FUJITSU

White Paper
Secure PRIMERGY Server Management Enterprise Security

PRIMERGY server management for secure, highly available platforms

Content

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.
For more details: https://www.bsi.bund.de/cln_165/EN/Publications/publications_node.html

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.

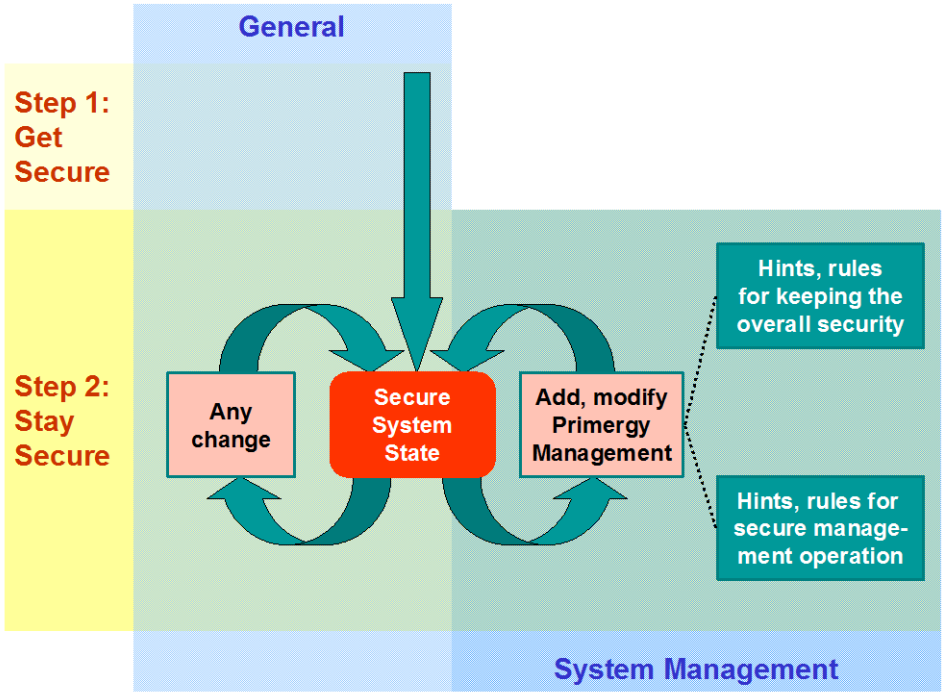


Fig. 1: Security Approach

Fig.1 illustrates this approach. The General approach consists of the two steps "Get Secure" and "Stay Secure". In a Microsoft environment, the Microsoft Baseline Security Analyzer (MBSA) can be used to support the first step “Get Secure”. It s a tool that helps small and medium businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. For more details please refer to http://technet.microsoft.com/en-us/security/cc184923.aspx

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 described in detail in: http://www.sans.org/top20.htm , or check: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

They are also 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 manual “ServerView Suite: Basic Concepts”, 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.

