choose port 8883, the *ServerView Suite* download page is displayed. Under the heading

Start As Remote Application Using Java™ Web Start select the entry:

ServerView Suite Enterprise Edition
(Java Web Start Application)

or the entry:

ServerView Suite Enterprise Edition
(Java Web Start Application, read-only mode)

4.2.2 Installation on Linux systems

On a Linux system the SVS EE user interface can only be started locally as a Java application.

The GUI is part of the ServerView Suite Enterprise Edition for the management server and is installed automatically. The GUI uses an internal JRE (installed under */opt/SMAW/JavaForWsa*).

Call:

```
# /opt/SMAW/bin/svsee <hostname> &
```

4.3 Uninstallation

4.3.1 Uninstallation on Windows systems

In the *Start – Programs – ServerView Suite Enterprise Edition* menu invoke the menu entry *Uninstall ServerView Suite Enterprise Edition* to uninstall the product.

4.3.2 Uninstallation on Linux systems

Nothing needs to be done here. The GUI is deleted by uninstalling the management server.

4.4 Configuration

If you want to start the SVS EE user interface as a secure JAVA application, you must

- configure the SSL protocol and
- enable the use of the HTTPS protocol

on the administration desktop. For the SSL protocol you must store your private key in the following system-specific file:

- Windows:

  `C:\wsa_certs\<login-username>\wsa_cert.p12`

- Linux:

  `/opt/SMAW/wsa_certs/<login_username>/wsa_cert.p12`

The HTTPS protocol is used by the Life Cycle Modules to communicate with the management server. Activation of the HTTPS protocol is described in the section “Protecting communication by means of HTTPS” on page 53.

Details of SSL configuration are provided in the section “SSL for TCP/IP connections” on page 45.

5 Managed nodes

The following hardware platforms can be managed by SVS EE:

- PRIMERGY (Linux or Windows system)
- PRIMEPOWER (Solaris system)
- PRIMEQUEST partition (Linux or Windows system)
- SPARC Enterprise Server (Solaris system)

5.1 Requirements

5.1.1 PRIMERGY servers with Windows

On PRIMERGY servers the ServerView agent must be installed from the latest ServerStart DVD.

A detailed description of the installation procedure is provided in the manual *PRIMERGY ServerView Suite; Installation; ServerView V4.61*.

5.1.2 PRIMERGY servers with Linux

The following packages must be installed:

- *at*
- *inetd* or *xinetd*
- *openssl* (x86 version)
- *ServerView Agent* (from the ServerStart DVD)
- *bash*
- *net-snmp* (Net-SNMP) version 5.1.3.1-0.6 or higher (SLES 9)
- *net-snmp* (Net-SNMP) version 5.1.2-11.EL4.6 or higher, including *net-snmp-utils* (RHEL 4)

A detailed description of the installation procedure is provided in the manual *PRIMERGY ServerView Suite; Installation; ServerView V4.61*.

Please note that the *atd* service and either the *inetd* or *xinetd* service must be activated. You can activate these services at CLI level using the *chkconfig* command (see *man chkconfig*) or by means of the installed system management application:

1. SLES: *YaST2*
   Select menu options *System* → *Runlevel Editor*.
2. RHEL: *Serviceconf*

Ensure that

- the */etc/hosts* file contains an entry with the public IP address of the management server and its host name.
- the time zone and system time are set to the local time of the location at which the service is operated (see *man hwclock*).

5.1.3 PRIMEQUEST partitions with Windows

Windows Server 2003/2008 with IA64 is required as the operating system.

The following software must be installed:

- *PRIMEQUEST Sever Agent* (*PSA* V1.9.0 or higher), a software attached to PRIMEQUEST hardware

The results of a DP action (Dynamic Partitioning) are only visible in the Performance Manager's GUI after the operating system has been restarted.

5.1.4 PRIMEQUEST partitions with Linux

At least SLES 9 SP2, RHEL 4 UR4 or RHEL 5 (IA64 version) is required as the operating system.

The following packages must be installed:

- *at*
- *inetd* or *xinetd*
- *openssl* (x86(i386) version)
- *compat-libstdc++-33* (V3.2.3-47.3 or higher) (RHEL)
- *compat-libstdc++* (V5.0.7-22.2 or higher) (SLES10)
- *ia32el*

- *FJSVpsa* (PSA V1.7.2 or higher)
- *bash* (x86(i386) version)
- *net-snmp* (Net-SNMP) version 5.1.3.1-0.6 or higher (SLES 9)
- *net-snmp* (Net-SNMP) version 5.1.2-11.EL4.6 or higher, including *net-snmp-utils* (RHEL 4)

Please note that the *atd* service and either the *inetd* or *xinetd* service must be activated. You can activate these services at CLI level using the *chkconfig* command (see *man chkconfig*) or by means of the installed system management application:

1. SLES: *YaST2*
   Select menu options *System* → *Runlevel Editor*.
2. RHEL: *Serviceconf*

Ensure that

- the */etc/hosts* file contains an entry with the public IP address of the management server and its host name.
- the time zone and system time are set to the local time of the location at which the service is operated (see *man hwclock*).

The results of a DP action (Dynamic Partitioning) are only visible in the Performance Manager's GUI after the operating system has been restarted.

5.1.5 PRIMEPOWER with Solaris

At least Solaris 8 or higher is required as the operating system.

The following package must be installed:

- *ESF 2.0 (Enhanced Service Facility)* or higher

5.1.6 SPARC Enterprise Server with Solaris

Solaris 10 or higher is required as the operating system.

The following package must be installed:

- *ESF 3.0 (Enhanced Service Facility)*

5.2 Installation

5.2.1 Installation on PRIMEQUEST partitions with Windows

Before you install the SNMP ServerView agents for Windows, it is essential that you install and activate the SNMP services in the operating system. Details are provided in the section “Installing and activating the SNMP service” on page 41.

Proceed as follows to install the SVS EE agents:

- ► Go to the *ServerView_Suite_Enterprise_Edition_Agent_Windows/all* directory and start the *ServerViewAgents_Win_x64.exe* program.
- ► Follow the instructions on the screen.

When you have confirmed that you agree to the license conditions, the system setup checks whether an older version of the SNMP ServerView agents is already installed on the server. If this is the case, you can perform an upgrade installation. During this, the present configuration is saved, then the old version is deleted and the new version is installed. The previous configuration is used here. In this case you cannot make any changes.

If no agents are present on the system, the following window will be opened:

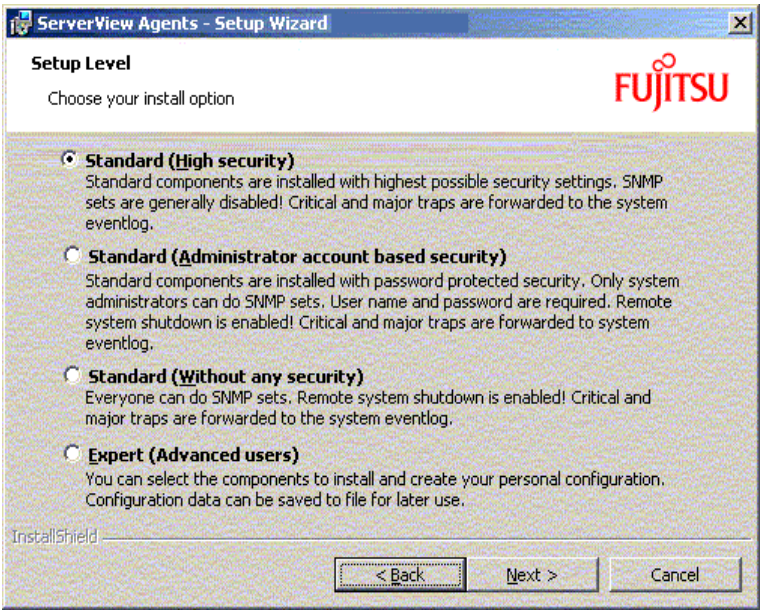

Figure 3: “Setup Level” window

The Setup Level window offers you four default modes for agent installation:

- Standard (High security)
- Standard (Administrator account based security)
- Standard (Without any security)
- Expert (Advanced users)

Select the *Standard (Without any security) mode*.

This mode is necessary when you want to use the SVS EE Life Cycle components (*Asset*, *Inventory*, *Performance*, *Update*) without restriction. The security settings are determined by an SNMP services configuration in the operating system (see section “Installing and activating the SNMP service” on page 41).

5.2.2 Installation on PRIMERGY / PRIMEQUEST partitions with Linux

The product is installed by invoking the *installer* script in the *ServerView_Suite_Enterprise_Edition_Agent_Linux* directory.

Proceed as follows to do this:

- Mount the ISO image in an existing directory, e.g. in */media*:

  ```
  # mount -o loop <absolute_pathname_of_the_ISO_file> /media
  ```

- Go to the directory of the product to be installed:

  ```
  # cd /media/ServerView_Suite_Enterprise_Edition_Agent_Linux
  ```

- Start installation using the following command:

  ```
  # ./installer
  ```

  A text like the one below will appear:

  ```
  +++ Installation of ServerView Suite Enterprise Edition started.
  ```

  Follow the instructions displayed.

- When installation has been completed, quit the mounting directory and unmount it, e.g.:

  ```
  # cd /
  # umount /media
  ```

An update installation automatically supports all SVS EE versions V1.0 and higher.

5.2.3 Installation on PRIMEPOWER / SPARC ES partitions

The product is installed by invoking the *installer* script in the *ServerView_Suite_Enterprise_Edition_Agent_Solaris* directory.

To do this, proceed as follows:

- Mount the ISO image in an existing directory, e.g. in */media*:

  ```
  # device=`lofiadm -a <absolute_pathname_of_the_ISO_file>`
  # mount -F hsfs -o ro $device /media
  ```

- Go to the directory of the product to be installed:

  ```
  # cd /media/ServerView_Suite_Enterprise_Edition_Agent_Solaris
  ```

- Start installation using the following command:

  ```
  # ./installer
  ```

  A text like the one below will appear:

  ```
  +++ Installation of ServerView Suite Enterprise Edition started.
  ```

  Follow the instructions displayed.

