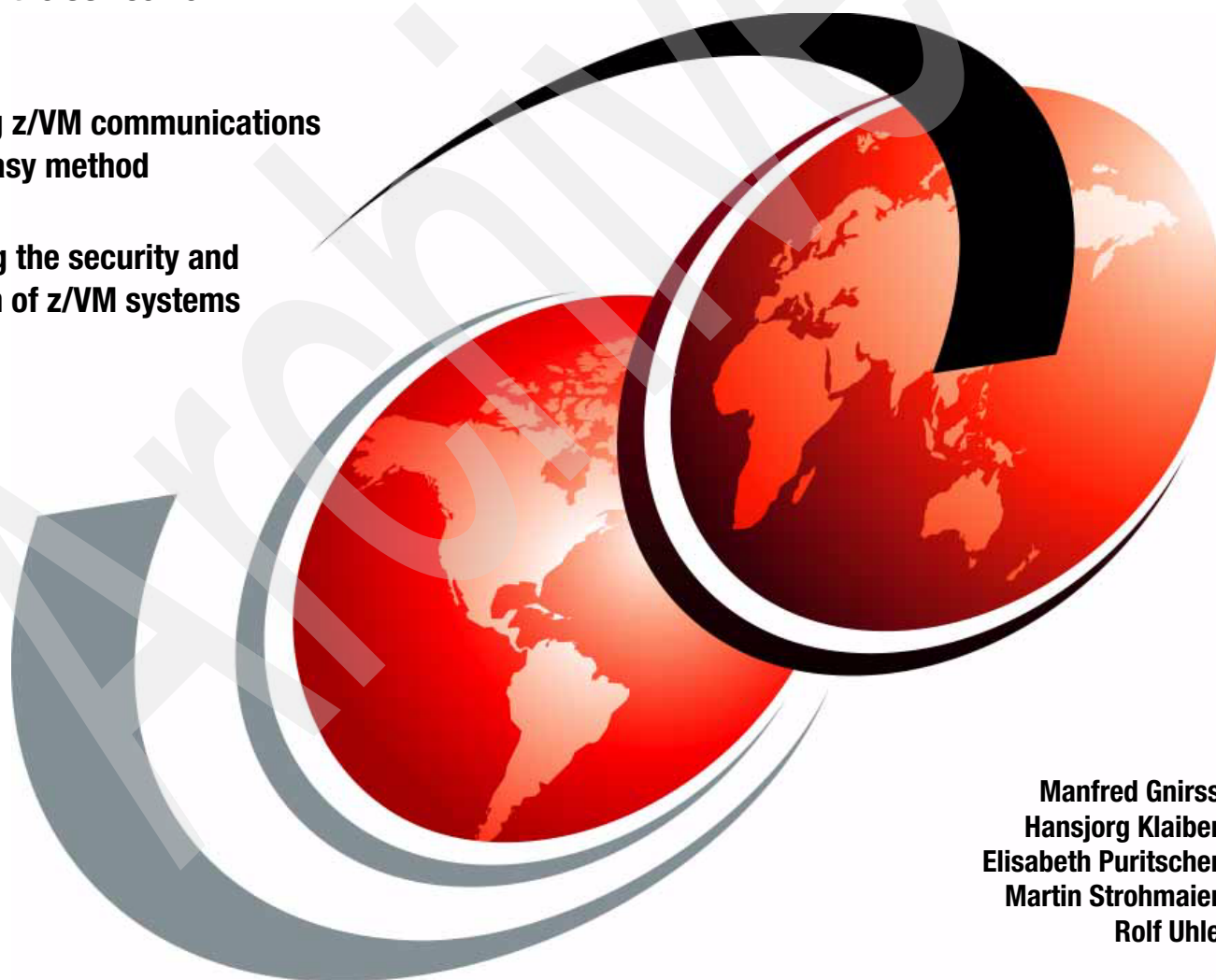


SSL Server Implementation for z/VM 5.2

Setting up the SSL server

Protecting z/VM communications
with an easy method

Increasing the security and
protection of z/VM systems



Manfred Gnirss
Hansjorg Klaiber
Elisabeth Puritscher
Martin Strohmaier
Rolf Uhle



International Technical Support Organization

SSL Server Implementation for z/VM 5.2

October 2007

Archived

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (October 2007)

This edition applies to Version 5, Release 2 of z/VM.

This document created or updated on October 18, 2007.

© Copyright International Business Machines Corporation 2007. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team that wrote this paper	vii
Become a published author	viii
Comments welcome	viii
Chapter 1. SSL Server overview	1
1.1 z/VM system layout	2
Chapter 2. Configuring Linux guest server for SSL	5
2.1 User directory entry	6
2.2 Providing the RPM package files to Linux	6
2.3 Installing the RPM package files	7
2.4 Configuration for the Linux server	7
2.4.1 Configuration for SUSE SLES8	7
2.4.2 Configuration for SUSE SLES9	9
2.4.3 Linux configuration for running z/VM SSL daemon (SUSE SLES8 and SUSE SLES9)	9
2.5 Re-establishing Linux network connectivity for service and update	10
Chapter 3. Configuring z/VM V5.2 for SSL	11
3.1 Customizing SSLSERV Profile	12
3.2 Updating the PROFILE TCPIP	12
3.3 Customizing ETC SERVICES	12
3.4 Updating the DTCPARMS file	14
Chapter 4. Setting up the certificate database	15
4.1 Start the SSL Server	16
4.2 Creating a self-signed certificate	17
4.3 Designating the secure ports	19
Chapter 5. Setting up IBM Personal Communications for SSL use	21
5.1 Installing a certificate on the client site (IBM Personal Communications Version 5.7) ..	22
5.2 Configuring 3270 sessions for SSL use	30
5.3 Using FTP client for secure file transfer	33
Appendix A. Miscellaneous	35
A.1 Determine cipher suites	36
A.2 Hardware encryption support	36
Related publications	37
Publications	37
Online resources	37
How to get IBM Redbooks publications	37
Help from IBM	37
Index	39

Archived

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.