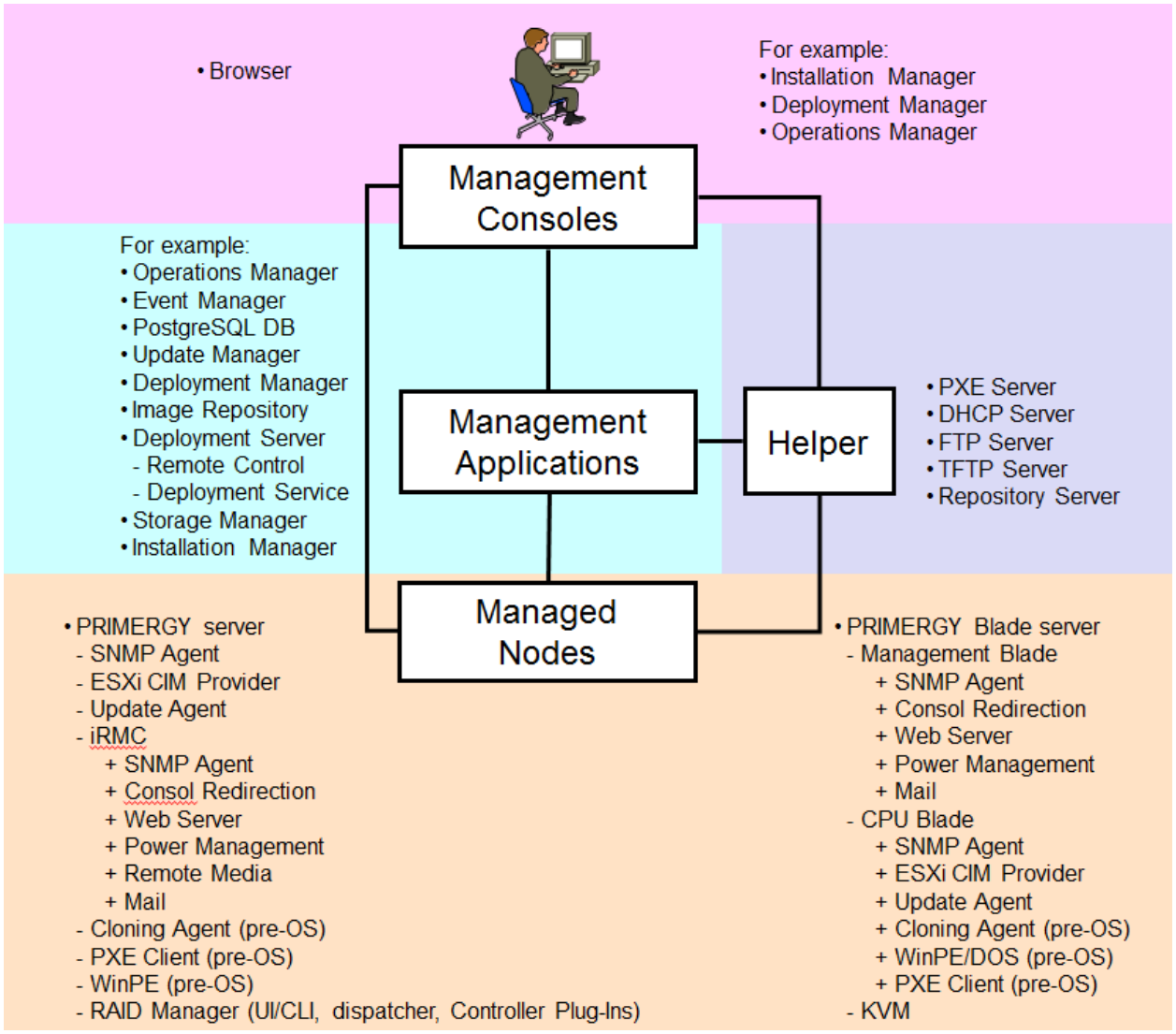


Fig 2: Communication Paths used by the ServerView Suite for PRIMERGY servers

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.

More details: 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 Browser ←→ Event Manager Browser ←→ Update Manager Browser ←→ Remote Management/Web Frontend Browser ←→ Deployment Manager Browser←→Virtual I/O-Manager	3169 (IANA-registered port): UDP/TCP JBoss Application Server 3170 (IANA-registered port): UDP/TCP JBoss Application Server over SSL 3172 (IANA-registered port): UDP/TCP 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 ←→ ServerView Tomcat	3170: HTTPS 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. 9092 (on localhost only, external access can be prevented by firewall): Internal Database H2 5480: Configuration port of Plugin appliance
vRealize Operations ←→ ServerView Tomcat	3170: HTTPS
The NAGIOS Plugin script accept variable port parameters. The following defaults are used: Script ←→ SNMP Script ←→ CIM-XML Script ←→ WS- MAN Script ←→ REST CIM Indications - Listener	 161 https: 5989, http: 5988 ESXi https: 8888, http: 8889, Other https:5986, http:5985 SCS: 3172 iRMC https: 443, http: 80 https and http: 3169
REST Client ←→ SysRollOut-Service	3169/3170: HTTP(S) (configurable)
Management Consoles – Managed Nodes	
Browser (Advanced Video Redirection) ←→ iRMC Web-Server Browser ←→ Management Blade: Web-Server	80: UDP/TCP Web HTTP (configurable)443: UDP/TCP HTTP over TLS/SSL (configurable)
Browser ←→ iRMC Remote Media	iRMC S1 & iRMC S2 with FW < 5.x: 5901 (configurable): UDP/TCP Transfer of FD/CDROM/DVD/Image/USB Memory Device iRMC S2 with FW > 5.0, iRMC S3: 80 (configurable): UDP/TCP Transfer of FD/CDROM/DVD/Image/USB Memory Device
Browser ←→ ESXi system	5989: Incoming and outgoing TCP CIM-XML transactions over HTTPS 5988: Incoming and outgoing TCP CIM-XML transactions over HTTP
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
Browser ←→ iRMC Text Console	22: TCP (SSH, configurable) 3172: TCP (Telnet, configurable) 623: UDP (RMCP+ / Serial over LAN)
Browser ←→ Digital KVM (BX 600 dKVM) Note: all default ports can be changed manually if desired	2068 + 2069: TCP Encrypted keyboard and mouse data 1078: TCP Video Port, Virtual Console (Viewer) 3169: TCP Virtual Media 80: Web Server HTTP
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) 636 UDP 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 (WinPE)	9213 (IANA-registered port): UDP/TCP Installation Manager Remote Control (configurable)
ServerView Tomcat ←→ ESXi, MMB	3170: TCP (cim.listening.port) 161: UDP/TCP SNMP 162: UDP/TCP SNMP traps 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.
Refish Client ←→ iRMC	iRMC S5 443: TCP (configurable) Redfish service
Management Console – Management Console (SVOM V6.10)	
JBoss	25 Mail SMTP Localhost Port
JBoss	1325 Remoting Port
JBoss	1445 TXN Recovery Environment Port
JBoss	4713 TXN Status Manager Port
JBoss	
JBoss	8009 Apache JServ Protocol (AJP) Port
JBoss	8090 OSGI HTTP Port
JBoss	9443 Management HTTPS Port
JBoss	9990 Management HTTP Port
JBoss	9999 Management Native Port
Management Console – Management Console (SVOM V6.11 and higher)	
JBoss	9999 Management Native Port
JBoss	All other ports are allocated dynamically from the “Dynamic Port” range defined by RFC 6335.

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	
Ports 1325, 1445, 4713, 8090, 9443, 9990, 9999 are no longer used	
Management Application - Directory Service	
Central Authentication Service ←→ Directory Service	389: LDAP default port (non-secure) 636: LDAP SSL default port 1473: LDAP port of ServerView's ApacheDS / OpenDJ(non-secure) 1474: LDAP SSL port of ServerView's ApacheDS / OpenDJ
Management Application - Management Application	
OpenDJ Control Panel ←→ OpenDJ	4444: Management Port of ServerView's OpenDJ (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
Deployment Manager ←→ Deployment Service (Deployment Server)	4971: UDP/TCP Private ports (Fujitsu) – not registered
Deployment Manager ←→ Image Repository Deployment Service (Deployment Server) ↔ Image Repository	137 / 138 / 445: Microsoft SMB Microsoft: Remote Network Drive
SysRollOut-Service ←→ SOA-Service	3169/3170: HTTP(S) (configurable) 9092 (on localhost only, external access can be prevented by firewall): Internal Database H2