- When installation has been completed, quit the mounting directory and unmount it, e.g.:

  ```
  # cd /
  # umount /media
  # lofiadm -d $device
  ```

An update installation automatically supports all PW SVS versions V2.2B10 and higher.

5.2.3.1 “LiveUpgrade” installation of the Solaris ServerView Agent

If you want to use of the *LiveUpgrade* capability of the Solaris ServerView Agent, proceede as follows:

- Mount the disk with the updated operating system on an already existing root path.
- Start the installation of the Solaris ServerView Agent to the disk with the updated operating system using the following command:
  `# ./installer -R <pathname>`
  where *<pathname>* is the root path to the operating system to the newly mounted disk.

  Instead of providing this path via option *-R <pathname>* you can set the environment variable *$PKG_INSTALL_ROOT* to the appropriate value.

When the new operating system is updated with the Solaris ServerView Agent you can switch to the new system by a reboot from the disk prepared in this way.

5.3 Uninstallation

Before the agent software on a monitored system is uninstalled, you are recommended to remove this system from the administration domain via the GUI.

5.3.1 Uninstallation on Windows systems

Remove the *ServerView Agents* using the system administration function *Start → Control Panel → Software → Add or Remove Programs*.

5.3.2 Uninstallation on Linux systems

The agent product is uninstalled by invoking the *deinstaller.ServerView_Suite_Enterprise_Edition_Agent_Linux* script in the */opt/SMAW* directory.

5.3.3 Uninstallation on Solaris systems

The product is uninstalled by invoking the *deinstaller.Server_ViewSuite_Enterprise_Edition_Agent_Solaris* script in the */opt/SMAW* directory.

5.4 Configuration

The SNMP service on the managed systems must be configured so that is permits the SNMP requests sent from *ServerViewSuite*. Details of SNMP configuration are provided in the chapter “SNMP configuration” on page 35.

ServerView Suite communicates with the managed nodes using TCP/IP and SNMP. For this purpose ports are assigned on the management server and the managed nodes.

If the standard assignment for the fixed ports or the ranges for the dynamic ports are changed, adjustments must also made on the managed nodes. Details are provided in the chapter “Port configuration” on page 55.

If PRIMEQUEST systems are to be managed by *ServerView Suite*, some adjustments must be made via the PRIMEQUEST’s MMB. These configuration activities are described in the section “Settings in the MMB Web-UI” on page 63.

In order to manage a SPARC Enterprise System by means of SVS EE, adjustments must be made via the XSCF board. Details are provided in the chapter “Configuring SPARC ES” on page 77.

When a Unix node is to be added to a secure domain, the SVS EE user’s public key must be installed in the */opt/SMAW/.cert/<user>* directory. Details are provided in the chapter “Protecting communication paths” on page 45.

6 SNMP configuration

Because the monitoring functions of *ServerView Suite* access the SNMP interface, the SNMP agents need to be installed and configured appropriately on each managed node.

On the management server SNMP requests are sent to the managed nodes and traps are received from the managed nodes.

When you install and configure the SNMP services, default values are provided. You can increase security on a managed node by modifying these values for the SNMP service. However, these modifications must always be made on both the managed nodes and on the management server.

The following parameters can be configured:

- Community name for incoming SNMP requests

  The community name (community string) is part of every SNMP request sent from the manager to the agent.

  The default community name is *public*. This default entry is used by most SNMP services. For reasons of security, we recommend that you change this entry. You can define an individual community for each server or server group.

- Rights for the community

  Rights can be assigned to the community (e.g. *read-only*, *read-write*). If you want to use the entire range of ServerView functions, you must assign *read-write* permission to the community. You can restrict access to certain functions by assigning *read-only access to them*.

  The ServerView Manager only supports one community per managed node for SNMP requests. For this reason you cannot configure different communities with different rights for a managed node. In addition, the community of the MMB must be used for all partitions of a PRIMEQUEST system. The same community of the management blade must also be used for all the blades of a blade server.

- Accept SNMP requests from selected servers/any server

  We recommend that you only enter the IP address of the server which is to function as management server. This will prevent the agent from accepting requests from unauthorized servers.

- Trap destination system

  IP address of the management server to which the SNMP agents send traps.

i If you assign no SNMP write permissions for the SVS EE management server on a managed node, the following performance management functions cannot be used:

  – Setting threshold values
  – Defining reports

  Existing threshold value and report settings for the managed node (which were defined when write permissions existed) can be evaluated without write permission.

6.1 SNMP configuration on the management server

On the management server SNMP requests (read and write requests) are sent to the managed nodes and traps are received from the managed nodes.

The SNMP requests are sent to port 161, and the traps are received at port 162. These ports cannot be changed.

The community with which the SNMP requests are sent is defined for every managed node when this node is added to the SVS EE management domain (*Community name* entry field in the dialog box for creating a PRIMERGY, PRIMEQUEST or Linux server). The community of the MMB must be used for all partitions of a PRIMEQUEST system. The same community of the management blade must also be used for all the blades of a blade server.

If the community is to be modified later, the node concerned must be removed from the domain and created again with the new community specified.

The default configuration works with the *public* community. If you specify a different community, you must also configure it on the system.

6.2 SNMP configuration on the managed nodes

The SNMP ServerView agents are written on the basis of the SNMP master agent (system-specific SNMP agent), i.e. the reception of SNMP requests and the sending of traps take place under the control of the SNMP master agent. It is therefore important to configure the SNMP master agent in such a way that

- the traps are sent to the management server and
- the SNMP requests (read and write) of the management server are accepted

The SNMP requests are received at port 161, and the traps are sent to port 162. These ports cannot be changed.

6.2.1 Linux systems

On Linux systems

- the SNMP master agent must be configured
- the SNMP ServerView agents must be configured

You must stop and restart the agents so that the changes become effective:

```
# /etc/init.d/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
# /etc/init.d/srvmagt start
```

You must also ensure that the SNMP master agents and the SNMP ServerView agents are started automatically after the system has been restarted.

6.2.1.1 Configuring the SNMP master agent

The SNMP master agent expects its configuration file at the following locations:

Linux	**SNMP configuration file**
SUSE, SLES 9	*/etc/snmpd.conf*
SUSE, SLES 10	*/etc/snmp/snmpd.conf*
Red Hat, RHEL	*/etc/snmp/snmpd.conf*

Table 1: Locations where the SNMP master agent expects its configuration file

Extend *snmpd.conf* so that the SVS EE manager is defined as the trap destination and is assigned read/write permission. You can edit the configuration file with a text editor such as *vi*. Information about the syntax is contained in Manual Page *snmpd.conf*(5).

Changes to the configuration file only become effective when the SNMP master agent is restarted.

You are recommended to specify the following values in *snmpd.conf*:

Variable	Explanation
syscontact	Contact data of the administrator responsible (name, mail address, telephone number).
syslocation	Location of the managed node.
authtrapenable	Send trap in the event of failed authentication: 1 (enable, recommended value) 2 (disable, default value)

Table 2: Values which should be specified in *snmpd.conf*

Supplement *snmpd.conf* in accordance with the template below. This describes the configuration which permits SNMP get and set commands and sends traps to the <*host*>. For <*host*>, enter the IP address of the SVS EE manager.

```
com2sec svSec    127.0.0.1           public
com2sec svSec    localhost           public
com2sec svSec    <host>              public
group   svGroup  v1                  svSec
view    svView   included .1
access  svGroup  "" any noauth exact svView svView none
trapsink <host> public
```

If you only want to permit read rights, the penultimate line must be changed as follows:

```
access  svGroup  "" any noauth exact svView none none
```

The community name in our example is *public*. If you want to use another community name for security reasons, replace *public* with your chosen name. In this case configure the community name on the manager side, too (see the section “SNMP configuration on the management server” on page 36). The same community must be used for all partitions of a PRIMEQUEST server (or all blades of a blade server).

The order of the *com2sec* definitions is important. It goes from specific IP addresses to generic IP addresses within the same community. If access is to be granted not just to special nodes but to an entire subnet, the com2sec lines with the subnet specification (<subnet>/<netmask>) must follow the host lines. Please note the following:

1. Ensure that the lines

   com2sec svSec 127.0.0.1 public
   com2sec svSec localhost public

   are **in front of** the line

   com2sec psalocal localhost psaprivate

2. If the *snmpd.conf* file contains the line

   com2sec notConfigUser default public

   delete it or place it behind the aforementioned com2sec lines for *svSec*.

You use *trapsink* to define the destination addresses for SNMP traps. Enter one line containing the IP address or the host name of the destination for each trap destination.

6.2.1.2 Configuring the SNMP ServerView agents

The configuration file for the SNMP ServerView agents is */etc/srvmagt/config*.

Changes to the configuration file only become effective when the SNMP ServerView agents are restarted.

You should set the following values in the version of */etc/srvmagt/config* supplied to allow the full functional scope of the of performance management to be used:

```
NoAccountCheck=1
AgentPermission=3
```

In this way you permit SNMP set operations without password inquiry on the managed server. These specifications are required in addition to the access specification in *snmpd.conf* (see the section “Configuring the SNMP master agent” on page 37).

A detailed explanation of the */etc/srvmagt/config* file is provided in the section “Configuring the SV SNMP agents under Linux” on page 85.

6.2.1.3 Starting and stopping the SNMP agents

The agents must be restarted for the changes to the configuration files to become effective. You can do this by entering a command or by rebooting the system. Before you do this you must configure automatic startup of the agents when the system is started.

Automatic start

Automatic start must be activated for the SNMP master agent *snmpd* and the SNMP ServerView agent *srvmagt*. You can do this using the relevant system management program or by means of the following commands.

```
# chkconfig snmpd on
# chkconfig srvmagt on
```

Or as an alternative using the system management program:

For SUSE systems:

- Execute YaST and select *System* → *Runlevel Editor*.
- Set *snmpd* and *srvmagt* to *enable* and save this setting.
- Set the operating system mode to at least 3.

For Red Hat systems:

- Start the *Service Configuration Tool* by selecting *System Settings* → *Server Settings* → *Services*.
- Set *snmpd* and *srvmagt* to *enable* by clicking in the box next to the name and save this setting.
- Set the operating system mode to at least 3.