This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®
z/OS®
z/VM®

z/VSE™
IBM®
Redbooks®

System z™

The following terms are trademarks of other companies:

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper publication gives a broad understanding of how to set up and configure the SSL server of z/VM® 5.2 in a short time frame. It also provides an easy method to protect the communication to z/VM server, especially for administrative tasks, thus increasing the total security and protection of the z/VM system. Sensitive information such as passwords from administrators are protected when accessing the system independently from the network.

This paper is designed for IT architects and system programmers that need clarification on how to use and set up this type of configuration.

The team that wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Poughkeepsie Center.

Manfred Gnirss is an IT specialist at the IBM Technical Marketing Competence Center (TMCC) and the Linux® Center of Competence, Boeblingen, Germany. Before joining the TMCC in 2000, he worked in z/VM and z/OS® development for more than 12 years. Currently he is involved in several Linux for System z™ Proof-of-Concept projects and customer projects running at the TMCC. Manfred holds a PhD in theoretical physics from the University of Tuebingen, Germany.

Hansjörg Klaiber is an expert for Linux for System z with more than 12 years Linux experience, and he was instrumental in the consolidation of distributed SAP® servers onto Linux for System z with Endress+Hauser. Since 2000, he has worked in System management with Endress+Hauser, and today he is responsible for all Linux on System z servers, including SAP Application servers.

Elisabeth Puritscher is an IT specialist at the IBM Technical Marketing Competence Center (TMCC) and the Linux Center of Competence, Boeblingen, Germany. She has an IT background for over 20 years and has extensive experience in the areas of z/OS, z/VM, z/VSE™, Linux for System z, and networking. Before joining IBM and the TMCC in 1999, she worked for consulting companies, where she was also active in the education of customers. Today she is managing the total TMCC environment, including all System z hardware and software installation, tuning, and debugging.

Martin Strohmaier is Senior Consultant at becom company, an IBM Business Partner in Germany. The last 30 years, he has worked at IBM Deutschland GmbH. He has experience in 370/390 Hardware and ITS Software Delivery running VSE under VM. Since 2000, he has been involved in several projects with SAP and LINUX on System z.

Rolf Uhle works in System Management with Endress+Hauser, Germany. He has more than 20 years experience in mainframe administration, and his many responsibilities include all of z/VM and z/OS systems as well as ADSM and TCP/IP. He was one of the key experts during the introduction of Linux on System z for SAP consolidation with Endress+Hauser.

Thanks also to the following people for their contributions to this project:

- ▶ Erich Amrehn
IBM Boeblingen
- ▶ Joel Hermann
IBM Boeblingen

Special thanks to the Endress+Hauser and becom companies for helping during the writing and testing of the paper.

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an e-mail to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

SSL Server overview

Depending on the security policy in an enterprise and depending on the network environment, customers might want to use secure (encrypt) communication for their connections to z/VM guest user IDs to avoid sending passwords in clear text over a network and to protect also the content of the communication.

In this paper, we describe how to set up and configure Secure Socket Layer (SSL) communication for z/VM users in a z/VM Version 5.2 system.

Note: This paper provides an overview of the topic. It is intended that you use this paper as supplemental information to the z/VM official documentation.

1.1 z/VM system layout

The SSL server that runs in the SSLSERV virtual machine provides processing support for secure (encrypted) communication between remote clients and z/VM TCP/IP servers that listen on secure ports. The SSL server manages the database in which the server authentication certificates are stored. The TCP/IP (stack) server routes requests for secure ports to the SSL server. The SSL server, representing the requested application server, participates in the handshake with the client in which the cryptographic parameters are established for the session. The SSL server then handles all the encryption and decryption of data.

Figure 1-1 illustrates the principal setup and information.

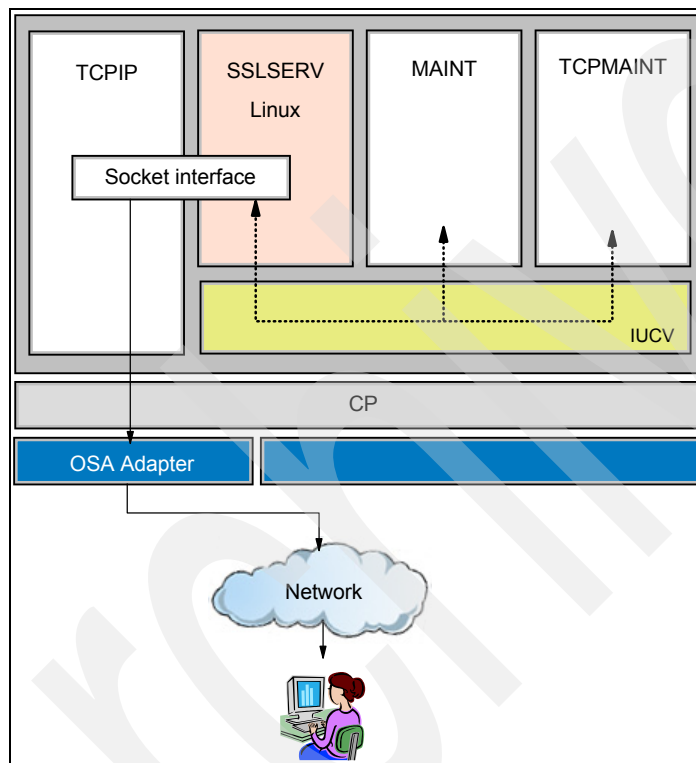


Figure 1-1 z/VM 5.2 system with SSLSERV and several VM administrator users

The SSL server is a *virtual service machine*, which is a special Linux server installed and configured for exclusive use of SSL. Only specific Linux distributions and kernel levels are supported for this purpose.

