

White Paper

Secure PRIMERGY Server Management

Enterprise Security

PRIMERGY server management for secure, highly available platforms



Content

1.	Preface	4
2.	"Security management is a Process"	4
2.1.	Establishing a Security Concept	4
2.2.	Permanent Adaptation is necessary	5
3.	General issues	6
3.1.	Communication Paths	6
3.1.1.	Network Ports used by the iRMC family	12
3.2.	Protection by Firewalls	13
3.3.	Open Ports	13
3.4.	Separate Management LAN	13
3.5.	SSL Certificate Management	14
3.5.1.	ServerView Certificates	14
3.5.2.	Certificate Fingerprints	15
3.6.	Directory Service Access	15
3.7.	Browser Configuration	16
3.7.1.	Cookies	16
3.7.2.	Scripting	16
3.7.3.	Certificate management	16
3.8.	Secure Boot	18
4.	Configuration, installation and deployment of PRIMERGY servers	19
4.1.	RAID Manager	19
4.2.	Remote Installation with the Installation Manager	20
4.2.1.	Installation of Deployment Components	20
4.2.2.	Reference Installation with the Installation Manager	21
5.	User Management	22
5.1.	Central Authentication Service and Single Sign On	22
5.2.	Unified Role-based access control (URBAC)	22
5.2.1.	Users, user roles and privileges	22
5.2.2.	User Role Assignments	22
6.	ServerView Agents and CIM providers on managed servers	23
6.1.	SNMP Service	23
6.1.1.	SNMP v3	24
6.1.2.	Communication between Agents on MMBs and CPU Blades	24
6.2.	ServerView Agents	24
6.3.	Securing SNMP messages with IPSec	24
6.4.	ServerView CIM Providers	25
6.4.1.	ServerView ESXi CIM Providers	25
6.4.2.	ServerView CIM Provider for Windows	25
6.4.3.	ServerView CIM Provider for Linux	25
6.5.	ServerView Connector Service	26
6.6.	ServerView System Monitor	26
7.	Administration (Operations Manager)	27
7.1.	SNMP Service	27
7.2.	Installation of the Web Server for the Operations Manager	27
7.3.	Exchanging SSL certificates for the Operations Manager	27
7.4.	Restricting the TLS/SSL Cipher Suites for the Operations Manager	28
7.4.1.	Cipher suite configuration resisting BEAST attacks	30
7.4.2.	Security settings for Operations Manager versions >= 8.00	30
7.4.3.	Security settings for Operations Manager versions >= 9.00	31
7.5.	Set Operations with User Authentication	31
7.6.	Event Manager and Antivirus Programs	31
7.7.	Changeable SNMP Ports	31
8.	Maintenance	33
8.1.	Update Management	33
8.2.	PrimeCollect	34
8.3.	Repository Server	34
9.	SNMP Agents for out-of-band management	35
9.1.	...on iRMC	35
9.2.	...on the Management Blade	35
10.	Special configurations	36
10.1.	Options for managing servers in a Demilitarized Zone	36
11.	Summary	37
12.	Log Files	39
13.	ServerView Default Certificates	40
13.1.	Management Controller/Management Blade	40
13.1.1.	Root CA	40
13.1.2.	iRMC Default Certificate	40
13.1.3.	MMB Default Certificate	40

13.2.	ServerView Connector Service (SCS)	40
13.2.1.	Root CA	40
13.2.2.	SCS Default Certificate	40
14.	More Information Regarding Enterprise Security	41
15.	Appendix: Overview of iRMC S4 / Cryptography Support	42
15.1.	IPMI	42
15.1.1.	RMCP	42
15.1.2.	RMCP+	42
15.1.3.	List of supported cipher suites in IPMI	42
15.2.	OpenSSH	43
15.3.	SNMPv3	44
15.4.	Web, KVM, VMEDIA, Redfish (iRMC S5 only)	44
15.4.1.	Cipher list for SSLv3	44
15.4.2.	Cipher list for TLSv1.2	44
15.5.	CIM/SMASH (iRMC S4 only)	45
15.6.	Linux Kernel Ciphers	45
16.	Glossary	46

1. Preface

In the first chapter this document shows that security management is a permanent process, just like quality management. Therefore, this paper is not a guide for security analysis and for establishing security policies. These are important steps, but much more general and much more comprehensive than the scope of this document.

The approach of this document is: You already have a secure system configuration without server management tools. If you now add the PRIMERGY server management components, this document will give you a lot of hints on how to keep the system secure, and how to increase the security of management operations. Of course, more security means also more effort, like planning or configuration. Which of the rules and hints you use, is your decision and should be decided in the context of your overall security policy.

The security considerations in this document cover all phases of the life cycle:

- Installation and Deployment (chapter 4)
- Monitoring and Administration (chapter 5, 6 and 7)
- Maintenance (chapter 8)
- Repair and out-of-band management (chapter 10)

2. "Security management is a Process"

Security cannot be provided by a product or a solution. Only a permanent security management process can provide security. It is comparable to the permanent quality management process.

The other point is that security cannot only be provided by prevention. Prevention systems are never perfect. A security policy must always encompass prevention, detection, and response.

2.1. Establishing a Security Concept

Robust and sensible IT system security comes from correct implementation and maintenance of a well-defined security policy. Such a security policy must take into account – besides the technical issues – a lot of various aspects, such as organizational issues, human aspects, risk probabilities, risk assessment, etc.

In principle, the following steps must be performed to have a well-defined Security Policy:

- Analysis of the values and assets to be protected
- Analysis of the threats
- Assessment of the risks
 - Primary effects, such as loss, destruction, financial effects
 - Secondary effects, such as delays, lost business
 - Tertiary effects, such as loss of trust, loss of customers
- Decision to protect against certain threats
- Selection of appropriate catalogue of measures
- Calculation of costs
- Assessment of the remaining risks

It is highly probable that some of these steps have to be done several times, i.e. it may be a cycle instead of a simple sequence. For example, if the "calculation of costs" shows that the costs are higher than the damage, one has to repeat the "selection of appropriate catalogue of measures" step.

2.2. Permanent Adaptation is necessary

Once you have covered all of these steps, you will have a security policy for the situation as it was at the point of time where the first step "Analysis of the values and assets to be protected" was performed. In an extreme case, the new security policy may already be obsolete. Normally, this is not the case but it illustrates that a security policy must be adapted periodically and in the event of major changes concerning the assets, new potential threats and the availability of new measures, etc.

The following situation is taken as an example for this document: It is assumed that an overall security policy has already been designed for the IT business, i.e. a framework of rules and their implementation in order to achieve the security goals. Whenever new components are added, processes are changed, or organizations are modified, etc., the security policy must also be adapted. An event that requires such an adaptation may also be the deployment of a certain server management tool.

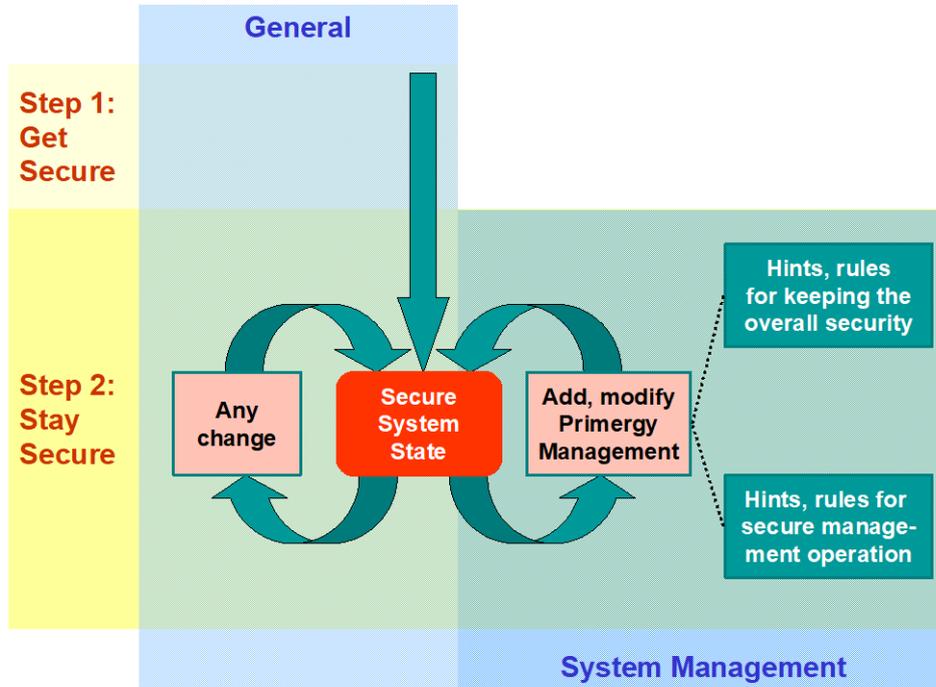


Fig. 1: Security Approach

Fig.1 illustrates this approach. The General approach consists of the two steps "Get Secure" and "Stay Secure".

This document follows the following approach: You have already done the first step, i.e. you have achieved a secure system configuration, and you now add or modify the configuration of a component of the ServerView Suite for PRIMERGY servers. This document provides two types of hints for this that aids you in the "Stay secure" step:

- Hints and Rules that help you keep your overall system secure. For example, installing a Web server may result in security holes if you don't apply certain rules.
- Hints and Rules that increase the security of the server management operations, e.g. so that no unauthorized persons can perform management operations.

The security aspects and implications of using a certain server management tool must be assessed in the context of the existing IT configuration as well as in the context of the existing security policy. Both are individual. Therefore, this document cannot provide security solutions concerning server management, but it will provide you with information and assistance for adapting your security policy when using the ServerView Suite for PRIMERGY servers.

As mentioned above, prevention systems are never perfect; the number of potential vulnerabilities is too high and attackers are opportunistic – taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely available attacking tools. A good strategy is to close these security holes.

They are referenced at various places in the subsequent sections.

3. General issues

3.1. Communication Paths

This section describes all the communication paths that are used by the different components/tools of the PRIMERGY ServerView Suite. As described in the "ServerView Suite: Basic Concepts" manual, the components of the ServerView Suite can be divided into four categories:

- management consoles,
- management applications,
- helpers, and
- managed nodes.

Figure 2 is a schematic view on these server management components, which category they belong to, and how they communicate with one another. These components can be installed on different computers. However, it is also possible to install several components from different categories on a single computer.

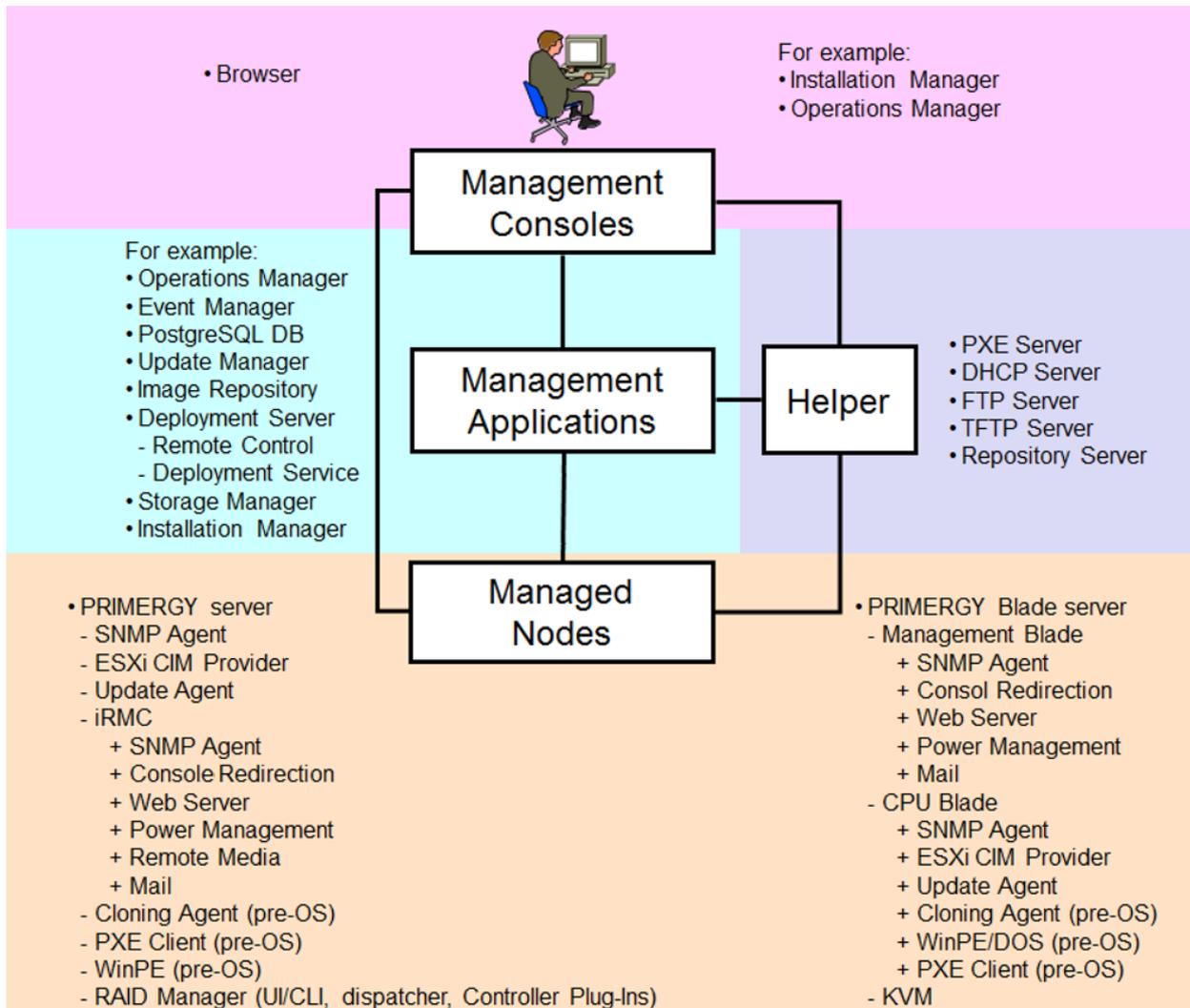


Fig 2: Communication Paths used by the ServerView Suite for PRIMERGY servers

Please note that the iRMC provides more communication paths which are not all used by the PRIMERGY ServerView Suite:

- IPMI
- SSDP
- eLCM
- virtual media
- AIS connect
- USB Host LAN
- AVR

For more information on iRMC security aspects, please see chapter 10.3.1.

The following table describes, which communication protocols are used and which ports are used per default. Per default mainly well known ports (range 0 through 1023) and IANA-registered ports (1024 through 49151) are used. The ports 3169 through to 3173, 3789, 4178, 9212 and 9213 have been registered at the IANA exclusively for PRIMERGY server management.

For more information, see <http://www.iana.org/assignments/port-numbers>.

However, most ports can be configured individually on other port numbers.