Manual start

To allow SNMP ServerView agents to be started the SNMP master agent *snmpd* must be started. The SNMP ServerView agents should be stopped before *snmpd* is stopped:

```
# /etc/init.d/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/snmpd start
# /etc/init.d/srvmagt start
```

6.2.2 Windows system

Only installation for the PRIMEQUEST partition (with Windows 2003/2008) is described here. Information on installation of SNMP ServerView agents on PRIMERGY systems is provided in the manual *PRIMERGY ServerView Suite – Installation under Windows – ServerView V4.60*.

Before you install the SNMP ServerView agents for Windows, it is essential that you install and activate the SNMP services in the operating system. If you do not do this, the management server cannot monitor the managed nodes.

6.2.2.1 Installing and activating the SNMP service

You must perform the following actions to activate the SNMP service if you have not already done this when the system was installed:

1. Installation
   - To perform installation, select *Start* → *System Settings* → *Control Panel* → *Add/Remove Windows Components* (path is OS-dependent!).
   - In the *Windows Components* window mark the *Management and Monitoring Tools* entry and then click on the *Details* button.

- ► Select the *SNMP (Simple Network Management Protocol)* entry and then click on the *OK* and *Next* buttons.

2. Configuration

- ► To perform configuration, select *Start* → *System Settings* → *Control Panel* → *Administrative Tools* → *Components Services*.
- ► Mark *SNMP Service* and select the *Properties* entry from the context menu.
  - ► Enter a name under *Community Name* in the *Traps* tab.

    The access authorization of the management server is controlled using *Community Name*. Only queries with this community are permitted. This value must be consistent with the community specification which was entered when the managed node was created in the SVS EE domain.
  - ► Under *Trap destinations* use *Add* to enter the IP address of the management server for the specified community. Traps are sent only to the management servers entered here.
  - ► *Security* tab:
    - ► Set the *Rights* for the community to *READ WRITE*.
    - ► *Accept SNMP packets from any host/Accept SNMP packets from these hosts*:

      Here you can select servers from which SNMP packages are to be accepted or select all. Enter the management server here.

      

      As SNMP is an open protocol without password protection, only the management servers which are also to perform this function should be entered. Unauthorized network participants could otherwise change important parameters in the system and thus disturb server operations.
- ► Click on *OK*.

3. Start

- ► Start the SNMP service under *Services*. To do this, select *Start* from the context menu.

6.2.2.2 Activating SNMP ServerView agents

To change the standard configuration of the SNMP ServerView agents defined during installation, select *Start* → *All Programs* → *Fujitsu* → *ServerView* → *Agents* → *Configuration* → *Agent Configuration* and follow the instructions on the screen. Details are provided in the section “Configuring the SV SNMP agents under Windows” on page 87.

7 Protecting communication paths

ServerView Suite uses two methods to protect communication:

- SSL, to protect the TCP/IP connections
- HTTPS, to protect the Web connections

Both methods can be configured independently of each other.

Both configurations must be used to protect all communications.

7.1 SSL for TCP/IP connections

ServerView Suite can use the SSL protocol to permit secure extension of the standard TCP/IP protocol. The secure socket layer is inserted between the transport layer and the application layer of the standard TCP/IP protocol stack. SSL-based communication between all components utilizes authentication with public/private keys on the basis of X509 certificates.

Communication using SSL begins with an exchange of information between the administration desktop and the management server. This exchange of information is known as the SSL handshake. Communication between the management server and the managed UNIX nodes (Linux and Solaris) is also protected by SSL.

The activities which are required to set up a secure domain are described below.

7.1.1 Setting up a secure domain

The system administrator must perform the following activities to set up a secure administration domain:

1. Specify the number of administration desktops and managed nodes in your domain.
2. Specify the number of users who are to have access authorization.
3. Create the certificates and keys required for each user on the management server. Each user should be assigned their own certificate, PEM certificate and key. Details are provided in the section “Generating a self-signed user certificate” on page 47.
4. Distribute the *WSA_cert.pem* certificates and the hash file "*.0" to all managed nodes and the management server over a secure path (*/opt/SMAW/.cert/<user> directory*).
5. Copy the *WSA_key.pem private keys*, certificates and hash files to the management server over a secure path (*$HOME/.cert_private* directory).
6. Distribute the *wsa_cert.p12* client certificate to all administration desktops which are to be assigned an access authorization for this domain over a secure path (directory */opt/SMAW/wsa_certs/<user>* or *C:\wsa_certs\<user>*, see also the paragraph “Administration desktop” on page 50).
7. Start *ServerView Suite* and generate the administration domain.

The following restrictions must be taken into account:

- The keys and certificates must be distributed manually and requires root authorization on all systems. The domain should then be created using *ServerView Suite*.
- A mixture of secure and non-secure computers is not supported.
- Non-secure administration desktops will no longer have access to a domain which has been made secure.

7.1.2 Generating a self-signed user certificate

The user certificate can be generated using the interactive command *MK-KEY* or using openssl commands. Both methods are described below.

At the end of the procedure the following files must be generated:

$HOME/.cert_private/WSA_key.pem
$HOME/.cert_private/WSA_cert.pem

/opt/SMAW/.cert/$USER/WSA_cert.pem
/opt/SMAW/.cert/$USER/[hash.0] -> WSA_cert.pem

/opt/SMAW/.cert/$USER/wsa_cert.p12

7.1.2.1 Using MK_KEY

Log in on the management server with the user authorization which you want to use to execute SVS EE.

Issue the following command:

```
# /opt/SMAW/SMAWssl/bin/MK_KEY -i
```

Follow the instructions on the screen.

Respond to each of the following requests

```
Enter pass phrase for WSA_key.pem:
Enter Export Password:
```

by entering the same password. You must then enter this password as the PEM password in the login mask of SVS EE (see the section “Login procedure” on page 50).

7.1.2.2 Using openssl commands

The *openssl* program has a command interface for the various encryption functions of the OpenSSL encryption library at shell level. It can be used

- to generate RSA, DH and DSA key parameters
- to generate X.509 certificates, CSRs and CRLs

Log in on the management server with the user authorization which you want to use to execute SVS EE.

1. Generating the private key:

   When */dev/urandom* is available, the private key must be created using the following command:

   ```
   # /opt/SMAW/SMAWssl/bin/openssl genrsa -des3 -out \
   $HOME/.cert_private/WSA_key.pem 2048
   ```

   When */dev/urandom* is not available, the private key must be created using the following command:

   ```
   # /opt/SMAW/SMAWssl/bin/openssl genrsa -des3 -out \
   $HOME/.cert_private/WSA_key.pem -rand \
   /opt/SMAW/SMAWwsaS/conf/prngsock 2048
   ```

   /opt/SMAW/SMAWwsaS/conf/prngsock is an alternative random generator which is installed when */dev/urandom* is not available.

2. Generating the self-signed root certificate:

   Enter the following command:

   ```
   # /opt/SMAW/SMAWssl/bin/openssl req -new -x509 -days 730 \
   -key $HOME/.cert_private/WSA_key.pem -out \
   $HOME/.cert_private/WSA_cert.pem
   ```

   The *-days* option defines the number of days until the expiry date of the certificate. The root certificate must also be copied to */opt/SMAW/.cert/<user>*.

   ```
   # cp $HOME/.cert_private/WSA_cert.pem /opt/SMAW/.cert/<user>
   ```

3. Indexing the certificate subject name:

   The certificates' subject names are used in OpenSSL for an index in which all certificates can be searched for using their subject names.

   Execute the following commands:

   ```
   # cd /opt/SMAW/.cert/<user>

   # ln -s WSA_cert.pem `openssl x509 -hash -noout -in \
   WSA_cert.pem`.0
   ```

4. Generating a PKCS12 file for the GUI:

   The *pkcs12* command enables PKCS#12 files (which are sometimes also called PFX files) to be created and analyzed. PKCS#12 files are used by several programs, for example Netscape, MS Internet Explorer and MS Outlook.

Execute the following commands:

```
# cd /opt/SMAW/.cert/<user>
```

```
# /opt/SMAW/SMAWssl/bin/openssl pkcs12 -export -in \
WSA_cert.pem -inkey /root/.cert_private/WSA_key.pem \
-out wsa_cert.p12
```

7.1.3 Installing public and private keys

A pair of public and private keys is installed for every user who wants to log in to *SVS EE*. The public and private keys must be installed as follows on the various types of systems which are involved in communication within SVS EE:

1. Management server

   The management server needs both keys: the public key and the private key:

   Copy the public key files *WSA_cert.pem*, *<hash>.0* and *wsa_cert.p12* into the */opt/SMAW/.cert/<user> directory*.

   Copy the private key files *WSA_key.pem* and *WSA_cert.pem* into the *$HOME/.cert_private* directory.

   Restrict the access rights for *$HOME/.cert_private* to read permissions for *root* and the user himself/herself.

2. Managed nodes

   Only the public key of the login user need be installed on these nodes.

   Copy the *WSA_cert.pem* and *<hash>.0 files* into the */opt/SMAW/.cert/<user>* directory.

   Make sure that the */opt/SMAW/.cert* directory is only available to privileged users (e.g. *root*).

   In this way the login user, i.e. the owner of the public key, is assigned *root* permission on this node. It must therefore be ensured that the installation directory */opt/SMAW/.cert* of the public key has only very restricted access rights. *ServerView Suite* requires the *root* rights to perform system administration and configuration tasks.

3. Administration desktop

   Only the user's private key need be installed on the administration desktop.

   Copy the *wsa_cert.p12* file into the system-specific installation directory:

   Windows: *C:\wsa_certs\<user>*

   Unix: */opt/SMAW/wsa_certs/<user>*

   If a user manages multiple domains and consequently requires multiple certificates, generate a subdirectory with the name of the management server (*C:\wsa_certs\<user>\<servername>*) in the installation directory and copy the key file into this directory.

   If the required certificate *wsa_certs/<user>/<servername>/wsa_cert.p12* does not exist, recourse will be made to the certificate in the higher-ranking directory *wsa_certs/<user>/wsa_cert.p12*.