For details and official instructions about z/VM, see the z/VM IBM Web page, which is available at:

<http://www.vm.ibm.com/related/tcpip/>

On this page you can find the link to SSL Server Configuration where all related information is available:

<http://www.vm.ibm.com/related/tcpip/vmsslinfo.html>

Especially check whether there are important service updates that might include new information such as necessary PTFs and APARs. Check this site for the latest information before you begin your implementation.

You must transfer and install two RPM package files (appropriate for the chosen Linux distribution) on the Linux guest that you select to run the z/VM SSL server:

- ▶ An IBM GSKit RPM package
- ▶ An SSL server RPM package

Table 1-1 and Table 1-2 list the available RPM packages and the distributions for which they apply.

Table 1-1 IBM GSKit package information

Linux environment	z/VM supplied RPM file	Linux RPM package file
31-bit environment	IBMGSK RPMBIN	gskbas-7.0.13.s390.rpm
64-bit environment	IBMGSKX RPMBIN	gskbas-7.0.13.s390x.rpm

Table 1-2 SSL RPM package information

Linux distribution	z/VM supplied RPM file	Linux RPM package file
SUSE SLES8 SP3 31-bit environment	VMSS8 rpmbin	vmssld-2.24.21-1.s390.rpm
SUSE SLES9 SP2 31-bit environment	VMSS9 rpmbin	vmssld-2.6.5-1.s390.rpm
SUSE SLES9 SP2 64-bit environment	VMSS9X rpmbin	vmssld-2.6.5-1.s390x.rpm
Red Hat Enterprise Linux AS3 U3 31-bit environment	VMSR3 rpmbin	vmssld-2.24.21-1.s390.rpm
Red Hat Enterprise Linux AS3 U3 64-bit environment	VMSR3X rpmbin	vmssld-2.24.21-1.s390x.rpm
Red Hat Enterprise Linux AS4 U2 31-bit environment	VMSR4 rpmbin	vmssld-2.6.9-1.s390.rpm
Red Hat Enterprise Linux AS4 U2 64-bit environment	VMSR4X rpmbin	vmssld-2.6.9-1.s390x.rpm

Note: If the Linux distribution that you select for running the SSL server is a more recent service level than cited in these tables, you must rebuild the **vmsock** kernel module locally. For details, check the z/VM SSL Server configuration Web site for rebuild information for **vmsock**:

<http://www.vm.ibm.com/related/tcpip/tcslvmsb.html>

The various SSL related RPM packages provided with TCP/IP for z/VM are supplied on the following minidisk of your z/VM 5.2 system:

Mdisk 493 of the User 5VMTCP20 (filetype RPMBIN)

The two RPM package files for GSKit and SSL Server must be transferred (FTP) and installed on the Linux guest that has been selected for running the z/VM SSL server.

Archived



Configuring Linux guest server for SSL

In this chapter, we describe how to set up the Linux virtual machine to act as an SSL Server. In our case, we used SUSE SLES 8 and SUSE SLES 9 distribution.

2.1 User directory entry

In the user directory of your z/VM 5.2 system, you can find a default entry for the SSLSERV machine. Use this guest user ID for the installation of your Linux system, which acts as an SSL server.

Example 2-1 shows our directory entry and the setup for the SSL server. The statements following * LINUX(SLES9) were added to the default entry (marked in bold type).

Example 2-1 Sample user directory entry

```
USER SSLSERV SSLSERV 128M 512M BG                                (storage may not exceed 2 GB)
  INCLUDE TCPCMSU
  IUCV ALLOW
  OPTION ACCT MAXCONN 1024 QUICKDSP SVMSTAT
  LINK 5VMTCP20 491 491 RR
  LINK 5VMTCP20 492 492 RR
  LINK TCPMAINT 198 198 RR
  LINK TCPMAINT 591 591 RR
  LINK TCPMAINT 592 592 RR
  LINK 5VMTCP20 493 493 RR(RPMBIN package files)
  MDISK 191 3390 6158 001 VZ1RES MR RSSLSERV WSSLSERV MSSLSERV
  MDISK 201 3390 6159 001 VZ1RES MR RSSLSERV WSSLSERV MSSLSERV
  MDISK 203 3390 6160 001 VZ1RES MR RSSLSERV WSSLSERV MSSLSERV (transition mdisk)
* LINUX(SLES9)
  MDISK 151 3390 0001 0850 LNX066 MR                                (root file system)
  MINIOPT NOMDC
  MDISK 152 3390 0851 2487 LNX066 MR                                (LVM)
  MINIOPT NOMDC
*
  DEDICATE E106 1A04                                (OSA Adapter )
  DEDICATE E107 1A05                                (OSA Adapter )
  DEDICATE E108 1A03                                (OSA Adapter )
*
  DEDICATE F100 FB06                                (Hipersockets – optional )
  DEDICATE F101 FB07                                (Hipersockets – optional )
  DEDICATE F102 FB08                                (Hipersockets – optional )
*
```

Note: The transition minidisk must be a CMS-formatted minidisk.