↔: communication path in both directions

← or →: communication in one direction

Communication	Port: Protocol Purpose
Management Consoles – Management Applications	
Browser ↔ Operations Manager	3169 (IANA-registered port): UDP/TCP
Browser ↔ Event Manager	TomEE Application Server
Browser ↔ Update Manager	3170 (IANA-registered port): UDP/TCP
Browser ↔ Remote Management/Web Frontend	TomEE Application Server over SSL
Browser ↔ Deployment Manager	3172 (IANA-registered port): UDP/TCP
Browser ↔ Virtual I/O-Manager	SV Connector Service (SCS)
Browser ↔ Installation Manager	3169 (IANA-registered port): UDP/TCP ServerView Application Service 3170 (IANA-registered port): UDP/TCP ServerView Application Service over SSL
Mailserver ← Event Manager	25: UDP/TCP SMTP Mail (configurable)
vCenter Plugin ↔ vCenter ServerView Plugin Appliance	3170: HTTPS Please see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1012382 for a list and description of further vCenter related port usages. 9092 (on localhost only, external access can be prevented by firewall): Internal Database H2 5480: Configuration port of Plugin appliance
vRealize Orchestrator ↔ vCenter ServerView Plugin Appliance	3170: HTTPS
vRealize Operations ↔ vCenter ServerView Plugin Appliance	3170: HTTPS
The NAGIOS Plugin script accept variable port parameters. The following defaults are used:	
Script ↔ SNMP	161
Script ↔ CIM-XML	https: 5989, http: 5988
Script ↔ WS- MAN	ESXi https: 8888, http: 8889, Other https:5986, http:5985
Script ↔ REST	SCS: 3172 iRMC https: 443, http: 80
CIM Indications - Listener	https and http: 3169
Browser <- -> System Monitor	3172: SV Connector Service (SCS) (IANA-registered port): UDP/TCP
Management Consoles – Managed Nodes	
Browser (Advanced Video Redirection) ↔ iRMC Web-Server	80: UDP/TCP Web HTTP (configurable) 443: UDP/TCP HTTP over TLS/SSL (configurable)
Browser ↔ Management Blade: Web-Server	
Administrator ↔ Linux CIM Agent	5989: Incoming and outgoing TCP CIM-XML transactions over HTTPS 5988: Incoming and outgoing TCP CIM-XML transactions over HTTP 5986: Incoming and outgoing TCP WS-MAN transactions over HTTPS 5985: Incoming and outgoing TCP WS-MAN transactions over HTTP

Communication	Port: Protocol Purpose
Administrator ↔ Windows CIM Agent	5986 / 443: Incoming and outgoing TCP WS-MAN transactions over HTTPS 5985 / 80: Incoming and outgoing TCP WS-MAN transactions over HTTP
Client ↔ iRMC Remote Manager/SMASH CLP	22: TCP (SSH, configurable) 3172: TCP (Telnet, configurable)
Client ↔ IPMI-over-LAN	623: UDP (RMCP+ / Serial over LAN)
Browser / S3 Client SW ↔ External KVM KVM S2-1611 / KVM S2-0411 / KVM S3-1621	3211: UDP/TCP Proprietary Protocol 2068: TCP Encrypted keyboard and mouse data, digitized video data, virtual media 8192: TCP Digitized video data 389: UDP LDAP (non-secure) 636UDP LDAP (secure)
Administrator ← iRMC/Management Blade: E-mail Alerting	25: UDP/TCP SMTP Mail (configurable)
Browser ↔ RAID Manager	3173 (IANA registered port):): UDP/TCP HTTP over SSL
Configuration Manager ↔ PRIMERGY Server Configuration Manager ↔ CPU Blade	3172 (IANA-registered port): UDP/TCP SV Connector Service (SCS)
Installation Manager ↔ Installation Agent	9213 (IANA-registered port): UDP/TCP Installation Manager Remote Control (configurable)
Installation Manager → Installation Agent	5001: TCP Installation Manager Remote Control (not configurable)
ServerView Tomcat ↔ ESXi, MMB	3170: TCP (cim.listening.port) 3169: Indication listener 161: UDP/TCP SNMP 162: UDP/TCP SNMP traps 5989: CIM service on ESXi Please see http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-ECEA77F5-D38E-4339-9B06-FF9B78E94B68.html and http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1012382 for a list and description of further vCenter related port usages.
Redfish Client ↔ iRMC	iRMC S5 443: TCP (configurable) Redfish service
ISM ↔ iRMC	iRMC S5 1900: UDP for autodiscovery by UPnP SSDP (closed if SSDP is disabled) 50000: TCP/UDP for UPnP description (closed if SSDP is disabled)
Management Console – Management Console (SVOM V7.11 and higher)	
TomEE	8005 Shutdown port
TomEE	8009 Apache JServ Protocol (AJP) Port
TomEE	All other ports are allocated dynamically from the "Dynamic Port" range defined by RFC 6335.
Management Console – Management Console (SVOM V7.20 and higher)	
TomEE	31705 Shutdown port
TomEE	All other ports are allocated dynamically from the "Dynamic Port" range defined by RFC 6335.
Ports 1325, 1445, 4713, 8009, 8090, 9443, 9990, 9999 are no longer used	

Communication	Port: Protocol Purpose
Management Application - Directory Service	
Central Authentication Service ↔ Directory Service	389: LDAP default port (non-secure) 636: LDAP SSL default port 1473: LDAP port of ApacheDS / OpenDJ of ServerView (non-secure) 1474: LDAP SSL port of ApacheDS / OpenDJ of ServerView
Management Application - Management Application	
OpenDJ Control Panel ↔ OpenDJ	4444: Management Port of OpenDJ of ServerView (only on IP address 127.0.0.1)
Operations Manager ↔ PostgreSQL DB (nur Linux) Event Manager ↔ PostgreSQL DB (nur Linux)	9212 (IANA-registered port): UDP/TCP
Event Manager → Operations Manager	Dynamic: UDP SNMP: Notification from Event Manager for Operations Manager
Operations Manager ↔ Storage Manager	4178 (IANA-registered port): UDP/TCP StorMan
Management Application - Management Application (SVOM V9.02 and higher)	
Operations Manager ↔ JMX bean	19876: Session Director (only on IP address 127.0.0.1)
Management Application – Managed Nodes	
Operations Manager ↔ SNMP-Agent Event Manager ↔ SNMP-Agent Operations Manager ↔ SNMP-Agent (CPU Blade) Event Manager ↔ SNMP-Agent (CPU Blade) Remote Control (DLL on Deployment Server) ↔ SNMP-Agent (CPU Blade) Operations Manager ↔ SNMP (Management Blade) Event Manager ↔ SNMP (Management Blade)	161: UDP/TCP SNMP 623: UDP IPMI over LAN / RMCP
Operations Manager ← SNMP-Agent Event Manager ← SNMP-Agent Event Manager ← SNMP-Trap(iRMC) Operations Manager ← SNMP-Agent (CPU Blade) Event Manager ← SNMP-Agent (CPU Blade) Operations Manager ← SNMP (Management Blade) Event Manager ← SNMP (Management Blade)	162: UDP/TCP SNMP Traps
Operations Manager ← Agent (Performance Management & Power Monitoring & Online Diagnosis & PrimeCollect & Configuration Manager & ServerListService & TestConnectivity & VME Services – Results)	3172 (IANA-registered port): UDP/TCP SV Connector Service (SCS)
Operations Manager ↔ ESXi CIM Provider	5989: Incoming and outgoing TCP CIM-XML transactions over HTTPS (5988: Incoming and outgoing TCP CIM-XML transactions over HTTP)
Update Manager ↔ Update Agent Update Manager ↔ Update Agent (CPU Blade) Update Manager ↔ Update Agent Provider (SOAP)	3171 (IANA-registered port): TCP Firmware flash (configurable) 3172 (IANA-registered port): UDP/TCP SV Connector Service (SCS) (Certificate Checks)
Update Manager ↔ Management Blade/ Connection Blade	161: UDP/TCP SNMP (read-only) 22: TCP (SSH, not-configurable) 80: UDP/TCP Web HTTP
Operations Manager ↔ iRMC	161: UDP/TCP SNMP (read-only) 623: UDP RMCP / IPMI over LAN 80: UDP/TCP Web HTTP 443: HTTPS
Installation Manager ↔ Installation Agent (WinPE)	9213 (IANA-registered port): UDP/TCP Installation Manager Remote Control (configurable)

Communication	Port: Protocol Purpose
Installation Manager → Installation Agent (WinPE)	5001: TCP Installation Manager Remote Control (not configurable)
Remote Management/Web Frontend ↔ Management Blade Text Console Redirection Remote Management /Web Frontend ↔ iRMC Text Console Redirection	623: UDP: IPMI over LAN / RMCP 3172 (IANA-registered port): UDP/TCP (SSL) Telnet: Console Redirection Remote Manager Interface (configurable)
Operations Manager ↔ VMware Host	443: UDP/TCP HTTP over TLS/SSL (SOAP)
Operations Manager ↔ Xen Host	9363: TCP XML-RPC
Operations Manager ↔ Hyper-V Host	135: WMI / DCOM, Remote procedure call. Dynamic: RPC Ephemeral Range 3172: (Hyper-V host) Performance and threshold data.
Operations Manager ↔ KVM Host	16509: TCP 16514: TLS
Virtual-IO Manager ↔ Management Blade	3172: (IANA-registered port): TCP (Telnet, configurable) 22: TCP (SSH, configurable)
Virtual-IO Manager ↔ Intelligent Blade Panel (IBP)	23: (IANA-registered port): TCP (Telnet, configurable) 22: TCP (SSH, configurable)
Virtual-IO Manager ↔ iRMC	623: UDP: RMCP (IPMI over LAN) 162: SNMP traps from iRMC to management station
vRealize Orchestrator → iRMC	623: UDP: RMCP (IPMI over LAN) 80/443: HTTP(S) Communication to eLCM REST API
vCenter Plugin → iRMC	623: UDP: RMCP (IPMI over LAN) 80/443: HTTP(S) Communication to eLCM REST API
vCenter ServerView Plugin Appliance ↔ iRMC	623: UDP: RMCP (IPMI over LAN) 80/443: HTTP(S) Communication to eLCM REST API 162: SNMP traps from iRMC to management station
vCenter Plugin → ESXi CIM Provider	5989: CIM-XML transactions over HTTPS (5988: CIM-XML transactions over HTTP)
vCenter ServerView Plugin Appliance ↔ ESXi CIM Provider	5989: CIM-XML transactions over HTTPS (5988: CIM-XML transactions over HTTP) 3169/3170: HTTP(S) (indications from host to management station)
vCenter ServerView Plugin Appliance ↔ SNMP (Management Blade)	161: UDP/TCP SNMP
vCenter ServerView Plugin Appliance ← SNMP (Management Blade)	162: UDP/TCP SNMP Traps
Management Application – Management Application	
Virtual-IO Manager ↔ Virtual-IO Manager	50042: Management Station internal communication

Management Applications – Helpers	
Update Manager ↔ PXE Server (Update Proxy)	3171 (IANA-registered port): TCP
Update Manager ↔ TFTP Server (Update Proxy)	Firmware flash (configurable)
Deployment Service ↔ PXE Server	Local
Managed Nodes – Helpers	
Update Agent ↔ PXE Server (Update Proxy)	3171 (IANA-registered port): TCP Firmware flash (configurable)
Update Agent ↔ PXE Server (PXE Boot)	67: UDP/TCP Bootstrap Protocol Server (bootps)
PXE Client ↔ PXE Server WinPE ↔ PXE Server PXE Client (CPU Blade) ↔ PXE Server WinPE (CPU Blade) ↔ PXE Server Update Agent ↔ PXE Server (PXE Boot)	4011: UDP/TCP Alternate Service Boot
PXE Client ↔ TFTP Server WinPE ↔ TFTP Server PXE Client (CPU Blade) ↔ TFTP Server WinPE (CPU Blade) ↔ TFTP Server Update Agent ↔ PXE Server (PXE Boot) Management Blade ↔ TFTP Server	69: UDP Trivial File Transfer (TFTP)
Management Blade ↔ TFTP Server	161: UDP/TCP SNMP 80: UDP/TCP Web HTTP
Update Agent ↔ SwitchBlade	22 SSH (Plink) ConnectionBlade FW flashing

3.1.1. Network Ports used by the iRMC family

For better readability the next table summerizes all ports used by the iRMC S4 / S5:

http:	80 inbound to iRMC (configurable)
https:	443 inbound to iRMC (configurable)
SSH:	22 inbound to iRMC (configurable)
Telnet:	3172(/23) inbound to iRMC (configurable)
SMTP:	25 outbound from iRMC (configurable)
SNMP:	161 inbound to iRMC, outbound from iRMC (configurable)
SNMP Traps:	162 outbound from iRMC (fixed)
LDAP:	389 (non secure) 636 (secure) outbound from iRMC (configurable)
CAS / Single Sign On:	3170 inbound to iRMC, outbound from iRMC (configurable)
RMCP:	623 inbound to iRMC (fixed as per IPMI 1.5/2.0 Spec)
iRMC S1 (AVR and Remote Media):	
AVR(Video):	5900 inbound to iRMC (configurable)
AVR(Secure):	5910 inbound to iRMC (configurable)
Remote Media:	5901 outbound from iRMC to Applet(configurable)
Remote Media:	5901 outbound from iRMC Standalone Storage Server (configurable/shared with Applet)
iRMC S2 (AVR and Remote Media - up to Firmware 5.0x)	
AVR(Video):	80 inbound to iRMC (configurable/shared with http port)
AVR(Secure):	443 inbound to iRMC (configurable/shared with https port)
Remote Media:	5901 outbound from iRMC to Applet (configurable)
Remote Media:	5901 outbound from iRMC Standalone Storage Server (configurable/shared with Applet)
iRMC S4 / S5	
tftp:	69 outbound from iRMC (fixed)...
iRMC S5	
Redfish:	443 inbound to iRMC (configurable)
SSDP:	1900 inbound to iRMC (only if SSDP is enabled) 50000 inbound to iRMC (only if SSDP is enabled)

3.2. Protection by Firewalls

Firewalls are used to prevent attacks from the Internet. If all components/tools of the PRIMERGY management products along with the managed systems are located behind the firewall, all communication paths are protected from attacks from the Internet. Nevertheless, the administrator may access the management at anytime and from anywhere by means of a browser via the Internet. I.e., in this ideal situation, only the communication paths

- between the browser with Java-Front-ends (Management Console) and the applications, like Operations Manager, and
- between the browser with Java-Front-ends (Management Console) and Web server on iRMC, and Management Blade have to pass the firewall, and these communication paths can be secured by a SSL, as is shown later.

Recommendation 1

Locate all components/tools of the PRIMERGY management suite along with the managed systems behind the firewall. The Web-based tools may be accessed by a browser via the Internet. This communication path should be secured by a SSL (see also Recommendation 30)

Sometimes, however, it may be sensible to have a configuration, where SNMP traps are sent through firewalls, in order to get information about certain events, which happen inside of the firewall. In this case, you must take care, that the firewall is open for UDP port 162, otherwise the SNMP traps are blocked.

3.3. Open Ports

Both, legitimate users and attackers connect to systems via open ports. The more ports that are open means that there are more possible ways that someone can connect to your system. Therefore, it is important to keep the least number of ports open on a system that is necessary for it to function properly. All other ports should be closed.

The tables above provide you with the necessary information needed to decide which ports must be open for the PRIMERGY server management. As the drawing shows, this varies from system to system and depends on the configuration and which components/tools are located on the system.