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
Deployment Service (Deployment Server) ←→ Cloning Agent (CPU Blade)	4973...4989: UDP Private ports (Fujitsu) – not registered
Deployment Service (Deployment Server) ←→ Cloning Agent (CPU Blade)	4972: UDP, 4974...4989: UDP/TCP Private ports (Fujitsu) – not registered
Installation Manager ←→ Installation Agent (WinPE)	9213 (IANA-registered port): UDP/TCP Installation Manager Remote Control (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. 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
vCenter Plugin ←→ iRMC	623: UDP: RMCP (IPMI over LAN) 162: SNMP traps from iRMC to management station 80/443: HTTP(S) Communication to eLCM REST API
SysRollOut-Service ←→ iRMC	3169/3170: HTTP(S) (configurable)
Management Application – Management Application	
Virtual-IO Manager ←→ Virtual-IO Manager	50042: Management Station internal communication
Management Applications – Helpers	
Update Manager ←→ PXE Server (Update Proxy) Update Manager ←→ TFTP Server (Update Proxy)	3171 (IANA-registered port): TCP 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)
Cloning Agent ←→ DHCP Server Cloning Agent (CPU Blade) ←→ DHCP Server Update Agent ←→ PXE Server (PXE Boot)	67: UDP/TCP Bootstrap Protocol Server (bootps)
Cloning Agent ←→ PXE Server PXE Client ←→ PXE Server WinPE ←→ PXE Server Cloning Agent (CPU Blade) ←→ 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
Cloning Agent ←→ TFTP Server PXE Client ←→ TFTP Server WinPE ←→ TFTP Server Cloning Agent (CPU Blade) ←→ TFTP Server PXE Client (CPU Blade) ←→ TFTP Server WinPE (CPU Blade) ←→ TFTP Server Update Agent ←→ PXE Server (PXE Boot) Management Blade ←→ TFTP Server iRMC S2 ←→ TFTP Server	69: UDP/TCP Trivial File Transfer (TFTP)
Management Blade ←→ TFTP Server	161: UDP/TCP SNMP 80: UDP/TCP Web HTTP

3.1.1.Network Ports used by the iRMC family

For better readability the next table summerizes all ports used by the iRMC S1 / iRMC S2 / iRMC S3 / iRMC S4:

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 outbound from iRMC (configurable)
SNMP Traps:	162 outbound from iRMC (fixed)
LDAP:	389 (non secure) 636 (secure) outbound from iRMC (fixed for iRMC S1, configurable iRMC S2 / S3 with Firmware > 5.2x), configurable iRMC S4/S5
CAS / Single Sign On:	3170 outbound from iRMC (iRMC S2 / S3, S4, S5 only; 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 S2 (AVR and Remote Media with Firmware > 5.0x) / iRMC S3 (Changed Remote Media from Applet)	
AVR(Video):	80 inbound to iRMC (configurable/shared with http port)
AVR(Secure):	443 inbound to iRMC (configurable/shared with https port)
Remote Media:	80 inbound to iRMC from Applet(configurable/shared with http port)
Remote Media:	5901 outbound from iRMC to Standalone Storage Server (configurable)
iRMC S2 / iRMC S3 / iRMC S4 / iRMC S5	
tftp:	69 outbound from iRMC (fixed)…
iRMC S5	
Redfish	443 inbound to iRMC (configurable)

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 or Deployment Manager,

and

- between the browser with Java-Front-ends (Management Console) and Web server on the RSB, iRMC, RSB S2, 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 (also see Recommendation 28)

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 mean 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, iRMC S2, iRMC S3, iRMC S4 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. You can look at the list of CA certificates contained in Firefox's trust store also here: https://mozillacaprogram.secure.force.com/CA/IncludedCACertificateReport

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. Both Internet Explorer and Firefox allow you to accept the certificate (i.e. trust it). At that point you can permanently import the certificate into the respective browser's trust store 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 ServerView's Operations Manager's server certificate, is described below in the section 7.3, "TLS/SSL 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 product's documentation. 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 CA's certificate 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 don't want to buy certificates signed by (commercial) CAs already trusted by the browser. Then import your CA's certificate 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 manual "User Management in ServerView". This manual can be downloaded from the ServerView 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 ServerView's start page, but display a warning like "This Connection is Untrusted" or "There is a problem with this website's security certificate" 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 server's private key. 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 keystore’s password. 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 server certificate’s fingerprint, 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 ServerView’s pre-produced certificates are not suitable for identifying a certain web server, their fingerprints are listed in this document for completeness, cf. section 14, “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 ServerView’s built-in directory service 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 user’s credentials 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. A very good and also well-written one is presented by the *United States Computer Emergency Readiness Team* (US-CERT) under http://www.us-cert.gov/reading_room/securing_browser/. If you obey the recommendations given there you can avoid most of the dangers contained in some of today’s web pages. But 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 ServerView’s web pages.

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

3.7.1. Cookies

As set out in the above US-CERT article, you should meticulously control the setting of cookies in your browser. Please note in this context that ServerView’s web pages 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 ServerView’s web pages.

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

`CASTGC`: This is the *Ticket Granting Ticket Cookie* of ServerView’s *Central Authentication Service* (CAS). 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 ServerView’s products.

`org.springframework.web.servlet.i18n.CookieLocaleResolver.LOCALE`: This cookie is set by the Spring Framework used by ServerView's CAS 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

As set out in the above US-CERT article, 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.