2.2 Providing the RPM package files to Linux

After Linux system is installed in the guest user SSLSERV, you need to transfer the RPM packages from the z/VM minidisk to your Linux system:

1. Log on to the user SSLSERV and IPL your LINUX system. Connect to your Linux using a telnet or ssh client. Log in with the root user on the selected Linux system (SSLSERV).
2. Initiate an FTP Session to the z/VM host where the needed RPMBIN package files reside:
ftp <vm_host_ip_address>

3. Log in with the user 5TCPIP20 (the default password is *5VMTCP20*):

```
user: 5vmtcp20
pass: <the_password>
cd 5vmtcp20.493
```

4. Establish binary transfer mode and retrieve the appropriate RPMBIN files:

```
bin
get <VM_IBMgskit_name.rpmbin> <Linux_IBMgskit_name.rpm>
get <VM_SSLpackage_name.rpmbin> <Linux_SSLpackage_name.rpm>
```

The names of the packages depend on the chosen distribution and whether you are using 31 or 64 bit environment.

5. Close the FTP Session after the files have been successfully transferred.

Attention: If in your environment the default password has not yet been changed, we recommend that you change it now.

2.3 Installing the RPM package files

To verify that you have packages that you can install, first issue the **rpm -I** commands:

```
rpm -qpi Linux_IBMgskit_name .rpm
rpm -qpi Linux_SSLpackage_name .rpm
```

Install the IBM GSKit package first, and then install the SSL server package:

```
rpm -Uvh Linux_IBMgskit_name .rpm
rpm -Uvh Linux_SSLpackage_name .rpm
```

To determine where the installation and readme files resides, issue the **rpm query** command:

```
rpm -qd Linux_SSLpackage_name .rpm
```

Examine the content of these files.

2.4 Configuration for the Linux server

You need to modify the Linux zIPL initial program loader file (zipl.conf) to identify the SSL server *transition* disk as one of the DASD to be used by Linux. There are small differences between SUSE SLES 8 and SUSE SLES 9 distribution on how to update the zIPL configuration. Therefore, we show these instructions separately.

2.4.1 Configuration for SUSE SLES8

When using SUSE SLES 8, use these steps to update the zIPL configuration:

1. Login as root user and change to the /etc directory:

```
cd /etc
```

2. Create a backup copy of the existing zIPL configuration file:

```
cp -p zipl.conf zipl.conf.org.nonvmssl
```

3. Determine the content of the current `zipl.conf` file:

```
cat zipl.conf
[defaultboot]
default=ipl
[ipl]
target=/boot/zipl
image=/boot/(kernel/newimage
#ramdisk=/boot/initrd
parameters="dasd=0152,0151 root=/dev/dasdb1 noinitrd"

[dumptape]
target=/boot
dumpto=/devrtibm0
```

In this sample of the `zipl.conf` file, the DASD device number is used for the IPL disk and device number 152 is used for some Linux space.

4. Create a modified copy of the `zipl.conf` file, which is used specifically for the SSL server configuration. The modified file must contain an updated `parameters=` entry that identifies the correct DASD device list. You can use any editor, for example `vi`, or the `sed` command in combination with I/O redirection:

```
sed s/0151/0151,203/ zipl.conf>zipl.conf.sslserv
```

In this example, the 203 device number corresponds to the Linux device file system name (that is *dasdc1*).

5. Verify the content of the modified `zipl.conf.sslserv` file:

```
cat zipl.conf.sslserv

...
[ipl]
target=/boot/zipl
image=/boot/(kernel/newimage
#ramdisk=/boot/initrd
parameters="dasd=0152,0151,203 root=/dev/dasdb1 noinitrd"
...
```

6. Return to the system root directory:

```
cd /
```

7. Write the modified initial boot information to the IPL device:

```
zipl -c /etc/zipl.conf.sslserv
```

8. Shut down and re-initialize Linux:

```
halt -n
system clear
ipl 151 clear
```

2.4.2 Configuration for SUSE SLES9

With Linux 2.6 a new device driver model has been introduced. Therefore configuring the transition disk to be online after IPL is lightly different in SUSE SLES 9.

1. Log in as the root user:

```
echo 1 > /sys/bus/ccw/devices/0.0.203/online
mkinitrd
zipl
```

2. Shut down and re-initialize Linux:

```
halt -n
system clear
ipl 151 clear
```

2.4.3 Linux configuration for running z/VM SSL daemon (SUSE SLES8 and SUSE SLES9)

After setting up the initial boot configuration and shutting down and re-IPLing, establish a telnet/ssh connection to the Linux system to set the mount point of the transition disk and to deactivate the general networking support of this Linux system for being prepared to run only as an SSL server.

Perform the following steps:

1. Log in as root, and create a backup copy of the existing `/etc/fstab` file:

```
cp -p /etc/fstab /etc/fstab.orig.backup
```

2. Modify the `/etc/fstab` file to identify the necessary mount point for the *transition* disk (mdisk 203):

```
echo "/dev/dasdc1 /opt/vmssl/parms ext2 defaults 1 1" >>/etc/fstab
```

3. Verify the content of the `/etc/fstab` file:

```
cat /etc/fstab

/dev/dasda1 swap swap defaults 0 0
/dev/dasdb1 / ext2 defaults 1 1
proc /proc proc defaults 0 0
# Entry for transition disk
/dev/dasdc1 /opt/vmssl/parms ext2 defaults 1 1
```

4. You need now to deactivate Linux Networking Support and establish symbolic links for automatic startup (and cancellation) of the z/VM SSL daemon program (`vmssl`). A utility script (`modsymlinks`) is provided in the `/opt/vmssl/bin` directory for this purpose. This script deactivates existing boot links in the `/etc/rc.d/rc{n}.d` directory (where `{n}` is the established runlevel) by renaming them and then creates those necessary for running `vmssl`.

```
cd /opt/vmssl/bin
```

```
./modsymlinks -m
```

This utility can also be used to restore links that were previously renamed through its use.