Recommendation 2

Minimize the number of open ports for each system. The tables above show you which open ports are required by the PRIMERGY ServerView Suite.

3.4. Separate Management LAN

The purpose of firewalls and of minimizing the number of open ports is to protect the management components against unauthorized access. This goal can be achieved also by separating the management LAN from the operational LAN by configuring a VLAN for server management. This shields the management LAN traffic from the operational traffic on a logical layer. Based on Figure 2 and the tables, which describe the communication paths used for PRIMERGY management, you can plan a VLAN topology for the complete management communication or for selected security relevant paths.

Recommendation 3

Separating the management traffic from the operational traffic on the LAN can improve the security significantly. You can achieve this by configuring a VLAN topology for the management traffic based on Figure 2 and the tables that describe the communication paths used for PRIMERGY management.

The Remote Management Controller (iRMC) as well as the Management Blade have their own physical network interfaces. This enables to build up a separate physical management LAN between these components and the corresponding front-ends. This results in some additional efforts, but obviously, it results also in a highly secure PRIMERGY management.

Recommendation 4

The iRMC and the Management Blade have their own physical network interfaces, which can be used to build up a separate physical management LAN. This assures on a physical base that all security-sensitive operations, which can be performed via these components, can only be started from nodes connected to this physically separated management LAN.

3.5. SSL Certificate Management

All HTTP connections to ServerView products are secured using the Secure Sockets Layer (SSL). Using this protocol includes transferring a certificate from the server to the client:

"In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual." (From: Wikipedia, the free encyclopedia.)

The client must trust the certificate, or refuse establishing the connection. For this purpose every client has a list of certificates he trusts on. This list is widely called a Trust Store. In general, a certificate is signed by a so-called Certificate Authority (CA), who is represented by another certificate. If a client trusts a CA, then he has to trust also all certificates signed by this CA. A certificate representing a CA can be signed on its side by another CA. Thus a single certificate may be trusted due of a chain of certificates. The CA standing behind the uppermost certificate of such a chain is called the Root CA. There is a lot of Root CAs whom the Internet Explorer and the Firefox browser trust by default. You can look up this list in the property settings of the respective browser.

3.5.1. ServerView Certificates

The table below shows in which ServerView products certificates are used, and for what purpose:

SV Product	Purpose	Remarks
Operations Manager	Encryption, Identification, Authentication	Created during Installation
Agents	Encryption	Created at production time
ServerView Raid	Encryption	Created during Installation
iRMC	Encryption	Created at production time / Online
MMB	Encryption	Created at production time

If you connect your browser to a ServerView web server which has only the certificate installed during its setup, you will receive a warning from the browser because such a certificate is never signed by a CA. At that point you can permanently import the certificate into the respective trust store of browser in order to avoid future warnings. When doing this, be very careful, and check the "fingerprints" (or "thumbprints") of the server certificate. How the fingerprint is retrieved in case of the server certificate of ServerView Operations Manager, is described below in the section 7.3, "Exchanging SSL certificates for the Operations Manager".

All ServerView products allow exchanging the server certificate by a customer-provided one. If you have the possibility to apply certificates signed by a CA, then it is recommended that you replace the installed certificates with CA-signed certificates. For details how to exchange the certificate, please have a look in the respective documentation of product. Even if you do not want to buy a signed certificate from one of the commercial CAs or their resellers, you can establish your own CA with a self-signed certificate and derive your server certificates from that CA. This has the advantage that you need only import the certificate of CA once into your browsers, because the derived certificates are then automatically trusted. This way, you will be less tempted immediately accepting an unknown certificate without fingerprint checking when opening a new HTTPS connection.

Recommendation 5

Establish your own Certificate Authority (CA) if you do not want to buy certificates signed by (commercial) CAs already trusted by the browser. Then import your certificate of CA into all browsers used for operating ServerView products.

Note that if you exchange a certificate that has already been imported, e.g. on managed nodes, you have to re-import the exchanged certificate. Therefore you should replace an installed certificate as soon as possible.

Recommendation 6

For security reasons, it is highly recommended to use the SSL option for the web interface of any ServerView product, and to replace the predefined certificate by a certificate from a Certificate Authority (CA) as soon as possible.

Hint

A description how the self-signed certificate of the ServerView Operations Manager (SVOM) is exchanged is found in section 4.2.4, "Replacing the certificate on the Central Management Station", of the "User Management in ServerView" manual. This manual can be downloaded from the [Manuals Download Page](#).

3.5.2. Certificate Fingerprints

Unlike with former versions of the Operations Manager, in version 5.00 or higher the server certificate is not only used for encryption, but also for identifying the server. Therefore the private key and the server certificate are not delivered on the installation medium, but only created individually when the installation takes place. As a consequence, the certificate is not signed by a Certificate Authority, but only self-signed. The browser will thus not present start page of ServerView, but display a warning like "This Connection is Untrusted" or "There is a problem with this security certificate of the website" and ask the user whether to proceed with loading the page, or not. If you proceed at this point and are not totally sure to which server you are connected, you should not issue any sensible data like passwords, but first check meticulously the server certificate by comparing its "fingerprint(s)" or "thumbprint(s)" with the one of the private key of server. You get the fingerprint(s) on the CMS by issuing the following command using an administrative account (or the account which JBoss is started with):

Linux:

```
{JAVA_BIN_PATH}keytool -keystore ${PKI_PATH}keystore -storepass ${STOREPASS} -list -v
```

Windows:

```
%JAVA_BIN_PATH%keytool -keystore %PKI_PATH%keystore -storepass %STOREPASS% -list -v
```

The meanings of the placeholders are the following:

JAVA_BIN_PATH: the path to the bin directory of the Java installation, e.g.
C:\Program Files (x86)\Java\jre6\bin\

PKI_PATH: the path to the pki directory of the ServerView Suite installation, e.g.
C:\Program Files (86)\Fujitsu\ServerView Suite\jboss\server\serverview\conf\pki\

STOREPASS: the password of keystore. Currently this is always changeit.

In the extensive output of this command the lines under the heading `Certificate Fingerprints` contain the requested information, like in the following example:

```
Certificate Fingerprints
MD5:   B9:6E:38:F4:B6:9C:80:0D:79:C4:ED:D4:FC:92:69:E4
SHA1:  58:DE:5C:0B:62:E2:94:77:51:09:40:9C:0A:6D:99:B1:0C:53:B5:C5
```

You will need this fingerprint when importing the server certificate of the CMS into the trust store of your browser. Therefore print it out, or copy it to a secure medium in order to have it for the comparison later on.

Recommendation 7

Print out the fingerprint of server certificate, or copy it on a medium like an USB stick for having the possibility to compare it with the value given by the browser when establishing the SSL-secured HTTP connection.

Although pre-produced certificates of ServerView are not suitable for identifying a certain web server, their fingerprints are listed in this document for completeness, cf. section 140, "ServerView Default Certificates".

3.6. Directory Service Access

ServerView makes use of a directory service for authentication and authorization of a user (cf. section 5, "User Management"). The directory service is accessed by means of the Lightweight Directory Access Protocol (LDAP). While built-in directory service of ServerView is automatically configured with the secure LDAP variant (LDAPS), the user is free to choose LDAP when setting up an external directory service. This is, however, not recommended except for experimental environments, because credentials of user are transferred decrypted via the LDAP connection.

Recommendation 8

Configure SSL-secured LDAP for accessing an external directory service.

For accessing the user data in the directory service, an account of a user of the directory service must be configured. For security reasons, this user account should have only lowest (read-only) user rights.

Recommendation 9

Configure the LDAP access to an external directory service using a service account with lowest user rights.

3.7. Browser Configuration

The browser is nowadays one of the main goals for attacks out of the Internet. Therefore you should configure and handle your browser with care in order to avoid security gaps. This is particularly valid if you use it also for browsing the Internet. Introductions into the possible security problems of Browser and their solution are found at various places in the internet. Please note that when using Internet Explorer, you should add all hosts running web servers of ServerView products to the list of trusted sites if you are operating the browser with standard security settings. Please note further that "in private" browsing is not supported by web pages of ServerView.

In the following, some special hints related to web page of ServerView are given:

3.7.1. Cookies

You should meticulously control the setting of cookies in your browser. Please note in this context that web pages of ServerView set the following cookies, which are necessary for their proper working:

JSESSIONID: This is the session tracking cookie prescribed by the [Java™ Servlet Specification](#). Because ServerView makes use of the Apache Tomcat Java Container contained in its JBoss Application Server, you must allow setting this cookie for proper operation of web pages of ServerView.

AURA: This is another session tracking cookie which is solely used by ServerView Raid.

CASTGC: This is the Ticket Granting Ticket Cookie of Central Authentication Service (CAS) of ServerView. If you prevent the service from setting this cookie, then you will not have the Single Sign On feature, i.e. you will have to login to any single web server of products of ServerView.

org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE: This cookie is set by the [Spring Framework](#) used by CAS of ServerView in order to store the language used at the GUI. You may refuse to let this cookie be set without functional disadvantages, because the used language is additionally always provided by the HTTP parameter `Lang`.

Please note further that in the cookies settings of Firefox the option **third-party cookies are allowed** must be set for proper working of the ServerView Operations Manager.

3.7.2. Scripting

You should also restrict the use of scripting languages as far as possible. But please note that you have to enable JavaScript and the use of Java Applets for operating ServerView web pages.

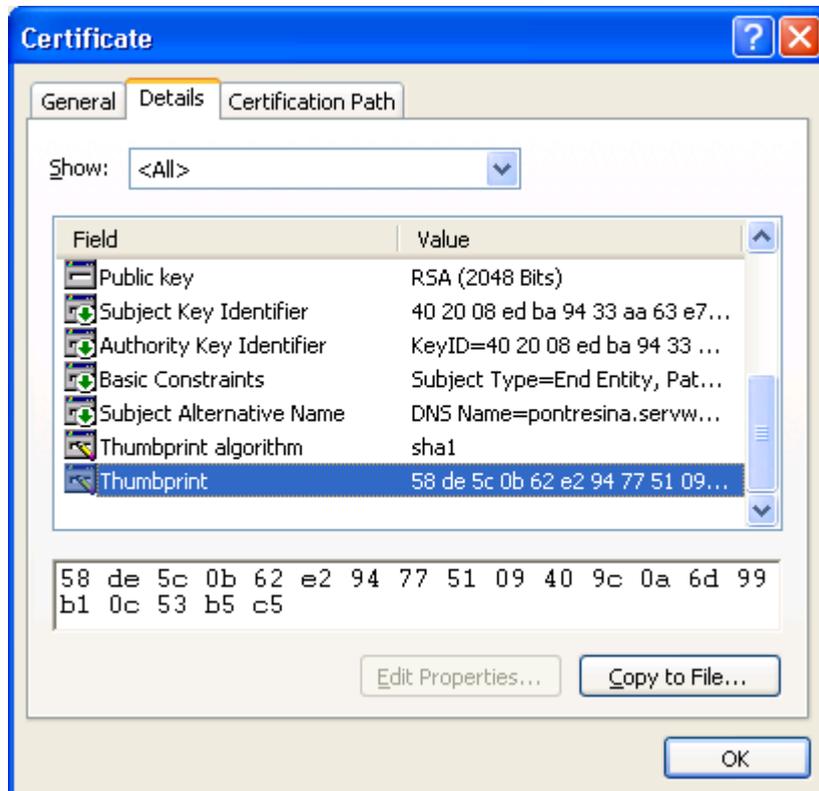
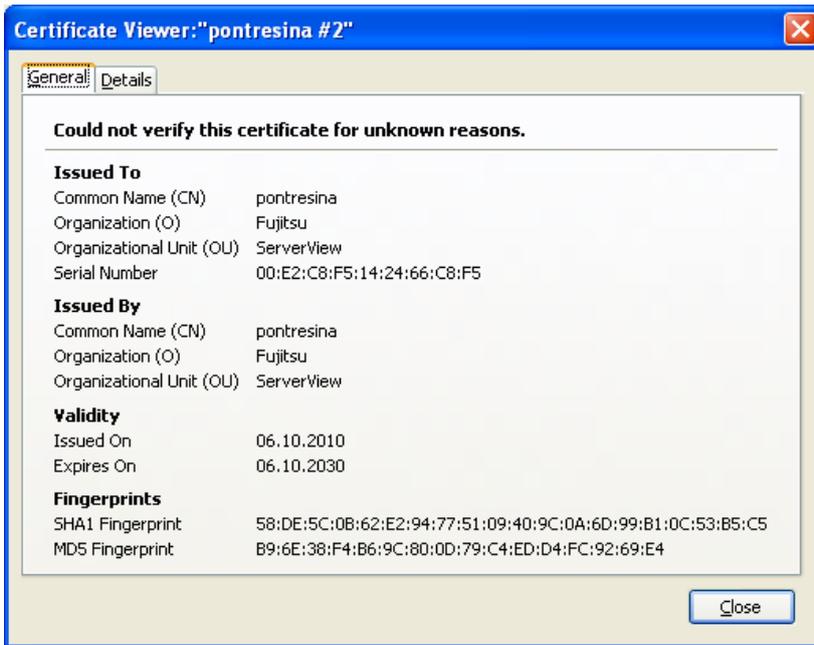
3.7.3. Certificate management

Web-based communication within the Operations Manager is secured by SSL connections. In former versions the Operations Manager provided secured access by connections secured by the Secure Socket Layer (SSL) as an option. With version 5.00 or higher this has become mandatory for security reasons, i.e., the Operations Manager can only be accessed using SSL-secured connections. The reason is that user passwords are sent as clear text across the connections, and these credentials should not be visible even within a firewall-protected Intranet.

In order to establish an SSL secured connection, a secret key for encryption and decryption of the data has to be exchanged between the client and the server side. This takes place during the initiation of the connection by means of the SSL handshake protocol, where the server first exposes a certificate containing, among other things, the public part of its key pair. The private key is used by the server itself for this exchange, while the client uses the public key.

As pointed out in section 3.5, "SSL Certificate Management", you may want to import server certificates, or the certificate of your own CA, into the trust store of your browser. But you must be sure that the certificate presented by the web server is really the one that you expect it is. This is achieved by comparing the fingerprint of certificate with the one that you have gotten from the server certificate on the server (cf. section 3.5.2, "Certificate Fingerprints").

Every browser provides the possibility to display at least one of the fingerprints of certificate, as for instance Mozilla Firefox or Microsoft Internet Explorer:



Most browsers provide the server certificate details by right-clicking on the page and then choosing the properties of page. Among the properties, you will easily find the certificate information.

Recommendation 10

Unless you are totally sure that you are connected with the desired Central Management Station (CMS), you should meticulously check the fingerprint(s) of the server certificate of CMS.

You can avoid checking the same certificate repeatedly by "importing" or "installing" it into the "trust store" of browser. With Firefox this is easily done by checking the box **Permanently store this exception** while **adding the exception** in order to establish the **untrusted connection**. In case of Internet Explorer, you can do the same by clicking on the **Install Certificate ...** button in the **General** tab of the **Certificate** window (see above). But be carefully and always check the certificates fingerprint(s)! If you nevertheless erroneously imported an unwanted certificate, you should remove it from the trust store of browser using the Certificate Manager of the browser.