7.1.4 Login procedure

The SVS EE user must log in using a valid user management server ID and the associated password. For secure connections the user must also enter the PEM password of the private key file:

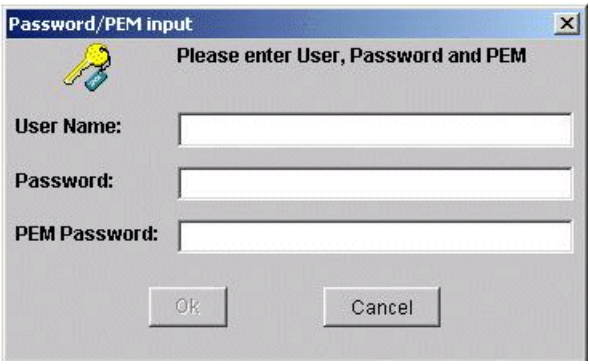

Figure 4: Dialog box for login with SSL

The GUI uses this password to read the private key file of the user concerned on the administration desktop. This private key file is used to authenticate the user on the management server using the SSL handshake protocol. After the

connection has been established, the GUI sends the private key password to the management server to enable the private key file to be opened on the administration desktop.

As SSL is used for communication between the administration desktop and the management server, the private key password is sent over a secure connection. This works only when the private key files on the management server are consistent with those on the administration desktop.

After the login procedure, communication between the administration desktop and the management server is secure and the management server has all the information needed to establish SSL-based communication with the managed node if required. This is indicated by the icon at the bottom left, which is now a closed padlock:

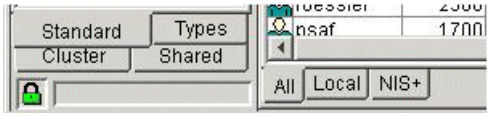

Figure 5: Icon for SSL connection

If no secure connection exists, the padlock is open.

7.1.5 Error situations

In this section a few situations are described in which secure communication is not possible. This means that no connection can be established between the relevant components of *ServerView Suite*.

1. The managed node does not contain the public key in a special user directory.

   If this node is already part of a domain (for example because older versions are used), this node is colored gray (inactive) on the GUI. No connection is established with this node.

2. The management server has no private keys

   This means that the management server is not able to authenticate itself to the managed node. Such a management server cannot be used. It is not possible to log in on this management server over an SSL connection using *ServerView Suite*.

3. The management server has no public keys for the login user

   The user is not able to log in on the management server. This user may not use this server to manage the domain.

7.2 Protecting communication by means of HTTPS

It is necessary to activate the HTTPS protocol to protect communication of the administration desktop with the management server when the Life Cycle Modules are called. The following activities are required here:

- On the Apache Web server activate the SSL module on the management server (for detailed information, please refer to the system manual for Linux administration).
- In the menu bar of the SVS EE interface select Preferences under the menu item *Edit* and select the *WebAccess tab*. In the dialog box which appears activate the *Use SSL setting*. The port will switch automatically to 443.

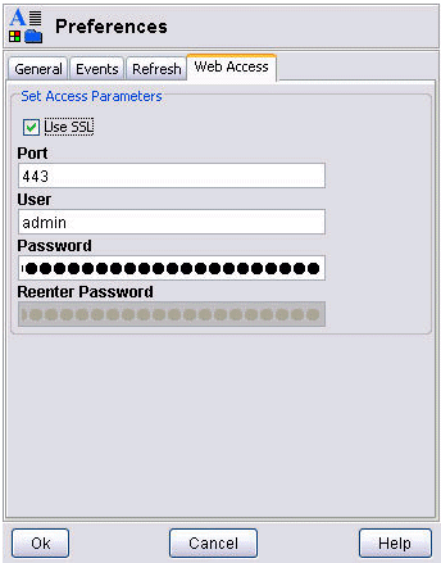

Figure 6: Specifying the SSL setting

8 Port configuration

8.1 Fixed ports

Fixed ports are configured in the */etc/services* and *http_addWSA.conf* files, while dynamic port ranges are defined in product-specific files. The lists of ports which are occupied by the default installation are as follows:

- 80 (TCP) (Life Cycle Management)
- 161 (UDP/TCP) (SNMP service)
- 162 (UDP/TCP) (SNMP trap reception)
- 8886 (UDP) (WSA Server)
- 8899 (UDP) (Domain Admin)
- 8881-8883 (TCP) (WebService)
- 3172 (Performance Management)
- 23460 (SSH communication)

8.1.1 Fixed ports on the management server

When *ServerView Suite* is installed, it creates the following entries in the */etc/services* file:

WSAserver	8886/udp	#Server administration
dom_adm	8899/udp	#Domain administration port

Table 3: Entries created in the */etc/services* file when *ServerView Suite* is started

The assignment of port 162 may not be changed. If *snmptrapd* is running, it will be stopped and restarted on port 8162.

The above-mentioned ports are essential for *ServerView Suite*.

For Web server functions, *ServerView Suite* uses ports 8881 through 8883, which are configured in the */opt/SMAW/SMAWapac/conf/http_addWSA.conf* file. These ports are only needed if Web server functions such as Java Web Start, application download, etc. are to be used.

These ports are used as follows:

- 8881: Java Web Start for read-write access
- 8882: Java Web Start for read-only access
- 8883: Download page for JRE, Windows application, online manuals, Java Policy template

8.1.2 Fixed ports on managed nodes

8.1.2.1 Windows system: PRIMERGY and PRIMEQUEST systems

SNMP requests must be received via port 161. The default system settings required for this should therefore not be changed.

Port 3172 is used by the performance manager's agent for communication with the management server.

8.1.2.2 Linux system

SNMP requests must be received via port 161. The following lines must therefore be entered in the */etc/services* file:

snmp	161/tcp	#Simple Net Mgmt Proto
snmp	161/udp	#Simple Net Mgmt Proto
dom_adm	8899/udp	#Domain management port

Table 4: Lines which must be entered in the */etc/services* file for SNMP requests

Port 3172 is occupied by the performance manager's agent.

8.1.2.3 Solaris systems

The following entry is created in the */etc/services* file when *ServerView Suite Agent* is installed:

dom_adm	8899/udp	#Domain management port

Table 5: Entry which is created in the */etc/services* file when *ServerView Suite* is installed

Additionally, the port 23460 is used for SSH communication.

8.1.2.4 MMB

Port 22 is used for SSH communication.

snmp	161/tcp	#Simple Net Mgmt Proto
snmp	161/udp	#Simple Net Mgmt Proto

Table 6: Entries in the */etc/services* file for MMB SSH communication

8.1.2.5 XSCF

Port 22 is used for SSH communication.

8.1.3 Reconfiguring port 8886: WSAserver

When changing the UDP port for the WSAserver service, a great deal of care must be taken because this port number has to be changed on the management server and on all administration desktops, too.

Change on the management server:

1. Edit the */etc/services* file and restart the intranet daemon used (*inetd* or *xinetd*).
2. Modify the */opt/SMAW/public_html/wsa.jnlp* and *wsa_ro.jnlp* files if you want to call the browser as a Java Web Start application.

Change on the administration desktop:

- Linux system:

  Modify the *opt/SMAW/bin/svsee* file and add the *–port <new_portnumber>* option to the Java startup line.

- Windows system:

  Modify the *<installation_directory>\wsa.bat* file and add the *–port <new_portnumber>* option to the Java startup line.

8.1.4 Reconfiguring port 8899: dom_adm

When changing the UDP port for the *dom_adm* service, a great deal of care must be taken because this port number has to be changed on the management server and on all managed Linux and Solaris nodes, too.

Change on the management server:

- ► Modify the */etc/services* file and restart the intranet daemon used (*inetd* or *xinetd*).

Change on all managed Linux and Solaris nodes with a ServerView Suite agent:

- ► Modify the */etc/services* file and restart the intranet daemon used (*inetd* or *xinetd*).

> **i** If you are using a firewall, ensure that the *dom_adm* port is transparent in the in transmission direction from the management server to the managed node.

8.1.5 Reconfiguring ports 8881-8883: Webserver ports

ServerView Suite uses ports with the numbers 8881, 8882 and 8883:

- 8881: Java Web Start for read-write access
- 8882: Java Web Start for read-only access
- 8883: Download page for JRE, Windows application, online manuals, Java Policy template

If these port numbers are already occupied by other applications, other port numbers in the range 1024 - 65536 can be used instead for *ServerView Suite*. To do this, proceed as follows:

- ► Log in as *root* on the server concerned.
- ► Change to the */opt/SMAW/public_html* directory and edit the specified port numbers in the *wsa.jnlp*, *wsa_ro.jnlp*, *help.jnlp* and *help_ro.jnlp* files.
- ► Modify the */opt/SMAW/SMAWapac/conf/http_addWSA.conf* file on the management server:

  Example

  Replacing port number 8882 by port number 9992:

  – Change *Listen 8882* to *Listen 9992*
  – Change <*VirtualHost _default_:8882*> to <*VirtualHost _default_:9992*>

Then reboot the WebServer:

- Red Hat: `/etc/init.d/httpd restart`
- SUSE: `/etc/init.d/apache2 restart`

8.2 Dynamic ports

Dynamic ports are defined in XML files. The number of ports needed depends both on the type of connection and the number of systems which are to be connected, and must be calculated carefully. Details are provided in the sections below.

8.2.1 Dynamic ports on the administration desktop

At least one port is needed for each *ServerView Suite* GUI instance on the administration desktop. If SSL communication is used, another port is required for each GUI instance.

Furthermore, the *ServerView Suite* application opens an additional port for each batch job. These batch jobs are:

- PRIMEPOWER Enterprise Server Alignment
- Dynamic Reconfiguration

The figure below shows the communication paths set up when two *ServerView Suite* applications run on one administration desktop and the two are connected with the same management server using SSL.