5. Shut down Linux:

```
halt -n
```

Now, Linux system is prepared for running as SSL server after it will be initialized again. The next step is to customize z/VM TCP/IP (see Chapter 3, “Configuring z/VM V5.2 for SSL” on page 11).

Note: After the SSL Server has been initialized using the z/VM VMSSL command, other Linux network functions such as telnet and ftp are no longer available for use.

2.5 Re-establishing Linux network connectivity for service and update

The following instructions are not part of the installation and configuration process for SSL server.

As mentioned previously, there is no more a general network connection available to the SSL server after it has been initialized via VMSSL command. In the case that you need to apply service/patches to Linux or to apply other changes to the SSL Server, you need to restore network access to the Linux server again. For this purpose, perform the following steps.

1. Log on to the z/VM SSL server user ID (SSLSESV) and stop automatic initialization. Then, issue this VMSSL command to set the z/VM SSL Server to an inactive state:

```
vmssl stop
```

2. After Linux has initialized, login through the 2370 console as the root user.
3. Reactivate Linux networking support and remove the symbolic links for automatic startup of the z/VM SSL daemon program:

```
cd /opt/vmssl/bin  
./modsymlinks -r
```

4. Shut down Linux and re-establish network connection:

```
halt -n
```

Modify the z/VM TCP/IP Configuration to gain again telnet/ssh access to the SSL Server Linux system. Then, re-initialize the SSL Server to an inactive state (using the `vmssl stop` command). Now it should be possible to establish FTP and telnet/ssh connections for performing the desired changes.

Configuring z/VM V5.2 for SSL

In this chapter, we describe how to configure SSL in a z/VM V5.2 environment. After installing the RPM packages and configuring the Linux system for a specific SSL server, you must perform the following configuration steps on the z/VM system:

- ▶ Customizing SSLSERV Profile
- ▶ Updating the PROFILE TCPIP
- ▶ Customizing ETC SERVICES
- ▶ Updating the DTCPARMS file

This chapter provides the details for these configuration steps.

3.1 Customizing SSLSERV Profile

Ensure that Linux is IPLed automatically when the SSLSERV user ID is started by TCP/IP. For this purpose, modify the profile of the SSLSERV user ID:

1. Log on as user SSLSERV and issue the following command to edit the user profile:

```
xedit profile exec a
```

2. Add statement VMSSL IPL 151:

```
/* SSLSERV Profile */  
'access 198 c'  
'access 591 e'  
'access 592 f'  
VMSSL IPL 151
```

3.2 Updating the PROFILE TCPIP

To update the PROFILE TCPIP, follow these steps:

1. Log on as user TCPMAINT.
2. Include the SSL server virtual machine user ID in the AUTOLOG statement of the TCP/IP server configuration file to start the SSL server automatically when TCP/IP is initialized.
3. Log on as user TCPMAINT again and verify that the following AUTOLOG statement was added to the PROFILE TCPIP:

```
AUTOLOG  
      SSLSERV 0 ; SSL Server
```

4. Verify that the following PORT statement is included in your TCP/IP Server configuration file and that this port matches the SSL administration port defined in the ETC SERVICES file:

```
PORT  
9999 TCP SSLSERV ; SSL Server - administration
```

3.3 Customizing ETC SERVICES

The ETC SERVICES file lists the Well Known Port Numbers as listed in RFC 1700. Verify that the ETC SERVICES file contains the following statement in the extensions section to define TCP port 9999 for SSL administration.

1. Log on as user TCPMAINT and issue the following commands:

```
acc 592 f  
acc 198 c  
copy etc sampserv f = services c  
xedit etc services c
```

2. Ensure that the following entry is defined and matches the port as defined in PROFILE TCP/IP:

```
ssladmin          9999/tcp          #administration port
```

```
ETC      SERVICES C1  V 80  Trunc=80 Size=1645 Line=49 Col=1 Alt=0
====>
T...+....1....+....2....+....3....+....4....+....5....+....6....+....7...
00049 rje          77/tcp      netrjs
00050 link        87/tcp      ttylink
00051 pop         109/tcp     postoffice pop2
00052
00053 # -----
00054 # IBM additions to RFC. May contain entries for sample programs,
00055 # experimental, or other non-standard services.
00056 # -----
00057
00058 # SSL
00059 ssladmin      9999/tcp      # administration port
00060 #
00061 # RVD service
00062 #
00063 rvd-control    531/udp      # rvd control port
00064 #
00065 # Andrew File System services
00066 #
00067 filesrv        2001/tcp
00068 console        2018/udp
00069 venus.itc      2106/tcp

MA  b 02/007
```