When using Firefox, you find the Certificate Manager by choosing **Tools** -> **Options** in the main menu, and among the options the **Encryption** tab in the **Advanced Window**. There you start the Certificate Manager by clicking on the button **View Certificates**.

Recommendation 11

Frequently check the imported certificates in your trust store of browser. Keep the store as small as possible – remove entries for servers and certificate authorities when they are no longer needed.

As already pointed out in section 3.5.1, " ServerView Certificates", you can avoid importing certificates if you install a certificate on the CMS which is signed by a CA trusted by the browser.

3.8. Secure Boot

The latest PRIMERGY Servers are being released with uEFI boot mode as standard. This allows user to select secure boot, which automatically makes for a more secure system. The following points should be noted:

- Boot can only succeed with signed drivers only
- only available in uEFI (not legacy) mode
- BIOS must be signed
- drivers for Adaptor cards must be signed
- Older Operating Systems do not support it.

4. Configuration, installation and deployment of PRIMERGY servers

For configuration, installation and deployment of PRIMERGY servers the following tools are available:

- Installation Manager for local or remote installation
- ServerView RAID Manager for administrating different RAID controllers with the same Web-based user interface
- Multi-Deployment Platform (MDP) provides a service platform from which actions can be initiated to support a locally or remotely driven deployment process on target servers.

The Bootable Update DVD enables the firmware for various server components and the server BIOS to be updated locally on the managed server before installing the operating system.

For more information, please refer to section 8.1

The purpose of the Download Manager is – as already mentioned – to keep the update repository on the management station up-to-date. If configured accordingly, it checks the FTS Web server frequently for new update packages and downloads them into the update repository on the Central Management Server (CMS).

Some of the files, which are downloaded from the offering Web site, are not signed for technical reasons. Since version 5.0, the secure HTTPS protocol is supported to avoid manipulation of those files while being downloaded.

Some of the files which are downloaded will have an associated signature file, these will be validated by the receiving program. E.g. when UMEiRMC.tar is downloaded it comes with a signature file which is encrypted to prevent alteration and the UMEiRMC.tar can then be validated by the iRMC before use.

Recommendation 12

For Download Manager function, please choose the HTTPS protocol if possible.

4.1. RAID Manager

ServerView RAID Manager can be used for configuring and administrating different RAID controllers with the same Web-based user interface. ServerView RAID Manager can be started locally or remotely. Every communication runs via HTTPS and the SV-registered port 3173, i.e. it is encrypted by means of TLS / SSL.

Before working with ServerView RAID Manager, the administrator must enter an account and a password.

It is highly recommended not to change manually the configuration from the SSL-secured to an unsecure HTTP connection, because in this case, the account and the password would travel as clear text over the line.

The security settings for RAID Manager network connection can be configured in file amDPatch.ini.

The file is located in the RAID Manager bin directory e.g.:

```
Windows:    C:\Program Files\Fujitsu\ServerView Suite\RAID Manager\bin\amDPatch.ini
Linux:      /opt/fujitsu/ServerViewSuite/RAIDManager/bin/amDPatch.ini
```

The recommended default SSL Security Options are to use at minimum TLSv1.1.

To enable custom security selection you have to adapt the value in line ClientSecurity

ClientSecurity = 4 (enable custom security selection)

The protocols which will be not allowed are listed in line SSLSecurityOptions

```
SSLSecurityOptions = SSL_OP_ALL:!SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS:SSL_OP_NO_SSLv2:SSL_OP_NO_
SSLv3:SSL_OP_NO_TLSV1
```

Optional defines:

```
SSL_OP_NO_SSLv2
SSL_OP_NO_SSLv3
SSL_OP_NO_TLSv1
SSL_OP_NO_TLSv1_2
SSL_OP_NO_TLSv1_1
```

E.g.: To disable TLSv1.1 you have to add :SSL_OP_NO_TLSv1_1 to this line.

```
SSLSecurityOptions = SSL_OP_ALL:!SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS:SSL_OP_NO_SSLv2:SSL_OP_NO_
SSLv3:SSL_OP_NO_TLSV1:SSL_OP_NO_TLSv1_1
```

To enable the changes you have to restart RAID Manager.

4.2. Remote Installation with the Installation Manager

Besides the local installation of PRIMERGY servers, the Installation Manager provides also remote installation. A remote Installation Manager installation consists of a local preparation phase followed by a remote installation as replication phase.

For the remote installation, a Deployment Server must be prepared.

During this preparation, the content tree of the Installation Manager DVD is copied to the hard disk of the Deployment Server as a network share. During the installation of the Installation Manager on the Deployment Server, the access to this network share can be protected by user name and password.

When a remote installation is initiated for a target system, the administrator must enter this name and password – otherwise the installation process on the target system cannot access the Installation Manager content. Unauthorized remote installations with Installation Manager are prevented by this mechanism.

The Installation Manager uses for Remote Installation another network share with the Installation Manager - OS (WinPE). This network share is accessed via TFTP with read-only access. If this is regarded to risky, it is recommended to use Installation Manager only in local mode.

Recommendation 13

Use an account in compliance with your security policy for protecting the network share with the Installation Manager content. This prevents from unauthorized remote installations with the Installation Manager. If the TFTP access to the OS share with read-only access is regarded to risky, it is recommended to use Installation Manager only in local mode.

The focus of the Installation Manager is the local or remote installation of a PRIMERGY server.

Basically, there are four phases, where security considerations are relevant:

- Installation of the components for using the Installation Manager
- Reference installation Session

Especially for deploying Blade servers, the Management Blade has an important role in the Installation Manager operation, please consider also Recommendation 4.

4.2.1. Installation of Deployment Components

There are two installation processes:

- The Web-based SV Installation Manager front end including the remote installation agent is usually installed on the same machine as the Operations Manager. This machine providing these components is called "CMS - Central Management Station".
- The platform containing the deployment services including PXE service, TFTP service and Installation Service is called "Deployment Server". This could be also a role of a CMS as well.

Remote Installation Agent

The Installation Agent uses the Fujitsu ServerView Application Service (Tomcat) and may be installed on the same machine as the SV Operations Manager. After successful installation, the Installation Manager graphical user interface (GUI) can be started. A Web browser is usually started on the same machine, i.e. in the standard case, the communication between the Web browser and the ServerView Application Service is local.

In this case you can increase the security, when you configure the Tomcat Application server in a way that it accepts only local HTTP requests.

However, if the Installation Manager is configured to use, the Web-based access is automatically secured by SSL.

Independent on the way the Installation Agent is accessed, a deployment session starts with a login-procedure. The authentication/authorization is based on the account (administrator account) that is specified during the installation of the Installation Service, because this service is contacted by the Installation Agent. Unauthorized access is not possible.

Recommendation 14

Authentication/authorization for a Deployment session is done by the Installation Engine on base of the user account that is defined at installation time of the Installation Service. If desired you can increase the security, by configuring the Tomcat Application server in a way that it accepts only local HTTP requests.

Installation Service

During the setup process of the Installation Service you specify the user account for accessing the Installation Server session. This account is used later for authentication/authorization when you start a deployment session with the Installation Engine.

4.2.2. Reference Installation with the Installation Manager

There are two ways for performing a reference installation, a local installation or a remote installation.

A local installation requires that the target server is connected to a CD-ROM and floppy disk drive via a USB interface. In addition, a monitor, keyboard and mouse must be connected to the blade server cabinet rear and routed to the desired server with an internal KVM switch. Although this hardware preparation is some effort, the local installation has two crucial advantages compared to the remote installation:

- The local installation offers the Guided Mode of Installation Manager, which automatically detects the target hardware configuration and takes this information into account during the complete installation process. This mode is the safest way to install a deployment blade error-free.
- There are no security issues, because the complete installation process runs locally.

Remote installation does not require the hardware preparation mentioned above, but you must install a deployment server from where you can perform the remote installation. This deployment server can be a PC or a notebook.

Remote installation is done in two steps: First you run the Installation Manager in preparation mode in order to generate a config file on the deployment server. In the second step, you prepare the PXE service/FTP service on the deployment server in a way that the deployment blade can boot and run the Installation Manager unattended mode with the previously generated config file from this PXE service.

Finally, you have to start the PXE boot on the target server.

There are two disadvantages:

- The preparation mode cannot detect the hardware configuration, because it does not run on the target hardware locally.
- The remote installation uses the DHCP and PXE services.

If there is only one DHCP and one PXE service in the LAN segment of the deployment blade, it can be taken as a secure configuration, because the target server will exactly contact these services only.

If there are other PXE services besides the one you have installed on the installation server, you should check the following:

- Are these PXE services passive, i.e. they react only on requests from configured MAC addresses?
- Are the PXE services trustworthy, i.e. their managed/scanned MAC addresses do not conflict with the MAC addresses of the PXE service on the deployment server?

If these conditions are not fulfilled, there is the risk that the target server is installed with other software as intended.

Recommendation 15

The most secure way is the local installation, which additionally provides the advantages of the guided mode, i.e. the automatic detection of the hardware configuration. If you use the remote installation, you should do the following checks:

- Is there another PXE service in the LAN segment besides the one installed on the deployment server?
- If yes; is this PXE service passive, i.e. it responds only on requests from configured MAC addresses, and is this PXE service trustworthy, i.e. its managed/scanned MAC addresses do not conflict with the MAC addresses of the PXE service on the deployment server?
- If there are two PXE services, none of them must be installed together with the DHCP service on one machine. Otherwise, only that PXE service is visible to the clients.

5. User Management

Beginning with Version 5 of the ServerView Operations Manager, a comprehensive user management has been introduced. This user management is always based on a directory service. When installing a ServerView product, the customer has the choice of using an existing one for that purpose, or built-in directory service of ServerView. The use of a directory service has several advantages:

- Real user identities – it is possible to use personal identities instead of unspecific local accounts.
- Central user rights management – the user authorizations are centrally defined.
- De-coupling of user and server management – a server administrator cannot change user rights unless he has the right to modify directory service data.

ServerView uses the directory service for both authentication and authorization of a user:

- Authentication defines a identify of user: "Who are you?"
- Authorization defines rights of user: "What are you allowed to do?"

5.1. Central Authentication Service and Single Sign On

The various ServerView products have their own Web Servers resp. Application Servers, which all have to individually determine a identify of user before allowing administrative access. This would require the user to repeatedly issuing his credentials whenever changing from one web page of product to the ones of another. Because such a behavior would be unacceptable, the so-called Single Sign On (SSO) feature was introduced with ServerView Operations Manager V5.00 or higher. SSO means that a user has to authenticate only once, and then gets access to any web-based ServerView interface without any further action. ServerView implements the SSO mechanism by means of a central authentication service (CAS), which processes the single sign-on procedure in a completely transparent manner from the point of view of user. The CAS stores the information about a identity of user in a secure cookie in the browser, which is deleted when the user explicitly signs off, or when he closes the browser. This means that an unattended browser session means a severe security gap.

Recommendation 16

Always sign off and close your browser if you have to let your PC unattended.

5.2. Unified Role-based access control (URBAC)

User management of the ServerView Suite is based on unified role-based access control (URBAC), which enables you to align your security concept with your structure of organization.

5.2.1. Users, user roles and privileges

RBAC controls the assignment of permissions to users by means of user roles instead of directly assigning the corresponding privileges to users:

- A set of privileges is assigned to each user role. Each set defines a specific, task-oriented permission profile for activities on the ServerView Suite.
- One or more roles are assigned to each user.

The concept of user roles offers important advantages, including:

- The individual permissions do not need to be assigned to each user or user group individually. Instead, they are assigned to the user role.
- It is only necessary to adapt the permissions of the user role if the permission structure changes.

5.2.2. User Role Assignments

Depending on the directory service used, several roles may be assigned to each user. In this case, the permissions for this user are defined by the sum of the permissions of all the assigned roles. There are three pre-defined user roles, namely Monitor, Operator and Administrator. The scope of permissions granted by the individual user roles increases from Monitor (lowest permission level) through Operator up to Administrator (highest permission level). Concerning the role-based permissions on accessing the Operations Manager, you can look up the table of the operations and the corresponding required roles in the document "User Management in ServerView" for assigning the appropriate role to a person.

Recommendation 17

Look up the table of the operations and the corresponding required roles ("Role-based permissions on accessing Operations Manager") in the document "User Management in ServerView" for assigning the appropriate role to a person.

Recommendation 18

Always assign the least privileged role that allows the required operations.

6. ServerView Agents and CIM providers on managed servers

This chapter discusses security issues with the several communication paths from the serverview management station to the agent node or managed server. The serverview management station may connect to several components running on the managed node which are in particular

- SNMP agents that run on top of the target OS on a PRIMERGY server, on a PRIMERGY server blade, or on a virtual servers (host and guest machines). SNMP agents, which run on a Remote Management Controller (iRMC) or on a Remote Management Board of a blade server, are regarded in the chapter 9" SNMP Agents for out-of-band management"
- CIM Providers using either the CIM XML or WS-MAN protocol stacks
- The SOAP based server view connector service

For managing a system by means of ServerView it is necessary to install the SNMP Service and the ServerView Agents on this system. The ServerView Agents get the management data from the system and transport them via SNMP to the requestor of this information, for example to the Operations Manager or the Event Manager.

The SNMP service must be installed on sides, the managed server and the manager (e.g., Operations Manager or Event Manager). In this chapter we only look at the managed server.

For the management of ESXi servers the server view CIM providers need to be installed on ESXi.

6.1. SNMP Service

SNMP is a widely used and accepted management protocol. SNMP v1 and SNMP v2c are not secure and do not provide encryption. Consider using SNMP v3 instead. Nevertheless, basic security can be achieved, if the SNMP Service is configured appropriately. Using the default settings should be avoided.

When you change the default settings on the managed node don't forget to also modify the settings at the manager site.

Recommendation 19

Modify the default settings of the SNMP service. For more information, see below.

The SNMP service parameters may vary from OS implementation to OS implementation. Details for the OS dependent installation and configuration are described in the manuals "ServerView – Installation under Windows" and "ServerView – Installation under Linux". If available, the following parameters should be set according to the following rules.

Community Strings for accepting SNMP requests: The community string is part of each SNMP request that is sent from the manager to the agent. It is the only authentication mechanism of SNMP and it is unencrypted. Lack of encryption may be a problem, but the default community string "public" is used by the majority of SNMP devices. Therefore, it should be changed according to rules as they are applied to passwords. If you change the default community on the agent site you must also modify the default setting of the community string at the manager site. On principle, you can use individual communities for each server or group of servers.

Community strings can be associated with rights, such as read-only, read-write etc. If you want to use the complete ServerView functionality you should use "read-write", but you can also restrict the agent functionality to "read-only" operations.

Note: Operations Manager supports only one community for SNMP requests. Therefore here you should not configure two different communities, such as "public" for read-only and "secret" for read-write.

Accept SNMP packets from selected servers/any server: Here you should explicitly define the IP addresses of the management application(s) and, if used, the Deployment Server. This prevents the agent from accepting SNMP requests from other servers other than the one(s) where the manager(s) are installed.

Note: In this case the IP address for the management application must not come via DHCP.

Trap destination: Here you should explicitly specify the IP addresses of those systems where management applications reside that should receive traps.

Note: The IP address for the management application must not come via DHCP.