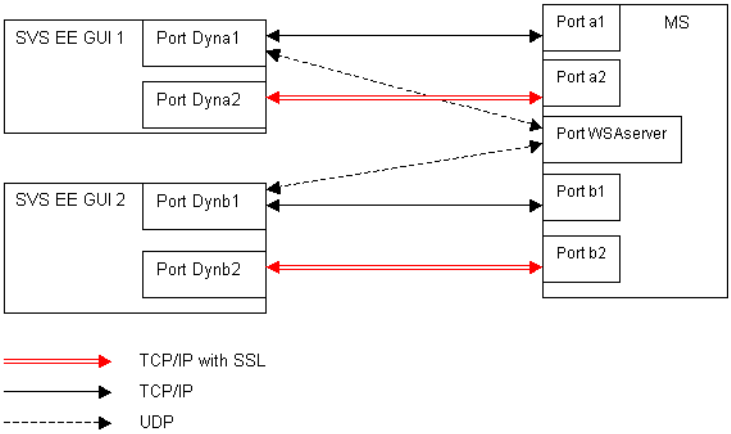

Figure 7: Communication paths

The configuration is defined in the *C:\wsa_certs\WSALocalPreferences.xml* file.

You must proceed as follows if you want to change the range of ports to be used:

1. Create the *C:\wsa_certs* directory (on Windows) or the */opt/SMAW/wsa_certs* directory (on Linux).
2. Call and then terminate the *ServerView Suite* application. This creates the configuration file *WSALocalPreferences.xml* in the aforementioned directory.
3. Adjust the following attributes in the configuration file *WSALocalPreferences.xml* to suit your requirements:

```
<void property="maxUDPport">
   <int>3100</int>
</void>
<void property="minUDPport">
   <int>3000</int>
</void>
```

8.2.2 Dynamic ports on the management server

The port configuration is defined in the */opt/SMAW/users/preferences.xml* file. The changes can be made using an editor.

1. At least one port is needed on the management server for each simultaneous connection between the administration desktop and the management server. If SSL communication is used, two ports are required for each simultaneous server connection. Additionally, one server port is needed for each batch job which has to run in parallel.

   Adjust the following attributes to suit your requirements:

   ```
   <!-- WSA Min Port -->
   <WsaMinPort>10000</WsaMinPort>
   <!-- WSA Max Port -->
   <WsaMaxPort>65535</WsaMaxPort>
   ```

   These changes can also be made via the SVS EE GUI (*Edit → Preferences → General*).

2. Three dynamic domain ports are needed for each managed node which is installed on the *ServerView Suite Agent*. This means that if 50 nodes are to be managed by the management server, at least 150 ports must be reserved.

   Adjust the following attributes to suit your requirements:

   ```
   <!-- Domain Min Port -->
   <DomainMinPort>20000</DomainMinPort>
   <!-- Domain Max Port -->
   <DomainMaxPort>65535</DomainMaxPort>
   ```

   These values only need to be modified on the management server.

Please note that communication is initiated by the managed node. The port number configured above is valid for the management server. Consequently the firewall between the management server and the managed node must be transparent for port 8899 in the transmission direction from the management server to the managed node. The ports in the configuration range DomainMinPort/DomainMaxPort must be transparent for the firewall in the opposite direction.

The figure below shows the communication paths set up between the management server and the administered nodes during a session:

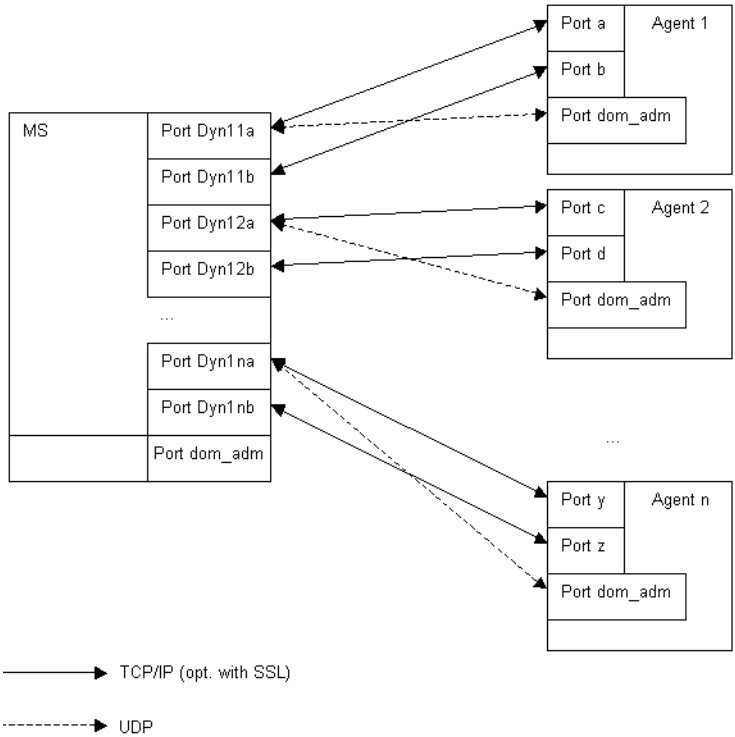

Figure 8: Communication paths

Where

```
dom_adm == 8899
DomainMinPort <= PortDyn1xx <= DomainMaxPort
1024 <= Port x <= 65535
```

8.2.3 Reconfiguring dynamic ports

Dynamic port ranges are easy to reconfigure. Just edit the configuration files mentioned (see the section “Dynamic ports on the management server” on page 61) on the management server and start the GUI again.

9 Configuring PRIMEQUEST

The PRIMEQUEST system must be configured before the PRIMEQUEST is added to the domain on the management server.

9.1 Settings in the MMB Web-UI

The *MMB Web-UI* is used to configure the PRIMEQUEST server. For details, refer to chapter "Setup" of the current *PRIMEQUEST Installation Manual* and in Part III "MMB" of the current *PRIMEQUEST Reference Manual: Basic Operation/GUI/Commands*.

The management LAN and the business LAN must belong to different subnetworks.

For details, please refer to section "LAN configuration (management LAN/private LAN/business LAN)" in the current *PRIMEQUEST System Design Guide*.

PRIMEQUEST Server Agent (PSA) must be correctly configured.

For details, please refer to chapter "Work Required After Operating System Installation" in the current *PRIMEQUEST Installation Manual*.

9.1.1 Configuring the management LAN

PRIMEQUEST servers contain a built-in network switch for switching the management LAN, which enables several modes to be set. Configure the PRIMEQUEST management port as follows:

In the *MMB Web-UI* select the menu options *Network Configuration* → *Management LAN Port Configuration* and enable

- *VLAN Mode* (communication between the partitions is permitted)

  or

- *No VLAN Mode* (communication between the partitions is not permitted).

Port Disable Mode may not be enabled because otherwise no information can be ascertained about the partitions.

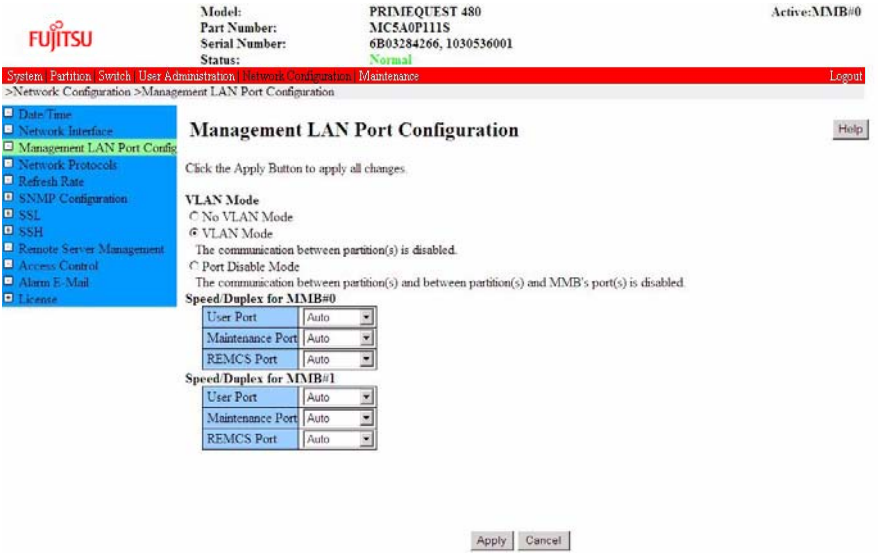

Figure 9: Configuring the management port

For details, please refer to chapter "Setup" of the current *PRIMEQUEST Installation Manual*.

9.1.2 Enabling SNMP

In the *MMB Web-UI* select the menu options *Network Configuration* → *Network Protocols* and enable the SNMP agent and SNMP trap.

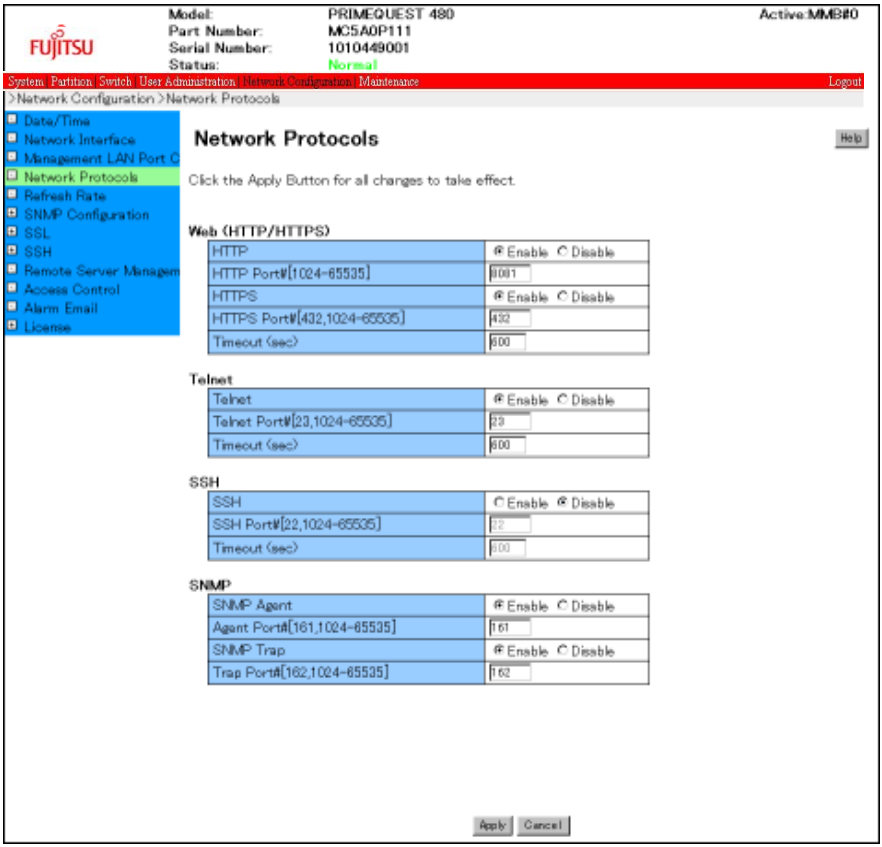

Figure 10: Enabling SNMP

The following settings must be made:

SNMP Agent
: Specify *Enable*.