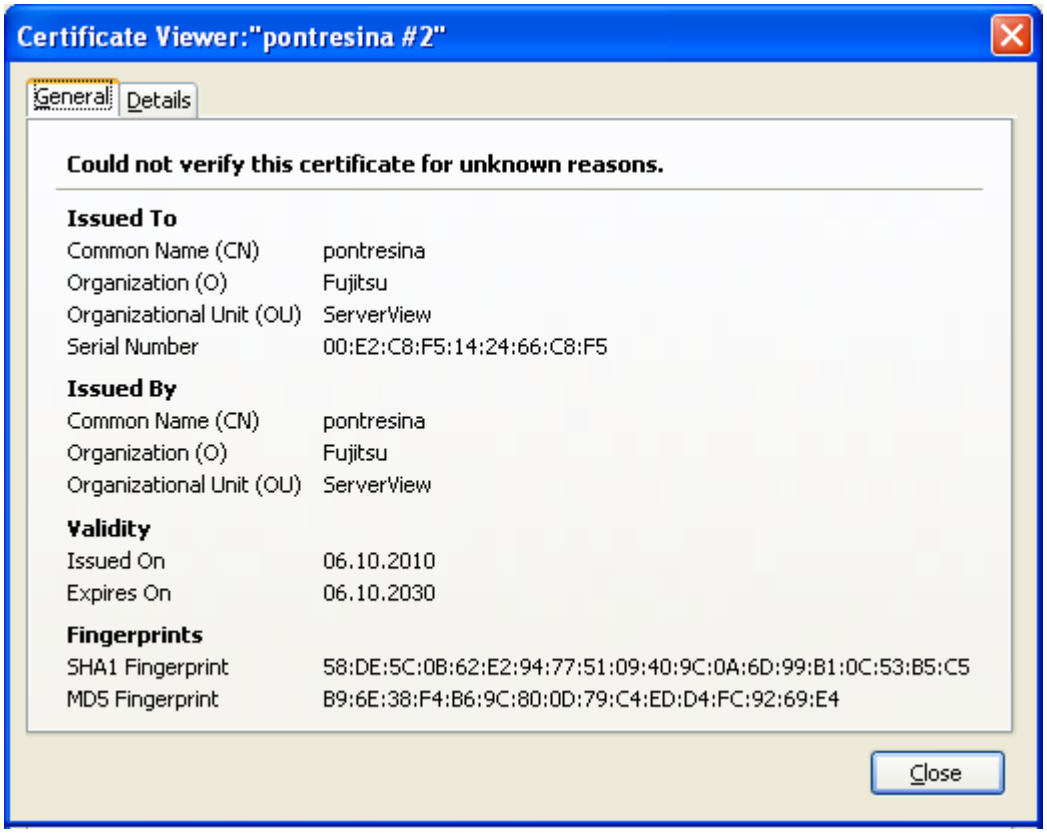
3.7.3.Certificate management

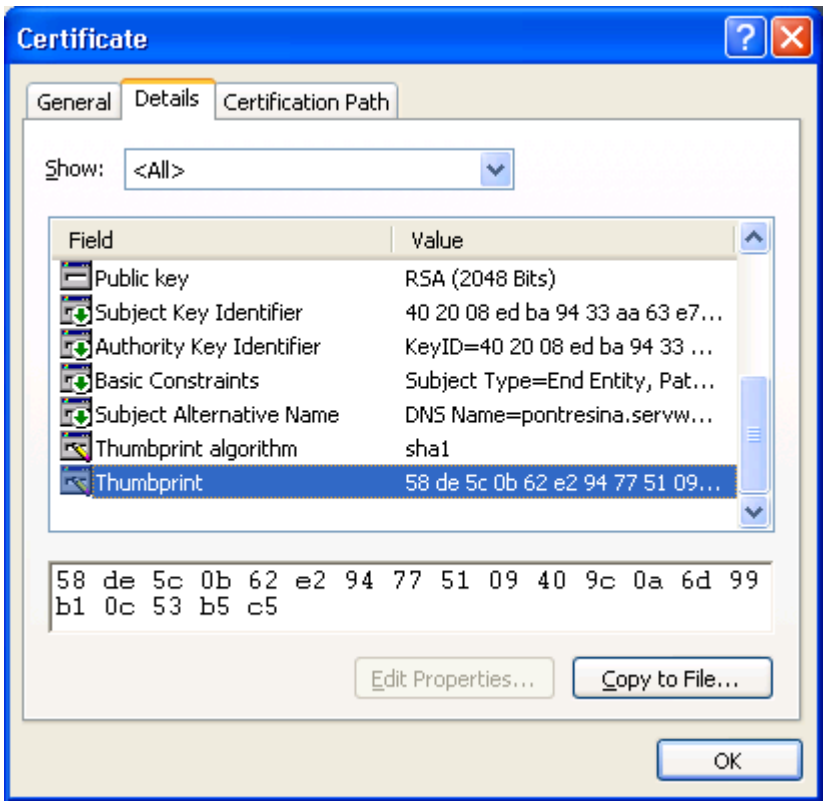
Web-based communication within the Operations Manager is secured by SSL connections. In former versions the Operations Manager provided secured access by connections secured by the Secure Socket Layer (SSL) as an option. With version 5.00 or higher this has become mandatory for security reasons, i.e., 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 certificate's fingerprint 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 certificate's fingerprints, as for instance Mozilla's Firefox or Microsoft's Internet Explorer:





Most browsers provide the server certificate details by right-clicking on the page and then choosing the page's properties. 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 CMS's server certificate.

You can avoid checking the same certificate repeatedly by "importing" or "installing" it into the browser's "trust store". 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 browser's trust store using the browsers Certificate Manager.

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".

In case of Internet Explorer, you can choose "Tools" -> "Internet Options", and then select in the new panel the "Content" tab where you start the Manager by clicking on the "Certificates" button.

Recommendation 11

> Frequently check the imported certificates in your browser's trust store. 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.

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
- SysRollOut Service for profile-based deployment
- 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 details, please refer to section 8.1 Update Management.

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 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.

Note: If ServerView RAID Manager is installed on old servers with Intel chipsets running LSI's MegaIDE software RAID implementation, there runs also a Windows service (SPYser.exe) or a Linux daemon (Spy) on the managed node listening on TCP port 5554. This service is not from Fujitsu, but a binary from the controller supplier, which is needed by ServerView RAID Manager. If random data are sent to this service, it may happen that it crashes. But this is not a real security problem. In this case, the service / daemon must be restarted. During normal operation, however, this does not happen.