Community String for Sending Traps: Here you specify the community string that is sent as part of an SNMP trap to the management application. The SNMP service at the management application side must be configured to accept traps with this community string.

Enable/Disable Set Requests: Some SNMP service implementations enable or disable the agent to perform SNMP set requests. Here again, if you want to use the complete ServerView functionality you should enable them. In this case you should also apply the "ServerView Security Concept for SNMP Set Operations"0. If you want to disable SNMP set operations for security reasons generally, you can configure the SNMP service correspondingly.

6.1.1. SNMP v3

SNMPv3 protocol is a security model, defining new concepts to replace the old community-based pseudo-authentication and provide communication privacy by means of encryption.

For privacy crypto algorithm as AES and DES and authorization with RSA-MD5 and des3-cbc-SH1 hash algorithm like Kerberos v5 are optional for SNMPv3 to ensure user privacy and user authorized access control. These are the attributes for the USM (User Security Model) and available in net-snmp package for the iRMC.

6.1.2. Communication between Agents on MMBs and CPU Blades

If a blade server is a managed system, you have the following situation: An SNMP agent runs on the Management Blade (MMB) and an SNMP agent runs on the server blades. ServerView managers communicate with both types of SNMP agents. On principle, one could configure different SNMP communities for the MMB agent and for the individual server blade agents. When the managers are configured correspondingly, the communication between the managers and the agents works without any problems.

If different server blades are assigned to different clients, you may have the requirement to use different communities for the server blades of different clients in order to avoid that one client gets information about the server blades of another client. In this case you have also to avoid, that a client gets information about the server blades of another client via the MMB

6.2. ServerView Agents

The only authentication mechanism of SNMP v1/SNMP v2c is the community string. It is transported as clear-text, because SNMP v1 does not support encryption. Therefore SNMP Set-operations may be regarded as risky. But ServerView provides a "ServerView Security Concept for SNMP Set Operations" additionally to the configuration of the SNMP services. This concept comprises three options for SNMP SET operations:

- Prohibit specific SET operations.
- Prohibit all SET operations.
- Protect SET operations with a user authentication

The options can be configured as described in the manuals "ServerView – Installation under Windows" and "ServerView – Installation under Linux".

Prohibiting SET operations with these options apply only to ServerView agents. SET operations for other SNMP agents are not affected.

The option "Protecting SET operations with a user authentication" works in the following way: When a ServerView agent is installed, a user group (local or domain) must be specified. Before the ServerView Manager sends an SNMP set operation to the managed node it asks the administrator to enter an account (name and password). The ServerView Manager asks the agent via SNMP for the account that has been specified with the installation of the agent. This information is weakly encrypted during the SNMP transport. The Server Manager only sends out the SNMP set request if the account received from the agent matches the account input by the administrator.

This user authentication only operates with ServerView managers. It does not work with other SNMP tools.

Recommendation 20

Specify a user group at the agent installation time which is used by the Operations Manager for authentication before sending SNMP SET requests to the agent.

For the Operations Manager since V5.0 most of the SET operations have been removed and the appropriate functions have been moved into the Server Configuration Manager, which has full RBAC protection (communication via ServerView Remote Connector Service, SSL encrypted). The remaining SET operations are protected by RBAC privileges (SET requests are only sent when the appropriate privileges are granted to the authenticated user).

6.3. Securing SNMP messages with IPSec

As mentioned above, SNMP v1 does not use encryption. This lack of security can be circumvented by configuring IPSec policies on all SNMP agents and managers. This prevents malicious users and attackers from intercepting SNMP messages.

But IPSec does not automatically encrypt the SNMP traffic. You must create filter specifications in the appropriate filter list for traffic between the SNMP managers and agents (see also Table "Communication Paths").

Recommendation 21

If it is necessary to circumvent the lack of encryption with SNMP v1, secure the SNMP messages with IPSec.

6.4. ServerView CIM Providers

6.4.1. ServerView ESXi CIM Providers

VMware ESXi does not have a console OS and furthermore SNMP is not supported. Therefore the ServerView Agents for Linux can not be used.

The monitoring of a VMware ESXi system is only possible according to the Common Information Model (CIM) defined by the Distributed Management Task Force (DMTF). CIM-XML is used for the data exchange between the managed server and the management station.

ServerView ESXi CIM Providers are supplied on the ESXi Installable and ESXi Embedded image from FTS. An Offline Bundle (Offline Bundle which includes VIB file – vSphere Installation Bundle file) is also available online on the support pages of the FTS Internet portal.

The ServerView ESXi CIM Providers are installed and usable after the VMware ESXi installation with ESXi Installable and ESXi Embedded image. Furthermore a already installed VMware ESXi system can be updated after the download of the Offline Bundle from the support pages of the FTS Internet portal with the following VMware commands

```
esxupdate (local)
```

```
vihostupdate (remote)
```

Both commands are described in detail in the VMware documentation.

ServerView ESXi RAID Core provider is also available in the ESXi Embedded image from FTS. Installation and update by Offline Bundle as described above will also be possible.

A description how to get the monitoring information in SV Operations Manager from the ESXi system is found in section 2.8.8, "Support for VMware ESX Server and VMware vSphere Hypervisor (ESXi)", of the "ServerView Operations Manager - Server Management" manual. This manual can be downloaded from the [Manuals Download Page](#).

The VMware document "ESXi Configuration Guide (available at: <https://docs.vmware.com/jp/VMware-vSphere/7.0/vsphere-esxi-701-installation-setup-guide.pdf>) contains a chapter "Security" with additional helpful information.

6.4.2. ServerView CIM Provider for Windows

ServerView CIM Providers are supplied as part of the "ServerView Agent & CIM Providers for Windows (x64)" package. For local access to the CIM classes WMI from Microsoft can be used, remote access can be done through Microsoft WSMAN.

The client who wants to access the CIM Providers must be administrator or belong to the user group created during the installation of the ServerView agents.

6.4.3. ServerView CIM Provider for Linux

To run the CIM Providers a CIMOM (CIM Object Manager) service must be available. Supported CIMOMs are SFCB and OpenPegasus. The CIM Providers can only be accessed as the "root" user on the server.

6.5. ServerView Connector Service

Shortened as SCS and sometimes called ServerView Remote Connector Service.

This is a TCP/IP web service with one port number (3172) for SSL and non-SSL calls where multiple Agent-Provider-Libraries can be addressed. This is a generic service based on a patent owned by FUJITSU LIMITED.

Interface is SOAP (and CGI-Like calls for diagnostic calls) and REST. In SCS are different security topics centralized. The called Agent-Provider-Libraries can decide for which operation which security recommendations are to be used.

Available is

- No security – all can read and work
- Simple authentications (userid/passwords/..) (Internal encryptions of authentication data)
- HTTP authentications, HTTP Digest authentication (... with corresponding encryptions)
- SSL Standard Usage (Standard SSL encryptions)
- WS-Security parts and using WS-Security-Interceptor technique to validate tokens (e.g. RBAC/SSO) (for RBAC combined with SSL encryption)
- If the callers sends SSL-Certificates then this certificates will be verified and checked for Certificate-Based-Access-Control.

For the last two points it is necessary to have the CA-certificates and corresponding configuration files of the to-be-trusted Management Stations In the Trust-Store of SCS (a copy of these files in the pki directory).

To do this see description in "User Management in ServerView" manual and subchapter "Preparing managed nodes for RBAC and client".

The administrator of the Managed Node decides whom this Managed Node trusts !

6.6. ServerView System Montor

ServerView System Monitor is an HTML5 based web application. The application establishes an HTTPS connection to the ServerView Remote Connector installed on the managed node.

The Remote Connector client access might be restricted to administrator users only or to members of a user group specified in the Agents Configuration or during the installation of the ServerView Agents.

7. Administration (Operations Manager)

7.1. SNMP Service

Analogously to the configuration of SNMP services on managed nodes, two configurations are necessary on the Central Management Server:

- Before the Operations Manager, the Event Manager or Win32-based ServerView is installed on the Central Management Server, the SNMP Service must be installed and configured for receiving SNMP traps from the agents. This configuration must correspond to the configuration of the SNMP services on the managed nodes (See Recommendation 19: "Trap Destination" and "Community String for sending traps").
- After the installation on the Central Management Server, you must configure the SNMP service for each managed server or group of managed servers: The community string that is to be used when the Central Management Server sends an SNMP request to the agent of the managed server. This must be done corresponding to the action of Recommendation 19, "Community String for accepting SNMP requests".

The ServerView Agents and the Central Management Server communicates via SNMP. As SNMP does not provide neither encryption nor secure authentication, it is highly recommended to install both the ServerView managers and the ServerView agents behind a firewall. SNMP should not cross the firewall.

Recommendation 22

Install both, the Central Management Server and the ServerView agents on the managed servers behind a firewall which protects the SNMP communication.

7.2. Installation of the Web Server for the Operations Manager

The big advantage of the Operations Manager is that it can run behind the firewall in the Intranet, but nevertheless you can access this management tool via any Web browser in the Internet - anytime and anywhere.

However, from security point of view, any installation of an application server may generate security holes in an existing configuration. The reason is threefold::

- The application server itself may contain undetected security flaws.
- The application SW running on the web server can have security holes.
- If the directories into which the application server is installed are not secured enough against write access, then a non-administrative user on the CMS could cause harmful behavior of the application server or the applications.

You as a customer can of course do nothing against such errors, which slipped through a thorough development and quality assurance process. But you can minimize the consequences of such errors, if you follow some rules.

First of all you should restrict the access rights of the web server and its application SW on the CMS as far as possible. For that purpose it is recommended that you create a user account with minimal access rights for running the Application Server (TomEE).

You specify this account during installation of the Operations Manager, when you are asked for the account the Application Server shall run as. It is strongly recommended that you create a non-administrative account for this purpose whose data cannot be accessed by any other account.

Recommendation 23

Create a non-administrative account dedicated for the Application Server that is installed with ServerView Operations Manager. Ensure that this security settings of account prevent all non-administrative users from reading or writing the account directories and files of Application Server.

7.3. Exchanging SSL certificates for the Operations Manager

Exchanging SSL certificates is described in section 4.2.4, "Replacing the certificate on the Central Management Station", of the "User Management in ServerView" manual. This manual can be downloaded from the [Manuals Download Page](#).

7.4. Restricting the TLS/SSL Cipher Suites for the Operations Manager

A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) network protocol. The structure and use of the cipher suite concept is defined in the documents that define the protocol ([RFC 5246](#) standard for TLS version 1.2). A reference for named cipher suites is provided in [RFC 2434](#), the TLS Cipher Suite Registry.

When a TLS connection is established, a handshaking, known as the TLS Handshake Protocol, occurs. Within this handshake, a client hello (ClientHello) and a server hello (ServerHello) message are passed. ([RFC 5246](#), p. 37) First, the client sends a cipher suite list, a list of the cipher suites that it supports, in order of preference. Then the server replies with the cipher suite that it has selected from the client cipher suite list. ([RFC 5246](#), p. 40) In order to test which TLS ciphers that a server supports an SSL/TLS Scanner may be used." (From: Wikipedia, the free encyclopedia.)

As there are weaker and stronger cryptographic algorithms, there are weaker and stronger cipher suites. Checking the strength of the TLS/SSL cipher suites offered by a web server is therefore part of the task of so-called "vulnerability scanners". Vulnerability scanners are tools being used to assess computers, computer systems, networks or applications for weaknesses. Normally a software vendor will always strive for making his products as strong as possible regarding security, that is, that all of his products will pass vulnerability scanning without errors. But applied to TLS/SSL cipher suites this could mean that a secure connection cannot be established because a client offers only cipher suites which are considered as weak by vulnerability scanners. Therefore some of the ServerView products don't restrict the use of cipher suites, but leave the decision about their application to the user.

The best SSL would be of course a configuration which allows only the latest SSL protocol version (namely TLSv1.2), and restricts the cipher suites to those which are considered as safe according to current standards. However, neither the SSL protocol version TLSv1.2 nor its direct predecessor TLSv1.1 cannot be presupposed for all of the systems which can be connected to the Operations Manager. Therefore the SSL default configuration of all current OM versions allows additionally TLSv1.0. However, this protocol is vulnerable against "BEAST" attacks when used with cipher suites of the "CBC" (Cipher Block Chaining) mode cipher suite. Unfortunately there is no alternative for the Java 7 based OM versions, because all of the cipher suites supported by Java 7 are either of the CBC mode type, or considered unsafe for other reasons, like the RC4 type cipher suites.

Consequently, no absolutely safe SSL configuration is possible when the Operations Manager is configured with TLSv1.0. But as BEAST attacks only allow retrieving of session cookies, but not decryption of the total data exchange, and further require a huge effort comprising a man-in-the-middle attack plus a specially modified client program, Fujitsu assesses the risk for this type of attacks much less than for "conventional" crypto attacks. A "relatively" safe configuration following this approach is described in the following, which is valid for Operations Manager versions >= 6.10. With these versions, you can restrict the cipher suites with the following configuration changes:

(A) Operations Manager versions <= 7.10:

- (1) Using a text editor, open the file

<ServerView Suite>\jboss\standalone\configuration\standalone.xml.orig on Windows, resp. /opt/fujitsu/ServerViewSuite/jboss/standalone/configuration/standalone.xml.sav on Linux. Look up the XML section <subsystem xmlns="urn:jboss:domain:web:1.1" ...>, and add there the attribute cipher-suite to the XML tag <ssl ...> like in this example:

```
<subsystem xmlns="urn:jboss:domain:web:1.1" default-virtual-server="default-host" native="false">
  <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http"/>
  <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
    <ssl name="https" password="changeit" certificate-key-file=".. /standalone/svconf/pki/keystore" cipher-suite="TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_EMPTY_RENEGOTIATION_INFO_SCSV" protocol="SSLv2" verify-client="false"/>
  </connector>
  <virtual-server name="default-host" enable-welcome-root="false"/>
</subsystem>
```

Please note that protocol=SSLv2 does not really specify SSL version 2, but the combination TLSv1.0 + TLSv1.1 + TLSv1.2.

It is a good idea to also try protocol=TLSv1, which effectively enables only the combination TLSv1.1 + TLSv1.2. If you do not experience connection problems with this configuration, you should keep it, because it is absolutely safe even against BEAST attacks.

- (2) Using a text editor, open the file <ServerView Suite>\opends\config\schema\02-config.ldif on Windows, resp. /opt/fujitsu/ServerViewSuite/opends/config/schema/02-config.ldif on Linux.

Change the objectclasses declaration ds-cfg-administration-connector so that the MAY line looks like this:

```
MAY ( ds-cfg-listen-address $ ds-cfg-ssl-cipher-suite $ ds-cfg-ssl-protocol )
```

- (3) In case of Operations Manager versions <= 7.10, you have additionally to change the configuration of the ServerView directory service (OpenDJ).

Using a text editor, open the file <ServerView Suite>\opends\config\config.ldif on Windows, resp. /opt/fujitsu/ServerViewSuite/opends/config/config.ldif on Linux.