Agent Port#
: Set the port number to *161*.

SNMP-Trap

Specify *Enable*.

Trap Port#

Set the port number to *162*.

9.1.3 Configuring SNMP

9.1.3.1 SNMP protocol parameters

In the *MMB Web-UI* select the menu options *Network Configuration* → *SNMP Configuration* → *Community* and set the parameters to match the SNMP protocol version v1 which is used.

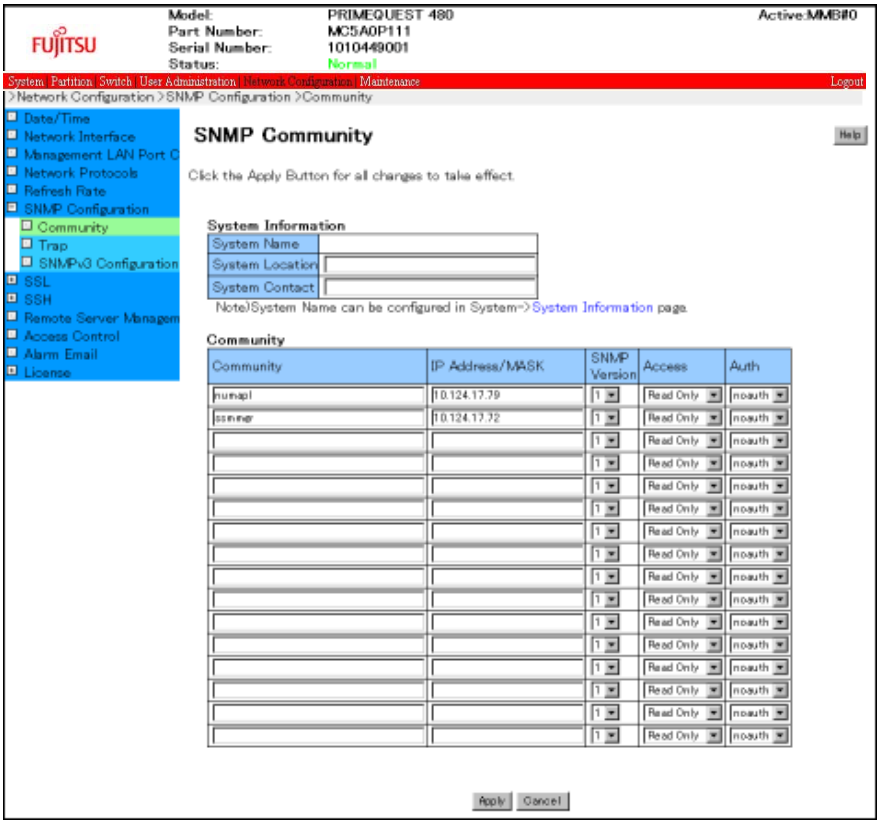

Figure 11: SNMP protocol parameters

The following settings must be made:

Community

Enter a community (up to 32 characters, default: *public*) for communicating with the management server.

IP Address/MASK

Specify the IP address and net mask of the management server that manages the PRIMEQUEST.

SNMP Version

Set the protocol version to *1*.

Access

Select the access authorization *Read Write*.

Auth

Specify *noauth*.

9.1.3.2 SNMP trap parameters

In the *MMB Web-UI* select the menu options *Network Configuration* → *SNMP Configuration* → *Trap* and set the parameters to match the SNMP protocol version v1 which is used.

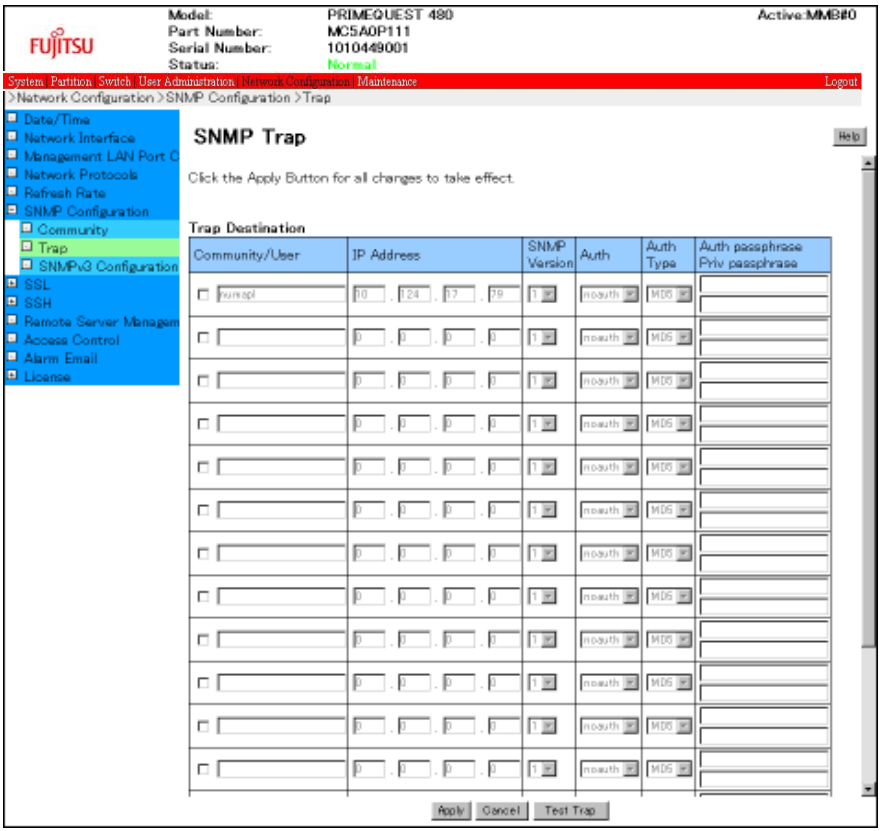

Figure 12: SNMP trap

The following settings must be made:

Community/User
: Specify *public*.

IP Address
: Specify the IP address of the SVS EE management server.

SNMP Version
Select *SNMP version 1*.

Auth
Specify nothing here.

Auth Type
Specify nothing here.

Auth passphrase/Priv passphrase
Specify nothing here.

9.1.4 Configuring access control

The MMB must be configured in such a way that the management server is assigned access rights for the SNMP protocols.

To do this, in the *MMB Web-UI* select the menu options *Network Configuration* → *Access Control*.

If no filter is set for the SNMP protocol, access is not restricted, i.e. you do not need to configure a filter.

If a filter exists, access from the management server must also be explicitly permitted via a filter. You generate a new filter by clicking on the *Add* button and selecting the following in the menu displayed:

- *Protocol*: SNMP
- *Access Control*: select *Enable*
- *IP Address*: IP address of the management server
- *Subnet Mask*: the range of network from whitch access is allowed. If only the access from the management server at *IP Address* is allowed, specify *255.255.255.255*.

Figure 13: Creating a filter

9.1.5 Configuring “Remote Server Management”

The following settings must be made:

In the *MMB Web-UI* select the menu options *Network Configuration* → *Remote Server Management* and set the parameters as shown below.

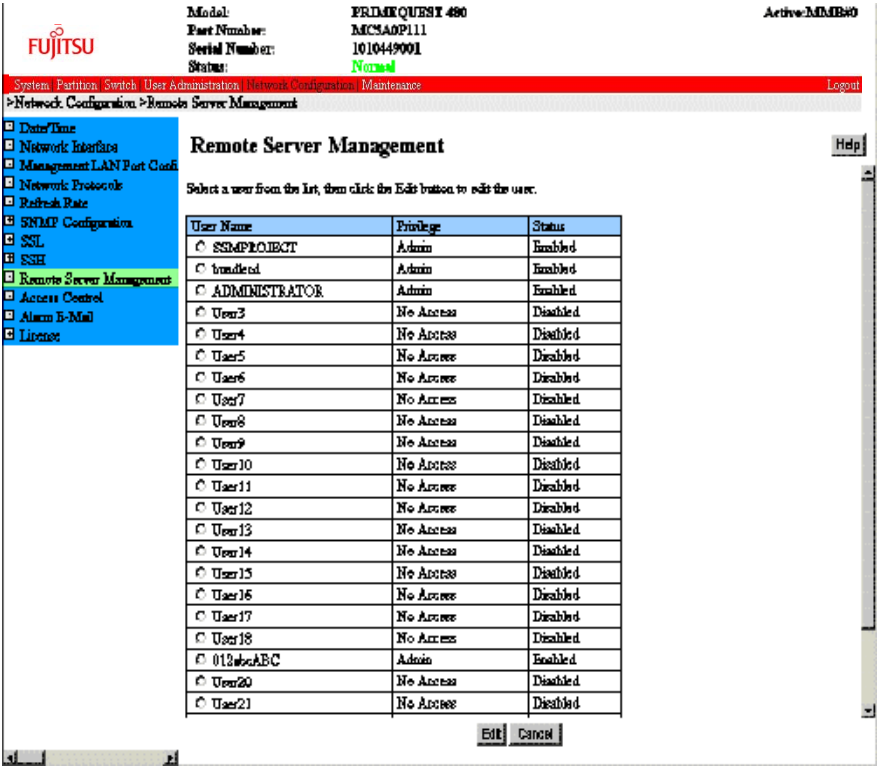

Figure 14: Remote Server Management

User Name

Mark the user name to be used. Select a user with system administrator authorizations.