4.2. Remote Installation with the Installation Manager

Besides the local installation of PRIMERGY servers, the Installation Manager provides also remote installation – for up to five systems in parallel. 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 12

> 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 SSL (see also Recommendation 28), 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 13

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 14

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 ServerView's built-in directory service. 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 user's identify: "Who are you?"
- Authorization defines a user's rights: "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 user's identify before allowing administrative access. This would require the user to repeatedly issuing his credentials whenever changing from one product's web pages 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 user's point of view. The CAS stores the information about a user's identity 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 15

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

5.2. Role-based access control (RBAC)

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

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 16

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 17

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 18

Modify the default settings of the SNMP service. For more detailed 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 as well as Win-32 based ServerView support 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", which is described in section 6.2. If you want to disable SNMP set operations for security reasons generally, you can configure the SNMP service correspondingly.

Since SV Deployment Manager v5.20 SNMP-set operations can be avoided by enabling telnet(ssh) in the "remote management ports" dialogue of SVDM.
Since V6.1 SNMP set operations are substituted by default by telnet(ssh). Accessing the management blade requires a username and password which must be assigned in deployment manager for the appropriate MMB.

6.1.1.Configuration of the SNMP Service via MS System Policy Editor

For Windows it is possible to provide settings for multiple users by using System Policy Editor to create an Ntconfig.pol file. These files can also be distributed to other servers. How to use this approach for configuring the MS SNMP Service is described in http://www.microsoft.com/technet/archive/winntas/maintain/getting.mspx#ELIAC in the section “Using the System Policy Editor”.

Recommendation 19

For the convenient configuration of MS SNMP Services on many servers you can use the MS System Policy Editor.

6.1.2.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 optinonal for SNMPv3 to ensure user privacy and user authorizied access control. These are the attributes for the USM (User Security Model) and available in net-snmp package for the iRMC.

6.1.3.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 or the Win32-based ServerView for authentication before sending SNMP SET requests to the agent.

This account (name and password) is also used by the Deployment Manager, if the ServerView Agent Shutdown method is used. In this case this name and password must be specified, when the administrator specifies the shutdown method for a server in the Deployment Manager.

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. In a Microsoft environment please follow the instructions given by Microsoft at http://technet.microsoft.com/en-us/library/bb726987.aspx sowie http://technet.microsoft.com/en-us/library/bb727017.aspx

6.4. ServerView CIM Providers

6.4.1. ServerView ESXi CIM Providers

VMware ESXi doesn’t have a console OS and furthermore SNMP isn’t supported. Therefore the ServerView Agents for Linux can’t 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 will be available in the future in the ESXi Embedded image from FTS. Installation and update by Offline Bundle as described above will also be possible.

In order to get the monitoring information in SV Operations Manager from the ESXi system an arbitrary user with the “Administrator” role for the object “ESXi host” must be created on the ESXi system.

The VMware document “ESXi Configuration Guide (available at: http://www.vmware.com/pdf/vsphere4/r41/vsp_41_esxi_server_config.pdf) contains a chapter “Security” with additional helpful information.

6.4.2. ServerView CIM Provider for Windows

CIM Providers are also available for newer versions of Microsoft Windows. The following versions are supported:

- Microsoft Windows® Server™ 2008 R2 all editions (x64)
- Microsoft Windows® Server 2012 (x64)
- Microsoft Windows® Server 2012 R2 (x64)

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

CIM Providers are also available for the following Linux versions:

- Novell (SLES11) as of SP 2 (x86_64)
- Novell (SLES12) (x86_64)
- Red Hat RHEL 5.8/5.9/5.10/5.11 (x86_64)
- Red Hat RHEL 6.3/6.4/6.5/6.6/6.7/6.8 (x86_64)
- Red Hat RHEL 7.0/7.1/7.2 (x86_64)

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). 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 Managament Stations In the Trust-Store of SCS (a copy of these files in the pki directory).

To do this see description in manual "User Management in ServerView" 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 Monitor

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 20: "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 20, "Community String for accepting SNMP requests".

Recommendation 22

> If you plan to use the Deployment Manager for cloning server blades, you must have configured the Remote Management Blades of these blade servers as managed nodes in the Operations Manager or the Win32-based ServerView. The reason is the Deployment Manager needs to access the MMB-IP for powercontrol actions on its managed blade servers. The Deployment Manager is also integrated in the Operations Manager or Win32-based ServerView and uses (if SNMP is enabled in the “remote managemet ports” dialogue) the SNMP community administration.

The ServerView Agents and the Central Management Server communicates via SNMP. As SNMP does 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 23

> 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 a security's 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 (JBoss).

You specify this account during installation of the Operations Manager, when you are asked for the account the JBoss application 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 24

> Create a non-administrative account dedicated for the JBoss application server that is installed with ServerView Operations Manager. Ensure that this account’s security settings prevent all non-administrative users from reading or writing the JBoss’s account directories and files.

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 manual “User Management in ServerView”. This manual can be downloaded from the ServerView 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 TSLv1.2 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` on Windows, resp. `/opt/fujitsu/ServerViewSuite/jboss/standalone/configuration/standalone.xml` 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_A
ES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH
E_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 don't 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_SH
A,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 don’t 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” attackes 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 thea 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.

7.5. 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 22), 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 snmptrap 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 won’t work!)
Don’t 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 <WINDOWSDIR>\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 -> Diagnotic 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 <WINDOWSDIR>\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 doesn’t 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 administrator’s efforts.

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 will in the future be 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 network

The 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 / iRMC S5

  In the eLCM package of the iRMC S4 / iRMC 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. And, 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 user's convenience!

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.

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 manual "PrimeCollect" 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 27

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 manual “PrimeCollect” contains a table that lists this information.