Figure 3-1 Sample of etc services file

3.4 Updating the DTCPARMS file

When you start the SSL Server, the TCP/IP server initialization program searches specific DTCPARMS files for configuration definitions that apply to this server. Tags that affect the SSL server are:

```
:NICK:SSLSERV:TYPE:SERVER      :CLASS:SSL
:NICK.SSL:TYPE:CLASS
      :NAME.SSL DAEMON
      :COMMAND:YES
      :DISKWARN.YES
      :PARMS.
```

```
SYSTEM  DTCPARMS C1  V 80  Trunc=80 Size=15 Line=0
====>
      |...+....1....+....2....+....3....+....4....+...
00000 * * * Top of File * * *
00001 .*****
00002 .* SYSTEM DTCPARMS
00003 .*****
00004 :NICK.TCPIP      :TYPE.SERVER
00005                :CLASS.STACK
00006 :NICK.VSWCTRL1  :TYPE.SERVER
00007                :CLASS.STACK
00008 :NICK.VSWCTRL2  :TYPE.SERVER
00009                :CLASS.STACK
00010 :NICK.SSLSERV     :TYPE.SERVER :CLASS.SSL
00011 :NICK.SSL        :TYPE.CLASS
00012                :NAME.SSL DAEMON
00013                :COMMAND.VMSSL
00014                :DISKWARN.YES
00015                :PARMS.
00016 * * * End of File * * *
```

Figure 3-2 Sample system DTCPARMS file

Setting up the certificate database

Under SSL protocol, the application server is always authenticated. To participate in an SSL session, an application server must provide a certificate to prove its identity. Server certificates are issued by Certificate Authority (CA). Server certificates and CA certificates are stored in a certificate database managed by the SSL server.

This chapter describes how to set up the certificate database in z/VM V5.2.

4.1 Start the SSL Server

Before you can issue `ssladmin` commands, the SSL Server must be running and TCPMAINT 591 must be accessed. If the server (SSLSERV) has not been autologged, you can start it manually. Follow these

Log on as TCPMAINT and issue the following commands:

```
acc 591 e
ssladmin query status
```

Figure 4-1 is an example of the `ssladmin` command output.

```
ssladmin query status
Maximum number of sessions: 100
Number of active sessions: 0
Administration port: 9999
Cipher_suites included :   RC4_128_SHA  RC4_128_MD5  3DES_168_SHA  RC2_128_MD5
DES_EXP1024_56_SHA  RC4_EXP1024_56_SHA  RC4_40_MD5  RC2_40_MD5  DES_56_SHA  NULL
_SHA  NULL_MD5  NULL
Cipher_suites exempted :
Trace Settings:
  Normal: OFF
  Connections: OFF
  Flow: OFF
  Address: 255.255.255.255:0
  Connection: 0

Ready; T=0.01/0.02 16:16:40
```

Figure 4-1 The `ssladmin status` command output

To see the certificates that are preloaded, issue the following command:

```
ssladmin query certificate *
```

Figure 4-2 shows an example of the command output.

```
Ready; T=0.01/0.01 15:46:47
ssladmin query cert
Labels are:

 1 - VMZ1SSL
 2 - EHCERT
 3 - Thawte Personal Premium CA
 4 - Thawte Personal Freemail CA
 5 - Thawte Personal Basic CA
 6 - Thawte Premium Server CA
 7 - Thawte Server CA
 8 - RSA Secure Server Certification Authority
 9 - VeriSign International Server CA - Class 3
10 - VeriSign Class 4 Public Primary Certification Authority - G3
11 - VeriSign Class 3 Public Primary Certification Authority - G3
12 - VeriSign Class 2 Public Primary Certification Authority - G3
13 - VeriSign Class 1 Public Primary Certification Authority - G3
14 - VeriSign Class 4 Public Primary Certification Authority - G2
15 - VeriSign Class 3 Public Primary Certification Authority - G2
16 - VeriSign Class 2 Public Primary Certification Authority - G2
17 - VeriSign Class 1 Public Primary Certification Authority - G2
18 - VeriSign Class 3 Public Primary Certification Authority

- MORE... VMZ1
```

Figure 4-2 Sample `ssladmin query certificate` output

4.2 Creating a self-signed certificate

An application server cannot participate in an SSL session unless a certificate for the server is in the certification database. To obtain a server certificate, create a label `X509INFO` file and issue the `ssladmin request` command to create a certificate request. Then, send the certificate request to a CA. In response to this request, the CA returns a server certificate that you must store in the certificate database. Depending on the owner of the CA, a providing server certificate signed by the CA is a *charged service* and might need some time. For testing purposes, a self-signed certificate is the fastest way to start. Because a self-signed certificate is not signed by an official CA, the client cannot use a real CA certificate to verify the server certificate. Therefore, you need to provide a copy of a self-signed certificate to the client.

In general, a self-signed certificate is not intended for production purposes, especially for accessing the server from a public network (that is the Internet).

To create a self-signed certificate, create an *fn* `X509INFO` file with XEDIT that includes information about the application server:

```
Logon TCPMAINT
Acc 198 c
X <fn> X509INFO C
```

In this command, *fn* is a meaningful file name. The format of an X509INFO file is:

```
Common common name
Organization organization
Unit unit
Locality city
State state
Country country
```

Figure 4-3 shows a simple example where EHDATA is used for *fn*.

```
EHDATA  X509INFO C1  F 80  Trunc=80 Size=3 Line=0 Col=1 Alt=0
====>
|...+...1...+...2...+...3...+...4...+...5...+...6...+...7...
00000 * * * Top of File * * *
00001 common vmz1.endress.com
00002 organization endress
00003 country de
00004 * * * End of File * * *
```

Figure 4-3 EHDATA X509INFO sample

When you create a self-signed certificate, you have to specify a label that will be associated with the certificate in the certificate database. This label cannot already exist in the database. In addition, this label is specified in the **PORT** statements in the TCP/IP configuration file that define the secure ports for the application server. Issue the **ssladmin self** command to create the self-signed certificate:

```
ssladmin self ehdata c 1024 EHCERT
```

In our case, the file *ehdata X509INFO C* contains information about the application server. A key size of *1024* is chosen for the public and private key to be generated and the label for the certificate is *EHCERT*.