Mark the appropriate *User Name* and then click the *Edit* button. The following window is displayed:

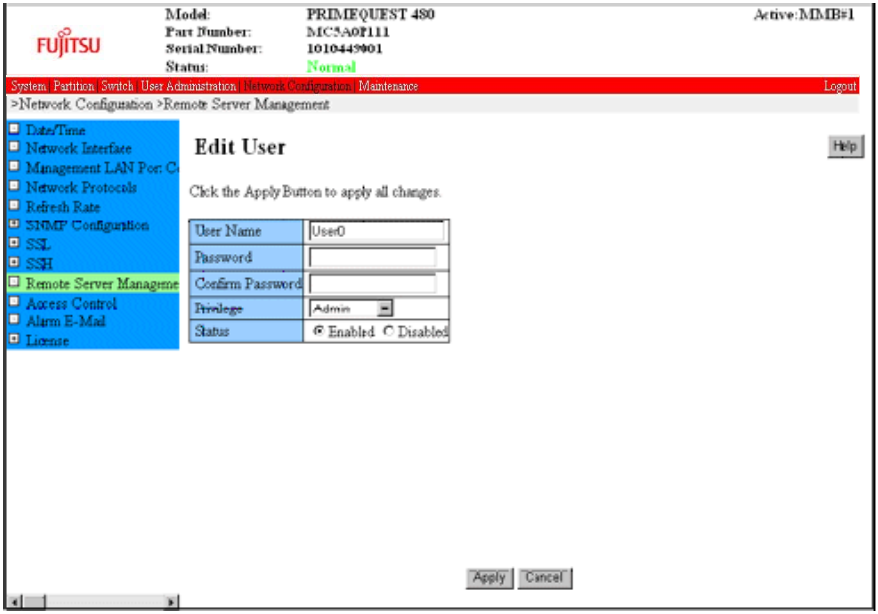

Figure 15: Remote Server Management: Edit User

User Name/Password/Confirm Password

Specify user name and password for communication with the management server.

Privilege

Select *Admin* from the listbox.

Status

Enable the selected user.

9.2 Changing the IP address of the MMB

When you change the IP address of the PRIMEQUEST *Management Board (MMB)*, the definition of the management server must also be updated.

Change the IP address of the MMB as follows:

- Delete the PRIMEQUEST server whose address is to be changed from the domain using the SVS EE GUI.
- Change the IP address of the MMB using the *MMB Web-UI*.
- Call *ServerView Suite* and add the PRIMEQUEST server to the domain again.

9.3 Changing the partition configuration

When you change the partition configuration of a PRIMEQUEST server using the *MMB Web-UI*, the definition of the management server is automatically updated if partitions are created or deleted.

If Linux partitions remain grayed out in one of the applications (*Config/User/Process/Task* etc.):

- Check whether PSA (PRIMEQUEST Server Agent) is installed correctly in the partition.
- Enter the *Domain* application and update the interface using the *Refresh all* button.

9.4 Updating of the management server settings

After changing the configuration of SNMP (see section “Configuring SNMP” on page 67) or of *Remote Server Management* (see section “Configuring “Remote Server Management”” on page 72) for a managed PRIMEQUEST server, the settings on the management server must be updated compatibly.

Change the settings as follows:

- Select the target MMB from the object table in the *Domain* application.
- Click the MMB with the right mouse button and then select the *Modify* function in the sub-menu.
- Change the setting in the dialog box for modifying the PRIMEQUEST server.

10 Configuring SPARC ES

The SPARC Enterprise Server system and the *ServerView Suite Enterprise Edition* management server must be set up in advance before adding the SPARC Enterprise Server to the domain on the management server.

ServerView Suite Enterprise Edition uses SSH to manage SPARC Enterprise Servers. It is necessary to exchange the SSH keys with the management server according to the following two sections before adding the server to the domain.

10.1 Public SSH key of the XSCF

The public SSH key must be installed on both the management server and the XSCF. Proceed as described below to do this.

The procedures described below in this section are not necessary for some models of the SPARC Enterprise Servers which do not have XSCF, such as T-Series models.

For details of XSCF and its SSH setting, refer to the *SPARC Enterprise Server M4000/M5000/M8000/M9000 Servers eXtended System Control Facility (XSCF) User's Guide*.

Check the following requirements for the XSCF.

- SSH is enabled. Check this using the *showssh* command.
- A user account with the *platadm* and *fieldeng* privileges must be prepared for communication with the management server. This user account is used to register the public SSH key of the management server with XSCF.

Registration of the public SSH key of the management server with XSCF

- Log on to the management server as user *root*.
- Execute the following command in order to display the public SSH key of the management server.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_ssh_pubkeyshow
  ```

- Log on to the XSCF as a user account with *useradm* privilege.
- Execute the following command on XSCF. The user account with the *platadm* and *fieldeng* privileges must be specified for the argument of the *-u* option. In the following example, the user account is *platxscf*.

  ```
  XSCF> setssh -c addpubkey -u platxscf
  ```

  This command prompts the user to enter the SSH key. Copy the SSH key specified above and paste it into the XSCF console as the input.

  You start execution by pressing the Enter key and then Ctrl+D (EOF).

- Execute the following command in order to check that the public SSH key is registered correctly.

  ```
  XSCF> showssh -c pubkey -u platxscf
  ```

Registration of the public SSH key of XSCF with the management server

The following procedure assumes that XSCF and the management server are connected to a secure network.

In the example below the IP address of XSCF is 192.168.20.10.

- Log on to the management server as user *root*.
- Execute the following command in order to accept the public SSH key of XSCF. The user account with the *platadm* and *fieldeng* privileges must be specified for the argument of the *-u* option. In the following example, the user account is *platxscf*.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -scf -i 192.168.20.10 -u platxscf
  ```

10.2 Public SSH key on managed node

The public SSH key must be installed on all managed nodes (partitions or T-Series models). Proceed as described below to do this.

The following procedure assumes the managed node and the management server are connected to a secure network.

In the example below the IP address of the agent is 192.168.20.20.

- Log on to the management server as user *root*.
- Execute the following command in order to exchange the public SSH keys of the management server and the partition.

```
# /opt/FJSVaplsc/sbin/aplsc_connect -par -i 192.168.20.20
```

Enter the root account password of the managed node when a password is requested. The password can be requested up to three times.

10.3 Changing the configuration

In some cases it may be necessary to change the SSH configuration for the entire SPARC Enterprise System or for its individual components. For example, a partition can already have a registration for another management server.

The sections below describe what steps must be taken to modify an existing SSH configuration.

The section “Agent with SSH information already registered” on page 84 describes what needs to be done when an agent’s SSH information is already registered on the management server before it is installed.

10.3.1 Changing the public SSH key of the management server

In the following example the IP addresses of XSCF and the managed node are 192.168.20.10 and 192.168.20.20 respectively.

- Log on to the management server as user *root*.
- Execute the following commands in order to delete the SSH information for XSCF and all of the SPARC Enterprise Server agents.

  a) The XSCF

  ```
  # /opt/FJSVaplsc/sbin/aplsc_disconnect -scf -i 192.168.20.10
  ```

  b) The managed node

  ```
  # /opt/FJSVaplsc/sbin/aplsc_disconnect -par -i 192.168.20.20
  ```

  Enter the root account password of the managed node when a password is requested.

- Execute the following command in order to create a new public key for the management server.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_ssh_keyreplace
  ```

- Execute the following commands in order to register the SSH information for XSCF and all of the SPARC Enterprise Server agents. The user account with the *platadm* and *fieldeng* privileges must be specified for the argument of the *-u* option. In the following example, the user account is *platxscf*.

  a) The XSCF

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -scf -i 192.168.20.10 -u platxscf
  ```

  b) The managed node

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -par -i 192.168.20.20
  ```

  Enter the root account password of the managed node when a password is requested. A password can be requested up to three times.

  Depending on the timing, the status of the managed SPARC Enterprise Server may become temporarily unknown after the SSH information has been deleted.

10.3.2 Changing the SSH public key or IP address of XSCF

- Delete the SPARC Enterprise Server from the domain in *ServerView Suite Enterprise Edition*.
- Log on to the management server as user *root*.
- Execute the following command in order to delete the SSH information for XSCF.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_disconnect -scf -i 192.168.20.10
  ```

- Change the XSCF operating environment.

  For details on how to change the operating environment of XSCF, refer to the *SPARC Enterprise Server M4000/M5000/M8000/M9000 Servers eXtended System Control Facility (XSCF) User's Guide*.

- Execute the following command in order to accept the public SSH key of XSCF. The user account with the *platadm* and *fieldeng* privileges must be specified for the argument of the *-u* option. In the following example, the user account is *platxscf*.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -scf -i 192.168.20.10 -u platxscf
  ```

- Add the SPARC Enterprise Server to the domain using the SVS EE GUI.

10.3.3 Changing the public SSH key, the host name or IP address of the managed node

Changing the public SSH key

Use the following procedure to change the public SSH key of the managed node.

- Log on to the management server as user *root*.
- Execute the following command in order to delete the SSH information for the SPARC Enterprise Server agent.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_disconnect -par -i 192.168.20.20
  ```

  Enter the root account password of the managed node when a password is requested.

> **i** If the host name or IP address was changed before the agent was deleted, a warning message is displayed, but can be ignored.

- Log on to the managed node as user *root*.
- Stop the SPARC Enterprise Server agent.

  ```
  # /opt/FJSVaplsa/sbin/svsagtctl stop
  ```

- Execute the following command in order to create a new public key for the managed node.

  ```
  # /opt/FJSVaplsa/sbin/svsagt_ssh_keyinit
  ```

- Start the SPARC Enterprise Server agent again.

  ```
  # /opt/FJSVaplsa/sbin/svsagtctl start
  ```

- Execute the following command on the management server in order to exchange the public SSH keys of the management server and the partition.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -par -i 192.168.20.20
  ```

  > **i** Enter the root account password of the managed node when a password is requested. A password can be requested up to three times.

Changing the host name or IP address

Use the following procedure to change the host name or IP address of the managed node.

- Delete the SPARC Enterprise Server whose host name or IP address is changed from the domain using the SVS EE GUI.
- Log on to the managed node as user *root*.
- Change the host name or IP address of the managed node.
- Change the public SSH key according to the procedure explained above.
- Add the SPARC Enterprise Server to the domain using the SVS EE GUI.

10.3.4 Changing the port number for SSH communication

ServerView Suite Enterprise Edition uses the port number 23460 by default for the SSH communication.

This is an example of how to change the port number to 23400.

- Log on to the management server as user *root*.
- Delete the SPARC Enterprise Server from the domain using the SVS EE GUI.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_disconnect -par -i 192.168.20.20
  ```

  Enter the root account password of the managed node when a password is requested.
- Log on to the managed node as user *root*.
- Add the following port entry in the */etc/inet/services* file in the proper format. If this entry already exists, check that the port number is correct.

  ```
  rcxsshport 23400/tcp
  ```
- Restart the SPARC Enterprise Server agent.

  ```
  # /opt/FJSVaplsa/sbin/svsagtctl stop
  ```

  ```
  # /opt/FJSVaplsa/sbin/svsagtctl start
  ```
- Log on to the management server as user *root*.
- Execute the following command in order to exchange the SPARC Enterprise Server agent.

  ```
  # /opt/FJSVaplsc/sbin/aplsc_connect -par -i 192.168.20.20 -p 23400
  ```

  Enter the root account password of the managed node when a password is requested. A password can be requested up to three times.