Recommendation 28

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 29

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.

Recommendation 30

> If you plan to use the Deployment Manager (and you have SNMP configured in the “remote management ports” dialogue of SVDM), configure the SNMP service on the Remote Management Board with a community string.
> Selection of SNMP/telnet(ssh) is configurable since SVDM V5.20 and by default telnet(ssh) since V6.1.
> It is also highly recommended to configure the SNMP address filtering according to the tables in Section 3.1 Communication Paths.

10. Out-of-band Management

As mentioned in the previous chapter, some tools of the ServerView Suite, like Operations Manager, use “out-of-band” SNMP agents for management purposes. The main tools for out-of-band management within the ServerView Suite, however, are in SV Remote Management, which comprises the following components:

- integrated Remote Management Controller (iRMC)
- Remote Management Blade

A lot of management solutions can be build with these components.

If the operating system is inactive, but the system hardware (at least basic system module functions) is active, the following management solutions are helpful:

- Remote Management /Web front-end and BMC/IPMI, also SNMP, CIM and Redfish for iRMC S4/S5
- Parallel management access to the Remote Management Controller (iRMC) or the Remote Management Blade via SNMP or HTTP (Web). Remote Management /LAN, Web or modem front-end; Web browser, Telnet or Terminal client.

If the operating system is inactive and the system hardware is not ready, the following management solutions are helpful:

- Parallel management access to the Remote Management Controller (iRMC) or the Remote Management Blade via SNMP or HTTP (Web). Remote Management/LAN, Web or modem front-end; Web browser, Telnet or terminal client.
- Basic remote management with Remote Management/LAN front-end and BMC/IPMI (e.g. text console redirection and power management).

The subsequent sections discuss all these solutions under security aspects. The subsequent Figure shows schematically the paths between the administrator and the managed nodes and where user accounts protect against unauthorized access.

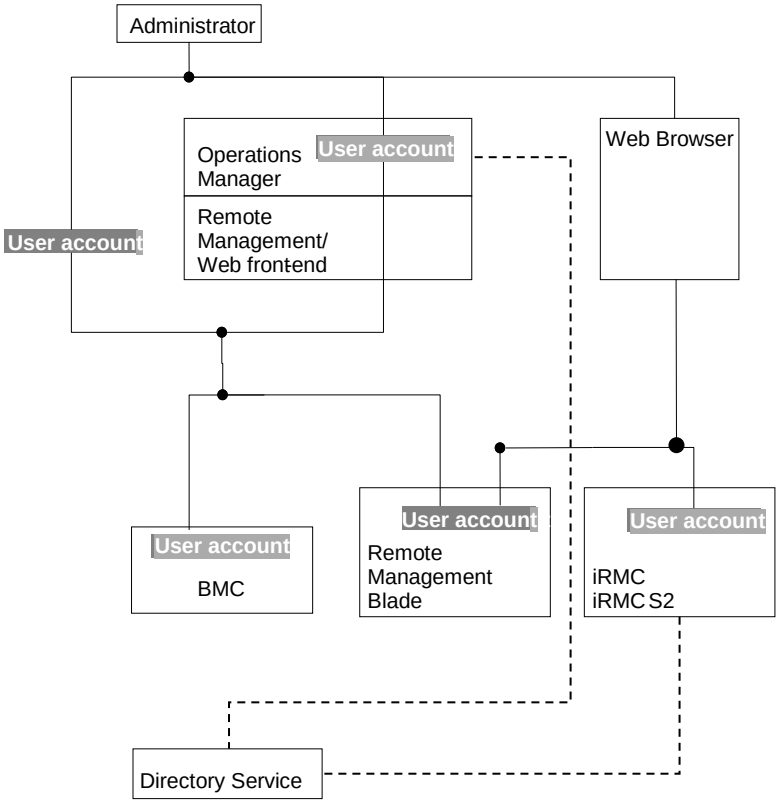


Fig. 3: Remote Management components and protection by user accounts

When delivered, many of the components have predefined default accounts. The following list shows these default accounts, which should be modified as soon as possible.

Component	Predefined default account
iRMC	Name/password: admin/admin
iRMC S2/S3/S4/S5	Name/password: admin/admin
Management Blade	Name/password: admin/admin
BMC	Name/password: admin/admin or OEM/OEM

10.1. Remote Management/LAN front-end with BMC/IPMI

The Remote Management/LAN front-end provides a working environment in which the various (console redirection) windows can be displayed.

To prevent unauthorized remote access to a server, the Remote Management/LAN front-end provides password protection. This protection is provided at the front-end side as well as on the target side (BMC, RSB, RSB S2, RSB S2 LP, Remote Management Blade).

When you start the Remote Management/LAN front-end for the first time, you are prompted to enter a password and confirm it. Here you should enter a password according to your company's security policy.

Recommendation 31

> Protect the access to the Remote Management/LAN front-end with a password according to your company's security policy.

When used with BMC/IPMI, the Remote Management/LAN front-end provides the following windows:

- Remote IPMI Manager window for access to a Baseboard Management Controller (BMC).
- Remote console window of type Telnet, if console redirection is started from a Remote IPMI Manager window that is connected to a BMC with firmware V2.x.

The connection from the IPMI Manager to the BMC is protected by user name/password. BMCs are shipped with preconfigured passwords. For security reasons, you are advised to change any preconfigured name/passwords as soon as possible, e.g. by means of the Server Management Tool, which is part of the Remote Management/Diagnostic System.

Recommendation 32

Change the preconfigured name/password of the BMCs as soon as possible.

10.2. Remote Management/Web front-end with BMC/IPMI

The Remote Management/Web front-end provides a working environment in which the various (console redirection) windows can be displayed. All that is required for display purposes at the remote workstation is a standard browser. The Remote Management/Web front-end is started from the Operations Manager and the installation of this application is therefore a necessary precondition. Therefore, unauthorized usage of the Remote Management/Web Front-end is prevented by the log-in procedure of the Operations Manager, which is described in section 7.3 TLS/SSL for the .