The label for the certificate to be specified in the **ssladmin** command is case sensitive and is used in the **PROFILE TCPIP** in this way. The **ssladmin self** command stores the just created certificate in the certificate database and saves a copy in a CMS file. In our case it is **EHDATA X509CERT** on the minidisk 198 of user **TCPMAINT**.

To verify that a certificate with this label resides in the certificate database, issue the **ssladmin query** command:

```
ssladmin query certificate ehcert
```

A self-signed certificate is only valid for a limited time period (three years). However, for testing purposes this time period seems to be sufficient. The client (for example, IBM Personal Communications) must have a copy of the self-signed certificate before it sends a connection request to initiate a test of the SSL environment.

4.3 Designating the secure ports

You must update the TCP/IP server configuration to designate your secure ports and to associate them with the certificates you have stored in the certificate database. Update the appropriate line with the port of the TELNET client in the PORT section of the PROFILE TCPIP configuration file with the label (in our example EHCERT) of the certificate and the SECURE operand. Example 4-1 shows our configuration.

Example 4-1 PROFILE TCPIP example

```
; -----  
; Reserve ports for specific server machines.  Port values used are  
; those defined in RFC 1060, "Assigned Numbers"  
; -----  
; Note that the MPROUTE and RouteD servers cannot be concurrently used  
; with the same TCP/IP stack server.  
; -----  
PORT  
20  TCP FTPSERVE  NOAUTOLOG ; FTP Server  
21  TCP FTPSERVE                ; FTP Server  
23  TCP INTCLIEN SECURE EHCERT ; TELNET Server  
; 23  TCP INTCLIEN                ; TELNET Server  
25  TCP SMTP                ; SMTP Server  
53  TCP NAMESRV              ; Domain Name Server  
53  UDP NAMESRV              ; Domain Name Server  
; 67  UDP BOOTPD                ; BootP Server  
; 67  UDP DHCPD                ; DHCP Server  
69  UDP TFTP                ; TFTP (Trivial FTP) Server  
81  TCP PERFSVM  NOAUTOLOG ; FCON/ESA INTERNET SERVER  
111 TCP PORTMAP              ; Portmap Server  
111 UDP PORTMAP              ; Portmap Server  
143 TCP IMAP                 ; IMAP Server  
161 UDP SNMPD                ; SNMP Agent  
162 UDP SNMPQE              ; SNMPQE Agent  
512 TCP REXECD               ; REXECD Server (REXEC)  
514 TCP REXECD               ; REXECD Server (RSH)  
515 TCP LPSERVE              ; LP Server  
9999 TCP SSLSERV SECURE EHCERT ; SSL SERVER - ADMINISTRATION  
; 9999 TCP SSLSERV              ; SSL SERVER - ADMINISTRATION  
; 520 UDP MPROUTE  NOAUTOLOG ; Multiple Protocol Routing Server
```

After you have designated the secure port in TCP/IP server configuration file, you must activate these changes:

- To activate the changes dynamically, use the **obeyfile** command.
- To make the changes permanent, restart the TCP/IP (stack) server.

Now the SSLSERVER is active and a telnet/ssh connection can only be established if the client on the workstation (for example, IBM 3270 Personal Communications) includes the correct certificate. In z/VM you can only run one single telnet server, either secured or unsecured. Therefore, ensure that you have installed the SSL certificate for the telnet/ssh client on your workstation successfully before you activate secure communication in z/VM.

Archived

Setting up IBM Personal Communications for SSL use

In our installation, we used a self-signed certificate for a server certificate. Because a self-signed certificate is not signed by a known Certificate Authority (CA), the client cannot verify it automatically. Therefore, we had to store our server certificate (manually) in the certificate database of the client.

In this chapter, we describe the installation of the generated server certificate on the client site in IBM Personal Communications Version 5.7 running on a Windows® PC. For information about how to create the certificate, see 4.2, “Creating a self-signed certificate” on page 17.

5.1 Installing a certificate on the client site (IBM Personal Communications Version 5.7)

After a certificate is created, the certificate is located on the MINIDISK 198 of the USER TCPMAINT.

Copy the content of the certificate using the copy and paste function to your PC. Then, save it in a file or transfer it with FTP to any directory on your workstation.

Attention: Depending how you transfer the certificate to the PC, avoid including or inserting blank spaces at the end of the lines in the certificate. These additional blank spaces can make the certificate unusable for SSL through IBM Personal Communications.

In our example, the certificate is located in C:\redp-4348 as Certificate.txt. Example 5-1 shows our example certificate.

Example 5-1 Our example certificate

```
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIEQ99s+TANBgkqhkiG9w0BAQQFADA6MQswCQYDVQQGEWJk
ZTEQMA4GA1UEChMHZW5kcmVzczEZMBcGA1UEAxMQdm16MS51bmRyZXNzLmNvbTAe
Fw0wNjAxMzAxMzU4MTdaFw0wOTAxMzExMzU4MTdaMDoxCzAJBgNVBAYTAmR1MRAw
DgYDVQQKEwd1bmRyZXNzMRkwFwYDVQQDExB2bXoxLmVuZlZlZG91c3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC9d9rjH65bADQM6og+vgx5t0DM0QFvg7tR
MCKFoi3rh4rTX1ve98N6Xxjkme9XPpKyv0wKfABMymWz/TgttL2T2TefPi fITdDN
Dbs1uWevgKra00EaKORbhHe2rnimar99hR90EaL4XjrtAn+dT7NGpAiZNTwbGx+J
UePVGnDKxwIDAQABMA0GCSqGSIb3DQEBAUAA4GBAGutaaF1EtDTnd4tno4W9SNm
c0CkxcRLX9q03feVNNk5MSytBqu0dYTV70q704ZVeCNV0T5P2dNi9bwobXKCvonk
pAnpr0BBLmjEf51qiPSGpwpkpTdE6QMRfojlLLB79E2tPRvCBBUm2Cjrw7NPFHuU
KGnp09GPpy5cCfM48XZwv
-----END CERTIFICATE-----
```

Note that when you update IBM Personal Communications with its certificate database, you might need Windows administration rights.