10.3.5 Agent with SSH information already registered

If an agent whose SSH information is already registered with the management server is installed on the server, you must first of all delete the SSH information from the management server.

- Log on to the management server as user *root*.
- Execute the following command in order to check whether the SSH information for the agent is registered with the management server.

  # **/opt/FJSVaplsc/sbin/aplsc_ssh_registered -i 192.168.20.20**

  If a text like the text below appears, the SSH information is already registered.

  ```
  192.168.20.20 23460
  ```

- If the SSH information is already registered, delete it from the management server.

  # **/opt/FJSVaplsc/sbin/aplsc_disconnect -par -i 192.168.20.20**

  Enter the root account password of the managed node when a password is requested. The following warning message is displayed, but can be ignored:

  ```
  can't delete remote user public key
  ```

11 Appendix

11.1 Configuring the SV SNMP agents under Linux

The configuration file for the ServerView agents is */etc/srvmagt/config*.

Lines which begin with # are comment lines. Other lines have the format:

<*keyword*>=<*value*>

- *AgentPermission*

  Basic permission for other systems to set values on the local node using SNMP commands (2: not permitted, 3: permitted, default: 2).

  If you wish to permit these SNMP set requests, you must set the value to "3" here and configure the SNMP services accordingly (for details, see chapter “SNMP configuration” on page 35).

- *AgentShut*

  Permission for other systems to shut down/reboot the local node using SNMP commands (2: not permitted, 3: permitted, default: 2).

  If you wish to permit these SNMP set requests, you must set the value to "3" here and configure the SNMP services accordingly (for details, see chapter “SNMP configuration” on page 35).

- *NoAccountCheck*

  If a value other than 0 is defined here, no password is inquired when settings are changed using ServerView. The default setting is 0, i.e. by default user authentication is enabled. In this case a user group must be specified under *UserGroup* to which the user who is to be able to execute the SET operations must belong.

  Note that a disabled password inquiry can present a considerable security risk.

- *UserGroup*

  If 0 was specified for *NoAccountCheck*, ServerView requires a user/password combination on the management server to be able to change SNMP settings. In order to obtain access permission, the user must belong to the group which is defined under *UserGroup*. The default value is *bin*, root also belonging to this.

  If the user group specified here does not yet exist, it must be created using operating system-specific resources.

- *ShutdownDelay*

  Defines the period (in minutes) between an SNMP shutdown request and shutdown.

- *ExpectMylex*

  If a value other than 0 is defined, a trap is always triggered when no Mylex GAM driver exists.

- *ScanTapeDevices*

  If a value other than 0 is defined here, the device files */dev/nst** for tape drives are opened to determine their current status. This can (depending on the driver) result in an inadvertent change to the tape's read/write position. If the tape is used simultaneously by multiple servers, this parameter ensures that ServerView does not disturb ongoing tape operations (e.g. data backup) with status queries.

  The default value is 0, i.e. the tape device files are not opened.

i A change to the *config* file only becomes effective after the agent has been restarted. To do this, restart the managed node or enter the following command as a system administrator:

```
# /etc/init.d/srvmagt restart
```

11.2 Configuring the SV SNMP agents under Windows

You can change the configuration of the ServerView SNMP agents by selecting the *Agent Configuration* menu option under *Start* → *All Programs* → *Fujitsu* → *ServerView* → *Agents* → *Configuration*. A window containing the following three tabs is opened:

- *Trap Forwarding*
- *System Shutdown*
- *Security Settings*

Trap Forwarding tab

All SNMP traps generated by ServerView agents can be reported in the system's event log or forwarded as an administrator message. Forwarding depends on the weight assigned to the trap. The following weights are available:

- critical (for critical traps)
- major (for important traps)
- minor (for less important traps)
- informational (for information traps)

Weighting of the event log types is as follows:

Trap weighting	**Event log type**
Critical and major traps	Error
Minor traps	Warning
Informational traps	Information

Table 7: Weighting of the event log types

The reporting service on the server must be configured and running before a trap can be forwarded to the administrator. The message targets must also already be defined in the properties of Windows Server Manager.

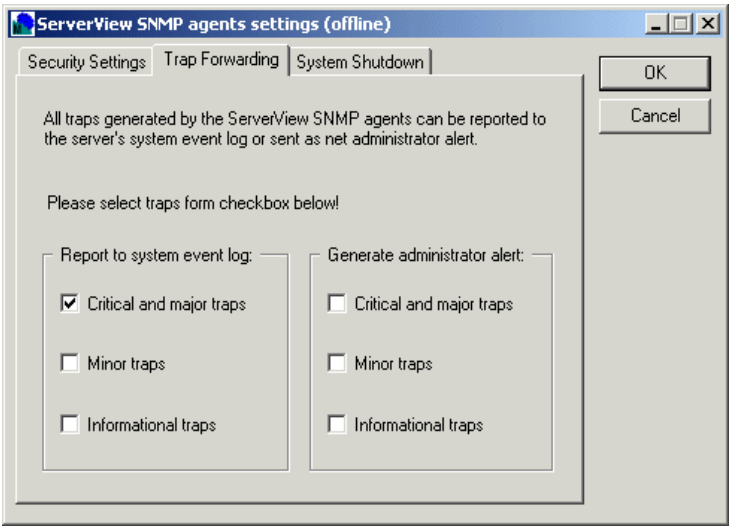

Figure 16: Trap Forwarding tab

Use the *Trap Forwarding* tab to select which types of SNMP traps will be forwarded to where. In the default setting, critical and major traps will be reported to the SVS EE Manager.

System Shutdown tab

ServerView agents can initiate a system shutdown. However, this function is not supported by SVS EE.

Security Settings tab

In conjunction with the management server, ServerView SNMP agents offer an extended security strategy in order to restrict SNMP SET operations on the server. You can prevent access to SET operations or, using user authentication protection, enable access to these operations when performed together with the management server.

If you select the user authentication option, the system will run a user authentication routine each time you start a SET operation. If the authentication routine is successful, the system will also check if the user belongs to a user group defined by the administrator.

The user authentication system only operates with ServerView on the management server. It does not work with other SNMP tools.

You can define the security settings on the tab shown below:

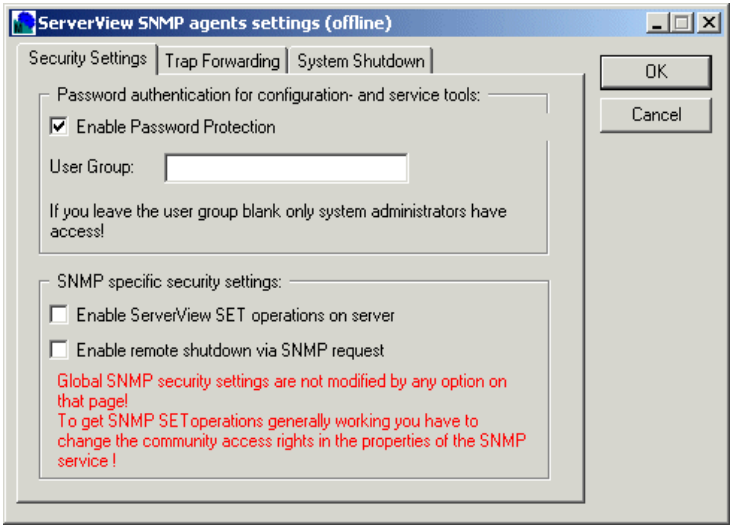

Figure 17: Security Settings tab

Enable ServerView SET operations on server

Enables SNMP SET operations by the ServerView agents. If you forbid SET operations, this will prevent access to all SNMP SETs irrespective of the tool used to run the SET.

This option is for ServerView agents only. It has no effect on the SET operations of other SNMP agents.

Enable Password Protection

This box enables/disables user authentication for SNMP SET operations.

User Group

Specifies the user group to which the users must belong in order to perform SET operations on the server. You can create a user group of your choice here.

If the user group specified here does not yet exist, it must be created on the server using operating system-specific resources.

However, no user group is assigned at this point. You assign a user to a user group at operating system level, either before or after installing the agents. For security reasons, we recommend that you enter one user only.

If you do not enter a name in *User Group*, only local system administrators will be allowed to execute SET operations on the server.

Enable remote shutdown via SNMP request

Some SET operations trigger a shutdown or a system restart. Use this checkbox to enable/disable these special types of SET operation.

No shutdown/restart operations are initiated by the SVS EE components.

Abbreviations

CLI
Command Line Interface

ES
Enterprise Server

GUI
Graphical User Interface

ID
Identifier

IP
Internet Protocol

JRE
Java Runtime Environment

LAN
Local Area Network

MMB
Management Board

MS
Management Sever

NFS
Network File System

PQ
PRIMEQUEST

PSA
PRIMEQUEST Server Agent

PW
PRIMEPOWER

PY
PRIMERGY

RHEL
Red Hat Enterprise Linux

SLES
SUSE Linux Enterprise Server

SNMP
Simple Network Management Protocol

SV
ServerView

SVS EE
ServerView Suite Enterprise Edition

TCP/IP
Transmission Control Protocol/Internet Protocol

UI
User Interface

URL
Uniform Resource Locator

VLAN
Virtual Local Area Network

WSA
Web-based System Administration

XVGA
eXtended Video Graphics Array

XSCF
eXtended System Control Facility

Index