Concerning the configuration of the BMC, please follow Recommendation 36.

Console redirection is encrypted and takes place Serial Over LAN (SOL).

10.3. Parallel Management with management devices like iRMC or Management Blade

Whereas the previous sections 10.1 and 10.2 discussed security aspects for situations, where the OS is not running, this section regards management solutions which can be used when the OS is not running as well as when the OS is running. This is possible, because special management devices on the target servers are involved. These special devices comprise:

- Remote Management Controller (iRMC/iRMC S2(iRMC S3) or
- Remote Management Blade

These management devices can be accessed via

- Any Web browser
  The RSB/iRMC and the Remote Management Blade, respectively, can provide powerful management operations that can be started from any Web browser at anytime and from anywhere via the Internet

Here again protection against unauthorized access is provided by authentication at both sides, at the front-end and at the management device, as shown in detail in the subsequent sections.

10.3.1. iRMC

The iRMC is an autonomous system on the systems' motherboard and it can be accessed with a Web Browser. It has its own operating system, a Web server, user administration and alarm management and is also supplied with power when the server is in standby mode. The iRMC offers enhanced security functions, including SSL encryption and efficient user authentication to ensure maximum security.

The user management uses two different types of user identifications:

- Local user identifications are stored locally in the iRMC's non-volatile storage and are managed via the iRMC user interfaces.
- Global user identifications are stored in the central data store of a directory service and are managed via this directory service's interfaces.
  The following directory services are currently supported for global iRMC user management:
  – Microsoft® Active Directory
  – Novell® eDirectory
  – OpenLDAP / OpenDJ (via standard ports)

User management for the iRMC permits the parallel administration of local and global user identifications.

The iRMC distinguishes between two mutually complementary types of user permissions:

- Channel-specific privileges, i.e. iRMC assigns these permissions on a channel-specific basis (users can have different permissions, depending on whether they access the iRMC over the LAN interface or the serial interface)
- Permissions to use special iRMC functions (configure user accounts, configure iRMC settings, …)

For details please refer to the manual "iRMC - integrated Remote Management Controller" or "iRMC S2/S3 - integrated Remote Management Controller", respectively.

The firmware of the iRMC is preconfigured with the account admin/admin, which possesses all permissions. It is urgently recommended to create a new administrator account as soon as possible once you have logged in, and then delete the default administrator account or at least change the password for the account.

Recommendation 33

The iRMC is shipped with predefined accounts. For security reasons, it is highly recommended to replace these accounts by new accounts for local or global users or at least to change the password.

10.3.2. Management Blade

To prevent unauthorized remote access to a blade server system, Remote Management supports a user name/password protection mechanism on the Management Blade. Management Blades are preconfigured with the accounts admin/admin. For each Management Blade you can define multiple user IDs, each with individual passwords and rights.

For security reasons, it is highly recommended to create new accounts and to delete the default account or at least to change the password. This can be by done means of the Web Console or the Console Menu application.

Recommendation 34

Management Blades are shipped with predefined accounts. For security reasons, it is highly recommended to replace these accounts by new accounts or at least to change the password.

For additional information about the security of the web interface please refer also to section 10.3.3 Web interface on iRMCor Management Blade.

10.3.3. Web interface on iRMCor Management Blade

The iRMC or Management Blade have integrated Web servers which provide the Web interface. In a previous section about Operations Manager, it was mentioned that installation or configuration of a Web server might generate security holes if it is not done carefully and did not follow appropriate security rules. However, this is no issue for the mentioned integrated Web server for two reasons:

- These Web servers come pre-installed and pre-configured with the iRMCor Management Blade.
- These Web servers are completely disconnected from the operational part of the PRIMERGY system, i.e. a potential attack via these integrated Web server cannot affect data, disks or processors of the PRIMERGY system.

The iRMCor the Management Blade provide two ports, port 80 for normal Web HTTP communication and port 443 for SSL-secured HTTP communication. Port 443 for SSL is always enabled; port 80 for HTTP can be enabled or disabled. For security reasons, you should keep port 80 disabled, but remember to reconfigure remote port as well on iRMC.

Recommendation 35

As you can perform powerful management operations from a browser via the Internet, it is highly recommended to make sure that port 80 iRMC or the Management Blade is disabled.

10.3.4. Remote Management/Front-ends for parallel management

The Remote Management front-end available for management with management devices, like iRMC or Management Blade is the Web browser.

In this case, the browser contacts directly the web interface of the iRMC or Management Blade. Therefore, access to this integrated web server is protected by the log-in procedures, which are described in the previous sections 10.3.1 and 10.3.2.

11. Special configurations

11.1. Options for managing servers in a Demilitarized Zone

A Demilitarized Zone (DMZ) is a network area that sits between an organization's internal network 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.

12. 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: Recommendation	Administration Level		
	Target OS up	Diag. OS up	Second. Mgmt. Channel
Installation PRIMERGY server management: Locates all tools/components along with the managed servers behind a firewall.			
General: Minimize the number of open ports for each system.			
Separate Management VLAN: Separate management traffic from operational traffic			
Non-administrative account for JBoss: Create a non-administrative account dedicated for the JBoss application server that is installed with ServerView Operations Manager. Ensure that this account’s security settings prevent all non-administrative users from reading the JBoss’s account directories and files			
Role Assignement Always assign the least privileged role that allows the required operations			
Separate Management LAN for management devices: Connect the network interfaces of iRMC, etc. to a separate management LAN			
Remote Installation with Installation Manager: 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.			
Deployment Manager JBoss Application Server: Configure the JBoss Application Server to accept only local HTTP requests			
Deployment Manager Reference Installation: The most secure way is the local installation			
Deployment Manager Image Repository: Restrict access to the repository for Deployment Manager components only			
Installation of SNMP agents: Modify the default settings of SNMP services. For mass settings you can use the MS System Policy Editor.			
Installation of SNMP agents: Specify User Group for the ServerView authentication/authorization mechanism for set operations			
Installation of SNMP agents: Secure SNMPv1 with IPSec – Follow Microsoft instructions			
Deployment Manager for cloning server blades: Configure Management Blades as managed nodes in ServerView			
Central Management Server (CMS) and SNMP agents: Install the CMS and the agents on the managed servers behind a firewall			
Installation of Web server for Operations Manager: Secure the connection to the browser by SSL			
Actualisation of Update Files: If the download via the Internet is regarded too risky, use the ServerView Update DVD			