For any cipher suite to be used, add the attributes ds-cfg-ssl-cipher-suite and ds-cfg-ssl-protocol to the entry cn=LDAPS Connection Handler, cn=Connection Handlers, cn=config like in this example:

```
dn: cn=LDAPS Connection Handler,cn=Connection Handlers,cn=config
objectClass: ds-cfg-ldap-connection-handler
...
ds-cfg-use-ssl: true
ds-cfg-ssl-cipher-suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ds-cfg-ssl-cipher-suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
ds-cfg-ssl-cipher-suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV
ds-cfg-ssl-protocol: TLSv1
ds-cfg-use-tcp-keep-alive: true
```

In the same configuration file, change the attribute ds-cfg-listen-address of the entry

dn: cn=Administration Connector,cn=config from 0.0.0.0 to 127.0.0.1:

```
dn: cn=Administration Connector,cn=config
objectClass: ds-cfg-administration-connector
objectClass: top
ds-cfg-listen-address: 127.0.0.1
ds-cfg-listen-port: 4444
cn: Administration Connector
ds-cfg-key-manager-provider: cn=Administration,cn=Key Manager Providers,cn=config
ds-cfg-ssl-cert-nickname: svs_cms
ds-cfg-trust-manager-provider: cn=Administration,cn=Trust Manager Providers,cn=config
```

In case of Operations Manager version 7.10, the ServerView directory service has changed to ApacheDS. Unfortunately there is no possibility to change the SSL configuration of this directory service by configuration.

- (4) On Windows restart the service "ServerView JBoss Application Server 7", either via the control panel, or by this command lines:

```
%WINDIR%\system32\net.exe stop "SVJBASSVC"
%WINDIR%\system32\net.exe start "SVJBASSVC"
```

On Linux restart the ServerView JBoss daemon by this command line:

```
/etc/init.d/sv_jboss restart
```

(B) Operations Manager versions > 7.10:

- (1) Using a text editor, open the file <ServerView Suite>\tomEE\conf\server.xml on Windows, resp. /opt/fujitsu/ServerViewSuite/tomEE/conf/server.xml on Linux. Look up the XML section <Connector port="3170" ...>, and add there the attribute ciphers, like in this example:

```
<Connector port="3170" protocol="org.apache.coyote.http11.Http11NioProtocol"
    maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false"
    sslEnabledProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
    ciphers="TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_EMPTY_RENEGOTIATION_INFO_SCSV"
    keystoreFile="svconf/pki/keystore" keystorePass="changeit"
    truststoreFile="svconf/pki/cacerts" />
```

It is a good idea to also try sslEnabledProtocols="SSLv2Hello,TLSv1.1,TLSv1.2", which enables only the combination TLSv1.1 + TLSv1.2. If you do not experience connection problems with this configuration, you should keep it, because it is absolutely safe even against BEAST attacks.

- (2) In case of Operations Manager version 7.11, the ServerView directory service has changed to ApacheDS. Unfortunately there is no possibility to change the SSL configuration of this directory service by configuration.

In case of Operations Manager versions >= 7.20, the ServerView directory service automatically adopts the configuration of TomEE.

- (3) On Windows restart the service "ServerView ApplicationService", either via the control panel, or by this command lines:

```
%WINDIR%\system32\net.exe stop "SVTomEE"  
%WINDIR%\system32\net.exe start "SVTomEE"
```

On Linux restart the ServerView ApplicationService daemon by this command line:

```
/etc/init.d/sv_jboss restart
```

7.4.1. Cipher suite configuration resisting BEAST attacks

As already said above, there is currently no safe cipher suite available under Java 7 that is safe against BEAST attacks when being used with the SSL protocol version TLSv1.0. (The only BEAST-safe cipher suites are `SSL_RSA_WITH_RC4_128_MD5` and `SSL_RSA_WITH_RC4_128_SHA`, but these are considered unsafe nowadays because they are based on RC4.) Because all of the "good" cipher suites offered by Java 7 are of the CBC mode type, you have to configure at least protocol version TLSv1.1, and exclude TLSv1.0 from the configuration.

7.4.2. Security settings for Operations Manager versions >= 8.00

Operations Manager starting from version 8.00 uses different than in previous versions technology to provide user interface on client station. The new front-end has a form of WebStart (Oracle Technology to run Java applets without web browser) application and thus web browser is only used to download .jnlp file which is a start point to Webstart application. As a consequence of the new technology being introduced only Java 8 is supported by those Operations Manager versions.

As Java 8 brings support for many more cipher sets, to keep configuration simple there is a security level selection dialog presented during Operations Manager installation. With this dialog an administrator can easily adapt security settings to his or her needs choosing one of three predefined levels. While "Modern" level provides best protection out of the box, the other two levels are designed to provide compatibility with legacy applications and should be used only when - due to particular business case - it is absolutely necessary to use some outdated components of Server View Suite which does not support latest security standards.

In rare cases when "Modern" level is not secure enough one can manually disable support for protocols other than TLSv1.2. In such case the accompanying software (like SV Agents) has also be adopted to use TLSv1.2. Please also note that there are known issues with some versions of Microsoft ODBC driver on Windows which has to be handled by the system administrator. (In such case update to latest version is required or – as a workaround – turning on FIPS compatibility mode. Please reach the following link for further information: <https://dba.stackexchange.com/questions/93127/sql-server-service-won-t-start-after-disabling-tls-1-0-and-ssl-3-0>)

To run pure TLSv1.2 configuration:

1. Select **Modern** security settings during installation.
2. After installation using text editor modify file `<install_dir>/tomee/conf/server.xml`:
 - 2.1. Find a line starting with `<Connector port="3170" /`.
 - 2.2. In attribute `sslEnabledProtocols=` remove everything but `TLSv1.2`.
 - 2.3. Save changes.
3. Using text editor modify file: `<install_dir>/apacheds/instances/default/conf/ou=config/ads-directoryserviceid=default/ou=servers/ads-serverid=ldapserver/ou=transport/ads-transportid=ldaps.ldif`:
 - 3.1. Remove all lines starting with `ads-enabledProtocols:` referring to protocols other than TLSv1.2.
 - 3.2. Save changes.
4. Restart Operations Manager services (or whole server if possible). From this point the whole Operations Manager should use only TLSv1.2 for communication.

Recommendation 24

Whenever possible stick to **Modern** security level during install/upgrade of Operations Manager. Do not apply manual changes described above unless absolutely necessary.

7.4.3. Security settings for Operations Manager versions >= 9.00

Operations Manager starting from version 9.00 uses different than in previous versions technology to provide user interface on client station. The new interface is in form of native HTML5 web application. Application Server runs on Java 8 LTS binaries provided by AdoptOpenJDK which are included in Operations Manager package.

Since version 8 of Operations Manager, security and cipher settings are managed during installation / upgrade procedure. There are three security levels:

- Modern (TLSv1.2)
- Intermediate (TLSv1.2, TLSv1.1, TLSv1.0)
- Old (TLSv1.2, TLSv1.1, TLSv1.0, and SSLv3)

To change the security settings after installation, run Change installation of FUJITSU Software ServerView Application Server (in "Programs and Features" utility on Windows) or run

`<install_dir>/svom/ServerView/Tools/ChangeComputerDetails.sh` script on Linux and select appropriate security settings.

7.5. Set Operations with User Authentication

If you have activated password authentication during the installation of the agents on the managed servers in order to protect SET operations with a user authentication (Recommendation 23), there may be a prompt for entering username and password and you have to enter the account data of a user account belonging to the specified ServerView user group or administrators group (depending on agents configuration).

7.6. Event Manager and Antivirus Programs

The Event Manager can be configured in a way that it informs administrators about events by means of e-mails. When an antivirus program runs on the Central Management Station, where the Alarm Service is installed, this antivirus program may prevent that the Alarm Service sends out emails. In order to allow the Alarm Service sending out e-mails, the antivirus program configuration must allow the following processes to send e-mails:

- Windows: `blat.exe` (SVOM before 7.11), `mail.exe` (SVOM including 7.11 and later)
- Linux, Solaris: `smtpm`

7.7. Changeable SNMP Ports

In order to use not the default ports 161 and 162 the following changes must be made:

ServerView Agent Linux on the managed node

ServerView Operations Manager Linux on the CMS

Regardless of SuSE (SLES) or Red Hat (RHEL), the following changes have to be made:

1. In file `/etc/services`, change entries:

- for `snmp` from 161 to `<new port 1>` (both protocol tcp and udp)
- for `snmptrap` from 162 to `<new port 2>` (both protocol tcp and udp, if present)

2. In file `/etc/snmp/snmpd.conf`:

- specify new port `<new port 1>` used by `snmp` for protocol udp.
- If IPv6 is used, also specify new port for protocol udp6:

```
agentAddress udp:<new port 1> [,udp6:<new port 1>]
```

3. Additional in file `/etc/snmp/snmpd.conf`:

- specify trap destinations with different port by adding port number to address:
- ```
trapsink machine:<new port 2> <community>
```

4. In file `/etc/snmp/snmptrapd.conf`:

- specify new port `<new port 2>` used by `snmptrapd` for protocol udp:
- ```
snmpTrapdAddr udp:<new port 2>
```

5. In file `/var/net-snmp/snmp.conf`

- specify default port used by `snmp`:
- ```
defaultPort <new port 1>
```

#### 6. Restart Services (or reboot OS)

- [/sbin/] service snmpd restart
- [/usr/bin/] sv\_services restart
- [/usr/sbin/] srvmagt restart

If any of these files is missing, create it with user "root" and permission 0644.

Check that directory /var/net-snmp has permission 0755 (on some OS, it has no permission for "group" and "other" – that will not work!)

Do not get confused by other directories (e.g., /var/lib/net-snmp) or filenames looking similar (snmp.conf/snmpd.conf).

### ServerView Agent Windows on the managed node

#### 1. In file <WINDOWS DIR>\System32\drivers\etc\services, change the entries:

- for snmp from 161 to <new port 1> (for protocol udp)
- for snmptrap from 162 to <new port 2> (for protocol udp)

#### 2. Restart Services for Agents and SNMP

- Restart ServerView Agents with Agents Tool **Restart Agents** under **Start -> All Programs -> Fujitsu -> ServerView Suite -> Agents -> Diagnostic Tools -> Restart Agents**

### ServerView Operations Manager Windows on the CMS

#### 1. Before below changes stop services in the following order

- ServerView Download Service
- ServerView Services
- SNMP Services

#### 2. In file <WINDOWS DIR>\system32\drivers\etc\services, change the entries

- for snmp from 161 to <new port 1> (for protocol udp)
- for snmptrap from 162 to <new port 2> (for protocol udp)

#### 3. In file C:\usr\snmp\persist\snmp.0.conf (if this file does not exist, create it), add the line

- defaultPort <NewPort-1>

#### 4. Restart Services in following order

- SNMP Services
- ServerView Services
- ServerView Download Service

## 8. Maintenance

For maintenance purposes, powerful tools like Update Management products and PrimeUp are offered to reduce efforts of administrator.

### 8.1. Update Management

The Update Management of the PRIMERGY ServerView Suite offers the administrator a convenient option for updating firmware or software of the components of the servers. The following tools are available for this task:

- **Update Manager (integrated in the Operations Manager)**  
The Update Manager allows reliable, network-wide updating of BIOS, firmware, drivers, and various server management products via a graphical user interface (GUI) or an command line interface (CLI). You can automatically update multiple servers simultaneously and scheduled, controlled via the management server. The Update Manager uses so-called update packages which are located on the central management server. This directory can be built initially either
  - by importing from the most recent ServerView Update DVD, or
  - via the Internet by using the integrated tool "Download Manager"In any case, the repository can be kept up-to-date by using the Download Manager regularly.
- **Update Manager Express and ASPs (Autonomous Support packages)**  
These products are developed to install and update BIOS and firmware of the various server components locally. ASPs are supplied with a signature file thereby ensuring their integrity.
- **Update Function in System Monitor**  
The Update Function in System Monitor allows also a reliable updating of BIOS, firmware and drivers, via the graphical user interface (GUI) of the System Monitor.  
The System Monitor operates autonomously on the server, without needed integration into the domain of the Operation Manager.  
The update packages may be provided by different ways:
  - ServerView Update DVD
  - Download from Web via FTS support side
  - Download from Repository Server, installed in the customer networkThe System Monitor is ingredient of the SV\_Agent package.
- **PrimeUp and PRIMERGY Support Packages (PSPs)**  
PrimeUp supports unattended updating of driver software and ServerView agents based on PSPs locally on the managed servers
- **Update Function in iRMC S4 / S5**  
In the eLCM package of the iRMC S4 / S5 are the functions for Online Update and Offline Update integrated. These functions can be configured and started via the iRMC WebUI or via a REST scripting API.  
To use the eLCM package, an SD card on the servers main board and also a valid eLCM license have to be installed.

Online Update includes all functions to allow a reliable updating of BIOS, firmware and drivers. A running SV\_Agent on the server is not needed, only the SVAS (Agentless package) has to be installed on the server.

The update packages may be provided by different ways:

- Download from Web via FTS support side
- Download from Repository Server, installed in the customer network

Offline Update includes all functions to allow a reliable updating of BIOS, firmware. A running SV\_Agent or SVAS (Agentless package) on the server is not needed, therefore, it is particularly well suited for ESXI installations.

The update packages may be provided by different ways:

- Download from Web via FTS support side
- Download from Repository Server, installed in the customer network

Updating firmware, BIOS and drivers is an operation which should be protected, because unauthorized updating can damage your servers significantly. Plus, in most cases, the system is rebooted after successful updating – which might cause unexpected system downtime!

While the local update mechanisms like Update Manager Express and PrimeUp request administrator privileges implicitly, a centralized service must take more care about this requirement - without reducing convenience of user!

Therefore, the Update Manager provides various security mechanisms for authentication. While former versions (< 5.0) use a user/password based mechanism, starting with version 5.0 the recommended procedure is to use a certificate-based authentication for "Single Sign-On" access.

#### Recommendation 25

When installing the Update Agent the first time, please create a user group and users on the managed server in advance. During installing the Update agent, select "Account Check" in the Security Settings screen, and use the just created group as "User Group for Update". After installation, distribute the CMS-specific certificate with the related Update Manager function or other means.

This guarantees that only those GUI users will have administrator access rights, who are part of the related LDAP configuration. If the certification process fails for any reason, the agent switches to user/password mode automatically; this keeps the managed node in a manageable, but still protected mode.

The purpose of the Download Manager is – as already mentioned – to keep the update repository on the management station up-to-date. If configured accordingly, it checks the FTS Web server frequently for new update packages and downloads them into the update repository on the Central Management Server (CMS).

Some of the files, which are downloaded from the offering Web site, are not signed for technical reasons. Since version 5.0, the secure HTTPS protocol is supported to avoid manipulation of those files while being downloaded.

#### Recommendation 26

For Download Manager function, please choose the HTTPS protocol if possible.

#### Recommendation 27

For updates of BIOS/iRMC for systems with operating system VMWare ESXi, MMBs and connections blades please configure Plink in Configuration Manager. Plink has two main uses in this context:

1. Confirming that the managed node is in maintenance mode
2. Updating of connection blade FW

## 8.2. PrimeCollect

PrimeCollect is a tool to collect information about the inventory, the operating system, sensor data (e.g. temperature values), different logs (e.g. System Event Log) and other support relevant data. The kind and amount of the collected data depends on the system configuration. All information is automatically added to a .zip respectively .tar file which can be sent to a service engineer. So, PrimeCollect enables the support engineer to analyze customer problems and speed up the time for a solution/workaround.

For security reasons you may want to know which information is sent to the service engineer in this archive. The "PrimeCollect" manual contains a table that lists possible files along with their contents that are contained in the archive. Depending on your security policy you can delete certain file in the archive before sending it or you may decide not to send the archive at all.

#### Recommendation 28

Before you send out the .zip archive with the information collected by PrimeCollect, you can check and – if required by your security policy – remove information from this archive. The "PrimeCollect" manual contains a table that lists this information.

#### Recommendation 29

For handling of CA-certificates and corresponding configuration files, see chapter "6.5 ServerView Connector Service".

## 8.3. Repository Server

A Repository Server allows you to maintain a repository of firmware components in a decentralized way. The (virtual) machine, which is installed using the Repository Server software product, serves as a proxy server for those monitored managed nodes which do not have a connection to the internet. The download process using the Repository Server is completely independent from the update of the managed nodes. Administrators may receive email messages about the download progress and error situations.

The managed nodes connect to the Repository Server to receive the necessary updates for their firmware components. The Repository Server can also be used to provide the repository for the FTS update management tools, e.g. eLCM, System Monitor or Update Manager.

## 9. SNMP Agents for out-of-band management

Chapter 6 "ServerView Agents and CIM providers on managed servers" has discussed the security issues with SNMP agents on managed servers, i.e. in the context of in-band management. In-band management means that the target server hardware and the target OS are required for accessing the management information. Additionally a piece of software, e.g. an SNMP agent, must be installed on top of the target OS.

Out-of-band management does not require a running target OS for accessing the management information on the managed server. Two cases are possible:

- The managed server hardware is running a special diagnostic OS.
- A completely independent hardware component is used for accessing the management information on a managed server, for example the Management Blade of a blade server.

This chapter discusses security issues with SNMP on such special management devices.

SNMP must be available on both sides, the special management devices and the Remote Management front-end. In this chapter we only look at the special management devices.

### 9.1. ...on iRMC

The integrated Remote Management Controller (iRMC) does support SNMP Protocol and SNMP trap delivery.

As usual, you can configure SNMP communities that are associated with rights, and you can configure trap destinations. SNMP Communities, which are configured on iRMCs must also be configured in the server properties of ServerView/Operations Manager. The iRMC has its own event management. Whereas SNMP agents notify SNMP managers by sending SNMP traps, the alarm handler on the iRMC can be configured to notify administrators via pager, Mail or SNMP trap. Whereas SNMP traps are considered to be unreliable because they may get lost, the other guaranteed deliveries are considered to be sufficiently reliable.

Recommendation 30

In order to prevent loss of notifications about certain events, it is recommended that you configure the alarm handler of the iRMC or the Management Blade appropriately, i.e. notification not only via SNMP traps.

### 9.2. ...on the Management Blade

Initially, the Management Blade has no community string and is 'read-only'.

The following ports are used on the Management Blade for communication:

|             |           |                                  |
|-------------|-----------|----------------------------------|
| http:       | 80        | inbound to MMB (configurable)    |
| https:      | 443       | inbound to MMB(configurable)     |
| SSH:        | 22        | inbound to MMB (configurable)    |
| Telnet:     | 3172(/23) | inbound to MMB (configurable)    |
| SMTP:       | 25        | outbound from MMB (configurable) |
| SNMP:       | 161       | inbound to MMB (fixed)           |
| SNMP Traps: | 162       | outbound from MMB (fixed)        |
| LDAP:       | 636       | outbound from MMB (fixed)        |
| CAS:        |           | not implemented                  |
| RMCP:       | 623       | inbound to MMB (fixed)           |
| WS-Man:     | 8889      | inbound to MMB (fixed)           |

In case other ports are open this is an error.

If you plan to use SNMP on the Management Blade you should be aware of configuring SNMP v3, because this mode is not supported by all products of the ServerView suite.

The SNMP service of older Management Blades uses this community string for all operations, i.e. for both, get and set operations. Newer Management Blades provide different community permissions

The Management Blade supports also SNMP address filtering, i.e. you can configure IP addresses, which are the only ones that the Management Blade accepts as SNMP requestors. It is highly recommended to configure this filter according to the tables in Section 3.1 Communication Paths.

## 10. Special configurations

### 10.1. Options for managing servers in a Demilitarized Zone

A Demilitarized Zone (DMZ) is a network area that sits between an internal network of organization and an external network, usually the Internet. The DMZ is usually separated from both by firewalls that restrict the communication flows. The security policy for a DMZ is shaped by the requirement for a high-level security. Two options for managing servers in such an area are considered in the following:

For the first option, it is assumed that the firewall is closed for management protocols, especially for SNMP. That means that active management of the servers in the DMZ is not possible. Nevertheless, some management information can flow from managed servers in such an environment through the firewalls:

- **Fault information**  
When SNMP traps are blocked by the firewall, information about events could pass the firewall for example in one of the following ways: If you install the Event Manager together with the SNMP agents on a server in the DMZ, you can configure the Event Manager to send an email, when a certain event occurs. Similarly, management devices like iRMC or management blades can be configured to send emails instead of SNMP traps. Another alternative is, to send log files to the Central Management Server, because ServerView creates entries in these log files.
- **Asset Information**  
If ServerView agents and the Operations Manager are installed on a server in a DMZ, the Operations Manager can be configured via HTTPS to write periodically information in report or archive files. In this case, the information delivered by SNMP agents is written into files on the managed node, i.e. no SNMP communication runs over the wire or through the firewall, i.e. data are collected locally. Afterwards, these files can be transported through the firewall to the Central Management Server.

The second option assumes that a separate management network is available for the servers in the DMZ. In this case, the management traffic flows through this network, while the security policy for the production network guarantees the required security level. The servers in the DMZ are connected to the separate management network via dedicated network interface cards or via the management devices, like iRMC or management blade. A gateway system can provide VPN access from the Central Management Server in the intranet to the separate management network for the servers in the DMZ.

## 11. Summary

Security is not for free. If you simply install all PRIMERGY server management components with default values, it is highly likely that everything works. But on the other hand, you have the lowest level of security. When you configure all components individually, you achieve a pretty good level of security, but all only works properly if all components are consistently configured. That means, before configuring you should carefully plan the overall configuration. These detailed plans are the basis for the configuration and for ongoing maintenance.

Three different Administration Levels are distinguished for the PRIMERGY server management:

- Administration Level "Target OS up": The target operating system must be booted on the managed server. Agents must be installed on this operating system, and the management information travels on the same paths as the operational communication.
- Administration Level "Diagnostics up": The target operating system is not booted, but the system board is working properly. A diagnostic operating system or a pre-OS agent may be booted.
- Administration Level "Secondary Management Channel": This type of communication is completely independent of both the target operating system and the system board. Specific facilities are used for this type of management, such as the iRMC or, in case of blade servers, the Management Blade. This type of management is also known as "secondary management channel".

The subsequent table summarizes all previously discussed recommendations and categorizes their purpose, i.e. whether they are for keeping the overall security, or for achieving secured management operations, and for which administration level

For keeping the overall security  
For achieving secured management operations

| Event:<br>Recommendation                                                                                                                                                                                                                                                                                                        | Administration Level |             |                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-------------|-----------------------|
|                                                                                                                                                                                                                                                                                                                                 | Target OS up         | Diag. OS up | Second. Mgmt. Channel |
| <b>Installation PRIMERGY server management:</b><br>Locates all tools/components along with the managed servers behind a firewall.                                                                                                                                                                                               |                      |             |                       |
| <b>General:</b><br>Minimize the number of open ports for each system.                                                                                                                                                                                                                                                           |                      |             |                       |
| <b>Separate Management VLAN:</b><br>Separate management traffic from operational traffic                                                                                                                                                                                                                                        |                      |             |                       |
| <b>Non-administrative account for JBoss:</b><br>Create a non-administrative account dedicated for the JBoss application server that is installed with ServerView Operations Manager. Ensure that this security settings of account prevent all non-administrative users from reading the account directories and files of JBoss |                      |             |                       |
| <b>Role Assignment</b><br>Always assign the least privileged role that allows the required operations                                                                                                                                                                                                                           |                      |             |                       |
| <b>Separate Management LAN for management devices:</b><br>Connect the network interfaces of iRMC, etc. to a separate management LAN                                                                                                                                                                                             |                      |             |                       |
| <b>Remote Installation with Installation Manager:</b><br>Protect the network share for the Installation Manager content with a password. If the TFTP access to the OS share with read-only access is regarded to risky, it is recommended to use the Installation Manager only in local mode.                                   |                      |             |                       |
| <b>Installation of SNMP agents:</b><br>Modify the default settings of SNMP services. For mass settings you can use the MS System Policy Editor.                                                                                                                                                                                 |                      |             |                       |
| <b>Installation of SNMP agents:</b><br>Specify User Group for the ServerView authentication/authorization mechanism for set operations                                                                                                                                                                                          |                      |             |                       |
| <b>Installation of SNMP agents:</b><br>Secure SNMPv1 with IPSec – Follow Microsoft instructions                                                                                                                                                                                                                                 |                      |             |                       |
| <b>Central Management Server (CMS) and SNMP agents:</b><br>Install the CMS and the agents on the managed servers behind a firewall                                                                                                                                                                                              |                      |             |                       |
| <b>Installation of Web server for Operations Manager:</b><br>Secure the connection to the browser by SSL                                                                                                                                                                                                                        |                      |             |                       |
| <b>Actualisation of Update Files:</b><br>If the download via the Internet is regarded too risky, use the ServerView Update DVD                                                                                                                                                                                                  |                      |             |                       |
| <b>Update Manager Configuration:</b><br>Specify User Group for the Update Manager authentication/authorization mechanism and configure the Update agent correspondingly.                                                                                                                                                        |                      |             |                       |
| <b>Updating drivers, agents, BIOS, firmware:</b><br>If you prefer local tools, you can use the local Command Line Interface of the Update agent and the Update Manager Express                                                                                                                                                  |                      |             |                       |
| <b>Configure SNMP interface on the iRMC:</b><br>Configure communities for read-only.                                                                                                                                                                                                                                            |                      |             |                       |
| <b>Configure the Alarm Handler on the iRMC or Management Blade:</b><br>For reliable notification, configure not only SNMP traps.                                                                                                                                                                                                |                      |             |                       |
| <b>BMC Configuration:</b><br>Configure IP addresses and password.                                                                                                                                                                                                                                                               |                      |             |                       |
| <b>iRMC/Management Blade accounts:</b><br>Replace the default accounts by new accounts or change at least the password.                                                                                                                                                                                                         |                      |             |                       |
| <b>iRMC/Management Blade ports:</b><br>Disable port 80 for HTTP; use only SSL-secured connections via port 443 for HTTPS                                                                                                                                                                                                        |                      |             |                       |

## 12. Log Files

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation Manager | Once the installation is complete, the installation log file is saved back to the status directory on the deployment server that had been created for the current remote installation process. There it can be displayed via the Installation Manager interface                                                                                                                                                                                                                                                                            |
| Asset Manager        | Inspection of log files via GUI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| RAID Manager         | By default file events are written to a ServerView RAID log file.<br>By default all events show up in the logging facility of operating system. On Windows based systems entries can be found in <b>Start -&gt; Settings -&gt; Control Panel &gt; Administrative Tools -&gt; Event Viewer</b> (Application) and on Linux systems in /var/log/messages.                                                                                                                                                                                     |
| Download Manager     | You can display the log files via GUI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Update Manager       | You can display the log files via GUI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Virtual-IO Manager   | The Virtual-IO Manager always creates log files in the directory<br><ServerView_Suite>\plugins\viom\Manager\logs.<br>On a Windows based management station <ServerView_Suite> is typically the directory<br>C:\Program Files\Fujitsu\ServerView Suite<br>On a LINUX based management station <ServerView Suite> is typically the directory<br>/opt/Fujitsu/ServerViewSuite<br>In addition the Virtual-IO Manager always writes log entries containing all configuration changes and errors to system event log (Windows) or syslog (LINUX) |
| iRMC                 | Error messages are written to the specified log file. If no log file is specified, the output is directed to the flbmc.log file.                                                                                                                                                                                                                                                                                                                                                                                                           |

## 13. ServerView Default Certificates

Here the certificates are listed which are installed by default by the different ServerView products. All certificates share the same certificate signature algorithm and SSL version, namely SHA1withRSA and 3:

### 13.1. Management Controller/Management Blade

#### 13.1.1. Root CA

Owner: EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA, O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
 Issuer: EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA, O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
 Serial No.: 0  
 Issued On: Wed Apr 22 16:37:44 CEST 2009  
 Expires On: Sat Apr 20 16:37:44 CEST 2019  
 Fingerprints: MD5: 8E:B5:8D:B8:DE:7D:4C:2E:6A:5C:E2:A5:A6:12:19:E2  
 SHA1: FD:9B:B0:3E:23:60:73:2E:85:B5:F6:25:38:7F:CF:99:EB:BF:37:CC

#### 13.1.2. iRMC Default Certificate

Self-signed, auto-generated certificate which is generated at the first iRMC boot.