Event: Recommendation	Administration Level		
	Target OS up	Diag. OS up	Second. Mgmt. Channel
Update Manager Configuration: Specify User Group for the Update Manager authentication/authorization mechanism and configure the Update agent correspondingly.			
Updating drivers, agents, BIOS, firmware: If you prefer local tools, you can use the local Command Line Interface of the Update agent and the Update Manager Express			
Configure SNMP interface on the RSB/iRMC: Configure communities for read-only.			
Configure the Alarm Handler on the RSB/iRMC or Management Blade: For reliable notification, configure not only SNMP traps.			
RSB as concentrator: Configure the communication with the BMCs with authentication method MD5			
Deployment Manager and Remote Management Blade: Configure the SNMP service on the Management Blade with a community string and also the SNMP address filtering			
Remote Management/LAN front-end: Configure a password for protecting the access			
BMC Configuration: Configure IP addresses and password.			
Remote Management/Diagnostic System: Do not forget to change the default password of the RTDS. Configure call-back mode for enhanced security.			
iRMC/iRMC S2/iRMC S3/Management Blade accounts: Replace the default accounts by new accounts or change at least the password.			
iRMC/iRMC S2/ iRMC S3/Management Blade ports: Disable port 80 for HTTP; use only SSL-secured connections via port 443 for HTTPS			
"Management Network Topology": For avoiding unsecured SNMP set operations and unreliable traps, create Web agents by pushing down the Web Extension/Alarm Management to the managed server.			

13. 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
Deployment Manager	The Deployment Service always creates log files in the C:\Program Files\Fujitsu\ServerView Suite\DeploymentService\bin\AutoLog and C:\Program Files\Fujitsu\ServerView Suite\DeploymentService\tftp\log directories
Asset Manager	Inspection of log files via GUI
RAID Manager	By default file events are written to a ServerView RAID log file. By default all events show up in the operating system's logging facility. On Windows based systems entries can be found in Start > Settings > Control Panel > Administrative Tools > Event Viewer (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 <ServerView_Suite>\plugins\viom\Manager\logs. On a Windows based management station <ServerView_Suite> is typically the directory C:\Programm Files\Fujitsu\ServerView Suite On a LINUX based management station <ServerView Suite> is typically the directory /opt/Fujitsu/ServerViewSuite 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 S2/ S3/S4/S5	Error messages are written to the specified log file. If no log file is specified, the output is directed to the flbmc.log file.

14. 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:

14.1. Management Controller/Management Blade

14.1.1. 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

14.1.2. iRMC Default Certificate

Subject: C=DE, ST=Bavaria, O=Fujitsu Technology Solutions GmbH, CN=iRMC/emailAddress=primergy-pm@ts.fujitsu.com
Issuer: O=fujitsu, OU=fujitsu, CN=Fujitsu Internal Issuing CA EMEIA - G1
Serial No.: 28:00:00:01:2e:45:0d:f8:cf:6e:ea:f7:81:00:00:00:00:01:2e
Issued On: Jun 23 13:24:16 2016 GMT
Expires On: Jun 22 13:24:16 2021 GMT
Fingerprints: SHA1
B9:DA:F0:45:BF:2C:8A:23:25:49:C5:80:F8:CB:13:68:78:11:27:1F

14.1.3. 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

14.2. ServerView Connector Service (SCS)

14.2.1. 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

14.2.2. 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

15. 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

16. Appendix: Overview of iRMC S4 / Cryptography Support

16.1. IPMI

16.1.1. RMCP

Algorithm	Symmetric/Asymmetric length
MD5	Symmetric – 128bit

16.1.2. 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

16.1.3. 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

16.2. OpenSSH

	Relaxed	Intermediate	Restricted
Key exchange	diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521	diffie-hellman-group-exchange-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group1-sha1 diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521	diffie-hellman-group-exchange-sha256 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
Server host key	rsa-sha2-256 rsa-sha2-512 ssh-rsa	rsa-sha2-256 rsa-sha2-512 ssh-rsa	rsa-sha2-256 rsa-sha2-512 ssh-rsa

Encryption	3des-cbc aes128-cbc aes128-ctr aes192-cbc aes192-ctr aes256-cbc aes256-ctr blowfish-cbc cast128-cbc rijndael-cbc@lysator.liu.se	aes128-ctr aes192-ctr aes256-ctr	aes128-ctr aes192-ctr aes256-ctr
MACs	hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1 hmac-sha2-256 hmac-sha2-512 umac-64@openssh.com	hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1 hmac-sha2-256 hmac-sha2-512 umac-64@openssh.com	hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha2-256 hmac-sha2-512
Compression	none zlib@openssh.com	none zlib@openssh.com	none zlib@openssh.com

16.3. SNMPv3

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

16.4. 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 are used depending on the firmware version.

16.4.1. 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

16.4.2. 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

16.5. CIM/SMASH (iRMCS4 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

16.6. 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

17. Glossary

Certificate	An electronic document that contains a subject's public key 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 organization's internal network 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* (http://www.jboss.org/jbossas/)
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
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WBEM	Web-Based Enterprise Management - an initiative