Subject: C=DE, ST=Bavaria, O=Fujitsu Technology Solutions GmbH, CN=iRMC/emailAddress=primergy-pm@ts.fujitsu.com  
 Issuer: C=DE, ST=Bavaria, O=Fujitsu Technology Solutions GmbH, CN=iRMC/emailAddress=primergy-pm@ts.fujitsu.com  
 Serial No.: Auto-generated  
 Issued On: Auto-generated  
 Expires On: Valid for 1825 days (5 years) since Issued On  
 Fingerprints: Auto-generated

#### 13.1.3. MMB Default Certificate

Owner: O=Fujitsu Technology Solutions, EMAILADDRESS=ServerView@ts.fujitsu.com, C=DE, ST=Bavaria, CN=PRIMERGY MMB 1024bit default RSA SSL Cert  
 Issuer: EMAILADDRESS=ServerView@ts.fujitsu.com, CN=ServerView Root CA, O=Fujitsu Technology Solutions GmbH, L=Munich, ST=Bavaria, C=DE  
 Serial No.: 54 (decimal)  
 Issued On: Mon Jun 15 16:50:10 CEST 2009  
 Expires On: Sat Jun 14 16:50:10 CEST 2014  
 Fingerprints: MD5: 40:78:F6:08:8D:3E:62:38:10:39:74:30:5F:06:7A:62  
 SHA1: 6D:E0:A2:35:F0:EA:17:75:32:1B:D8:89:3C:DA:6F:B5:EF:E4:26:1B

### 13.2. ServerView Connector Service (SCS)

#### 13.2.1. Root CA

Owner: CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE  
 Issuer: CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE  
 Serial No.: 0  
 Issued On: Thu Feb 26 14:17:15 CET 2009  
 Expires On: Sat Nov 05 14:17:15 CET 2022  
 Fingerprints: MD5: B4:BC:CA:41:16:23:4D:9F:08:10:34:64:D6:57:A1:84  
 SHA1: 22:DE:20:A1:BE:2B:6D:D2:4B:BA:C9:18:BB:C0:C8:97:D2:87:0A:99

#### 13.2.2. SCS Default Certificate

Owner: CN=RemoteConnector, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE  
 Issuer: CN=Fujitsu Technology Solutions, OU=IP SW SV, O=Fujitsu Technology Solutions, L=Munich, ST=Bavaria, C=DE  
 Serial No.: 2  
 Issued On: Thu Feb 26 14:18:52 CET 2009  
 Expires On: Sat Nov 05 14:18:52 CET 2022  
 Fingerprints: MD5: CC:8A:B2:C7:8D:01:32:98:5F:DC:C9:97:5C:66:03:D7  
 SHA1: 09:25:E8:C6:6E:6C:44:B5:3C:78:F5:FF:32:91:21:D0:EF:55:93:63

## 14. More Information Regarding Enterprise Security

Fujitsu is at the forefront of secure systems developments. Building on the foundation of our highly available servers, we work with the leading enterprise security partners to offer customers sophisticated and proven technology that addresses every area of enterprise security. You will find more information about this topic at:

[http://ts.fujitsu.com/solutions/it\\_infrastructure\\_solutions/security/index.html](http://ts.fujitsu.com/solutions/it_infrastructure_solutions/security/index.html)

## 15. Appendix: Overview of iRMC S4 / Cryptography Support

### 15.1. IPMI

#### 15.1.1. RMCP

| Algorithm | Symmetric/Asymmetric length |
|-----------|-----------------------------|
| MD5       | Symmetric – 128bit          |

#### 15.1.2. RMCP+

| Algorithm    | Symmetric/Asymmetric length |
|--------------|-----------------------------|
| HMAC-SHA1    | Symmetric – 160bit          |
| HMAC-SHA1-96 | Symmetric – 96bit           |
| HMAC-SHA256  | Symmetric – 256bit          |
| HMAC-MD5-128 | Symmetric – 128bit          |
| MD5-228      | Symmetric – 128bit          |
| AES-CBC      | Symmetric – 128bit          |

#### 15.1.3. List of supported cipher suites in IPMI

| ID | Authentication Algorithm | Integrity Algorithm | Confidentiality Algorithm |
|----|--------------------------|---------------------|---------------------------|
| 1  | RAKP-HMAC-SHA1           | NONE                | NONE                      |
| 2  | RAKP-HMAC-SHA1           | HMAC-SHA1-96        | NONE                      |
| 3  | RAKP-HMAC-SHA1           | HMAC-SHA1-96        | AES-CBC-128               |
| 6  | RAKP-HMAC-MD5            | NONE                | NONE                      |
| 7  | RAKP-HMAC-MD5            | HMAC-MD5-128        | NONE                      |
| 8  | RAKP-HMAC-MD5            | HMAC-MD5-128        | AES-CBC-128               |
| 11 | RAKP-HMAC-MD5            | MD5-128             | NONE                      |
| 12 | RAKP-HMAC-MD5            | MD5-128             | AES-CBC-128               |
| 15 | RAKP_HMAC_SHA256         | NONE                | NONE                      |
| 16 | RAKP_HMAC_SHA256         | HMAC-SHA256-128     | NONE                      |
| 17 | RAKP_HMAC_SHA256         | HMAC-SHA256-128     | AES-CBC-128               |

## 15.2. OpenSSH

|                 | Relaxed                                                                                                                                                                                                                                                                                                                                  | Intermediate                                                                                                                                                                                                                                                                                                                             | Restricted                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Key exchange    | diffie-hellman-group-exchange-sha1<br>diffie-hellman-group-exchange-sha256<br>diffie-hellman-group1-sha1<br>diffie-hellman-group14-sha1<br>ecdh-sha2-nistp256<br>ecdh-sha2-nistp384<br>ecdh-sha2-nistp521<br><br>*Added in iRMC S4 9.60F, iRMC S5 2.60P and later:<br><br>diffie-hellman-group14-sha256<br>diffie-hellman-group16-sha512 | diffie-hellman-group-exchange-sha1<br>diffie-hellman-group-exchange-sha256<br>diffie-hellman-group1-sha1<br>diffie-hellman-group14-sha1<br>ecdh-sha2-nistp256<br>ecdh-sha2-nistp384<br>ecdh-sha2-nistp521<br><br>*Added in iRMC S4 9.60F, iRMC S5 2.60P and later:<br><br>diffie-hellman-group14-sha256<br>diffie-hellman-group16-sha512 | diffie-hellman-group-exchange-sha256<br>ecdh-sha2-nistp256<br>ecdh-sha2-nistp384<br>ecdh-sha2-nistp521<br><br>*Added in iRMC S4 9.60F, iRMC S5 2.60P and later:<br><br>diffie-hellman-group14-sha256<br>diffie-hellman-group16-sha512 |
| Server host key | *Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>rsa-sha2-256<br>rsa-sha2-512<br>ssh-rsa<br><br>* iRMC S4 9.60F, iRMC S5 2.60P or later:<br><br>ecdsa-sha2-nistp256<br>ecdsa-sha2-nistp384<br>ecdsa-sha2-nistp512                                                                                                                     | *Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>rsa-sha2-256<br>rsa-sha2-512<br>ssh-rsa<br><br>* iRMC S4 9.60F, iRMC S5 2.60P or later:<br><br>ecdsa-sha2-nistp256<br>ecdsa-sha2-nistp384<br>ecdsa-sha2-nistp512                                                                                                                     | *Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>rsa-sha2-256<br>rsa-sha2-512<br>ssh-rsa<br><br>* iRMC S4 9.60F, iRMC S5 2.60P or later:<br><br>ecdsa-sha2-nistp256<br>ecdsa-sha2-nistp384<br>ecdsa-sha2-nistp512                  |
| Encryption      | 3des-cbc<br>aes128-cbc<br>aes128-ctr<br>aes192-cbc<br>aes192-ctr<br>aes256-cbc<br>aes256-ctr<br>blowfish-cbc<br>cast128-cbc<br><a href="mailto:rijndael-cbc@lysator.liu.se">rijndael-cbc@lysator.liu.se</a>                                                                                                                              | aes128-ctr<br>aes192-ctr<br>aes256-ctr                                                                                                                                                                                                                                                                                                   | aes128-ctr<br>aes192-ctr<br>aes256-ctr                                                                                                                                                                                                |
| MACs            | hmac-sha1<br>hmac-sha2-256<br>hmac-sha2-512<br><a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a><br><br>*Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>hmac-ripemd160<br><a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>                                                                      | hmac-sha1<br>hmac-sha2-256<br>hmac-sha2-512<br><a href="mailto:umac-64@openssh.com">umac-64@openssh.com</a><br><br>*Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>hmac-ripemd160<br><a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>                                                                      | hmac-sha2-256<br>hmac-sha2-512<br><br>*Used up to iRMC S4 9.20F and iRMC S5 2.50P:<br><br>hmac-ripemd160<br><a href="mailto:hmac-ripemd160@openssh.com">hmac-ripemd160@openssh.com</a>                                                |
| Compression     | none<br><a href="mailto:zlib@openssh.com">zlib@openssh.com</a>                                                                                                                                                                                                                                                                           | none<br><a href="mailto:zlib@openssh.com">zlib@openssh.com</a>                                                                                                                                                                                                                                                                           | none<br><a href="mailto:zlib@openssh.com">zlib@openssh.com</a>                                                                                                                                                                        |

### 15.3. SNMPv3

| Algorithm | Symmetric/Asymmetric length |
|-----------|-----------------------------|
| SHA       | Symmetric – 160             |
| MD5       | Symmetric -128              |
| AES       | Symmetric – 128,192,256 bit |
| DES       | Symmetric – 56bit           |

### 15.4. Web, KVM, VMEDIA, Redfish (iRMC S5 only)

These services use OpenSSL libraries which is part of the iRMC firmware. OpenSSL version 0.9.8, 1.0.1, 1.0.2 are used depending on the firmware version. For more information, see the iRMC manuals provided for the iRMC release used.

#### 15.4.1. Cipher list for SSLv3

| Ciphers                               | Key Exchange | Authentication | Encryption     | MAC  |
|---------------------------------------|--------------|----------------|----------------|------|
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA      | DH           | RSA            | AES(256)       | SHA1 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA      | DH           | RSA            | AES(128)       | SHA1 |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA | DH           | RSA            | Camellia (256) | SHA1 |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA | DH           | RSA            | Camellia (128) | SHA1 |
| TLS_RSA_WITH_AES_256_CBC_SHA          | RSA          | RSA            | AES(256)       | SHA1 |
| TLS_RSA_WITH_AES_128_CBC_SHA          | RSA          | RSA            | AES(128)       | SHA1 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA     | RSA          | RSA            | Camellia (256) | SHA1 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA     | RSA          | RSA            | Camellia (128) | SHA1 |

#### 15.4.2. Cipher list for TLSv1.2

| Ciphers                               | Key Exchange | Authentication | Encryption     | MAC    |
|---------------------------------------|--------------|----------------|----------------|--------|
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384   | DH           | RSA            | AESGCM(256)    | AEAD   |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA256   | DH           | RSA            | AES(256)       | SHA256 |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA      | DH           | RSA            | AES(256)       | SHA1   |
| TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA | DH           | RSA            | Camellia(256)  | SHA1   |
| TLS_RSA_WITH_AES_256_GCM_SHA384       | RSA          | RSA            | AESGCM(256)    | AEAD   |
| TLS_RSA_WITH_AES_256_CBC_SHA256       | RSA          | RSA            | AES(256)       | SHA256 |
| TLS_RSA_WITH_AES_256_CBC_SHA          | RSA          | RSA            | AES(256)       | SHA1   |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA     | RSA          | RSA            | Camellia (256) | SHA1   |
| TLS_DHE_RSA_WITH_AES_128_GCM_SHA256   | DH           | RSA            | AESGCM(128)    | AEAD   |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA256   | DH           | RSA            | AES(128)       | SHA256 |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA      | DH           | RSA            | AES(128)       | SHA1   |
| TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA | DH           | RSA            | Camellia (128) | SHA1   |
| TLS_RSA_WITH_AES_128_GCM_SHA256       | RSA          | RSA            | AESGCM(128)    | AEAD   |
| TLS_RSA_WITH_AES_128_CBC_SHA256       | RSA          | RSA            | AES(128)       | SHA256 |
| TLS_RSA_WITH_AES_128_CBC_SHA          | RSA          | RSA            | AES(128)       | SHA1   |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA     | RSA          | RSA            | Camellia (128) | SHA1   |

## 15.5. CIM/SMASH (iRMC S4 only)

Cipher list for TLSv1.1

| Ciphers                           | Key Exchange | Authentication | Encryption     | MAC  |
|-----------------------------------|--------------|----------------|----------------|------|
| TLS_RSA_WITH_AES_256_CBC_SHA      | RSA          | RSA            | AES(256)       | SHA1 |
| TLS_RSA_WITH_CAMELLIA_256_CBC_SHA | RSA          | RSA            | Camellia (256) | SHA1 |
| TLS_RSA_WITH_AES_128_CBC_SHA      | RSA          | RSA            | AES(128)       | SHA1 |
| TLS_RSA_WITH_CAMELLIA_128_CBC_SHA | RSA          | RSA            | Camellia (128) | SHA1 |

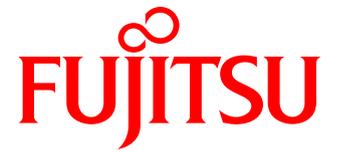
## 15.6. Linux Kernel Ciphers

The following algorithms are available in the Kernel and may vary based on Kernel configurations in different FW versions.

| Algorithm | Symmetric/Asymmetric length |
|-----------|-----------------------------|
| DES       | Symmetric -56               |
| 3DES      | Symmetric – 56,112,168      |
| MD5       | Symmetric - 128             |
| SHA1      | Symmetric – 160             |

## 16. Glossary

|                         |                                                                                                                                                                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AVR                     | Advanced Video Redirection                                                                                                                                                                                                                                                                                                         |
| Certificate             | An electronic document that contains a public key of subject and identifying information about the subject. The certificate is signed by a Certification Authority (CA) to bind the key and subject identification together.                                                                                                       |
| CA                      | A Certification Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual they claim to be. |
| CGI                     | Common Gateway Interface                                                                                                                                                                                                                                                                                                           |
| DHCP                    | Dynamic Host Configuration Protocol                                                                                                                                                                                                                                                                                                |
| DMZ                     | Demilitarized Zone: is a network area that sits between an internal network of organization and an external network, usually the Internet.                                                                                                                                                                                         |
| HTML                    | Hypertext Markup Language                                                                                                                                                                                                                                                                                                          |
| IANA                    | Internet Assigned Numbers Authority                                                                                                                                                                                                                                                                                                |
| IIS                     | Internet Information Server (Microsoft)                                                                                                                                                                                                                                                                                            |
| JBoss                   | Synonym for the JBoss Application Server ( <a href="http://www.jboss.org/jbossas/">http://www.jboss.org/jbossas/</a> )                                                                                                                                                                                                             |
| KVM                     | Keyboard Video Mouse                                                                                                                                                                                                                                                                                                               |
| OS                      | Operating system                                                                                                                                                                                                                                                                                                                   |
| POST                    | Power On Self Test                                                                                                                                                                                                                                                                                                                 |
| PXE                     | Pre-boot Execution Environment                                                                                                                                                                                                                                                                                                     |
| iRMC                    | Integrated Remote Management Controller (RSB functionality on board)                                                                                                                                                                                                                                                               |
| LDAP                    | The Lightweight Directory Access Protocol is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.                                                                                                                                                         |
| RSB                     | RemoteView Service Board                                                                                                                                                                                                                                                                                                           |
| RTDS                    | Remote Test and Diagnosis System                                                                                                                                                                                                                                                                                                   |
| Security Mechanism      | A process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system. Examples: authentication exchange, checksum, digital signature, encryption, etc.                                                                                       |
| Security Policy         | A set of rules and practices that specify or regulate how a system or organisation provides security services to protect sensitive and critical system resources                                                                                                                                                                   |
| Self-signed certificate | A certificate that is its own Certificate Authority (CA), such that the subject and the CA are the same.                                                                                                                                                                                                                           |
| SNMP                    | Simple Network Management Protocol                                                                                                                                                                                                                                                                                                 |
| SSL                     | Secure Socket Layer – a protocol on top of TCP/IP                                                                                                                                                                                                                                                                                  |
| SSDP                    | Simple Service Discovery Protocol                                                                                                                                                                                                                                                                                                  |
| TCP                     | Transmission Control Protocol                                                                                                                                                                                                                                                                                                      |
| TFTP                    | Trivial File Transfer Protocol                                                                                                                                                                                                                                                                                                     |
| UDP                     | User Datagram Protocol                                                                                                                                                                                                                                                                                                             |
| WBEM                    | Web-Based Enterprise Management - an initiative                                                                                                                                                                                                                                                                                    |



---

*All rights reserved, including intellectual property rights. Technical data subject to modifications and delivery subject to availability. Any liability that the data and illustrations are complete, actual or correct is excluded.*

Designations may be trademarks and/or copyrights of the respective manufacturer, the use of which by third parties for their own purposes may infringe the rights of such owner.

For further information, see [ts.fujitsu.com/terms\\_of\\_use.html](https://ts.fujitsu.com/terms_of_use.html)