To import the certificate into the key database of IBM Personal Communications, you have to invoke the Certificate Management utility. Follow these steps:

1. Click **Start** on your windows desktop. Then, click **All programs** → **IBM Personal Communications** → **Utilities** → **Certificate Management**. The IBM Key Management dialog box opens as shown in Figure 5-1.

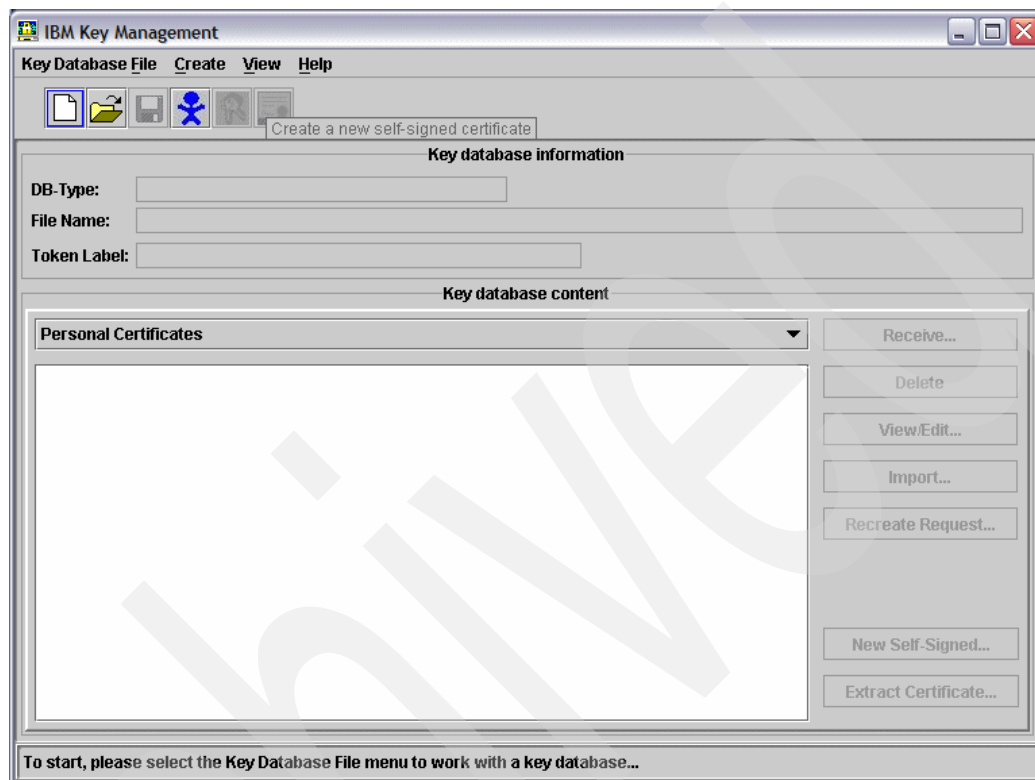


Figure 5-1 Key Management dialog box

2. Click **Key Database File** and then click **Open**. In the Open dialog box, specify the file name of the database that you want to open, as shown in Figure 5-2. In our example, we work with the default database. Click **OK**.

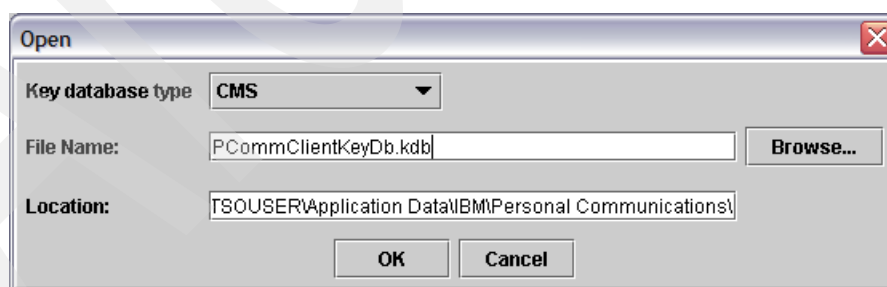


Figure 5-2 Open dialog box

3. Because the access to the data base is protected, you need to specify a password. If this is the first time that you are using this database, the default and initial password is *pcomm*. The utility might ask you to change the password. See Figure 5-3.

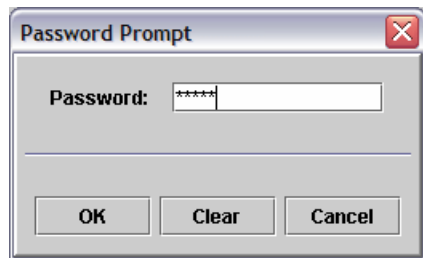


Figure 5-3 Database password verification

4. After the database is opened, you see a list of certificates that are included in the database (Figure 5-4). To import the certificate, you have to specify the file name where you have stored the certificate after downloading to your PC. Then, select **Add**.

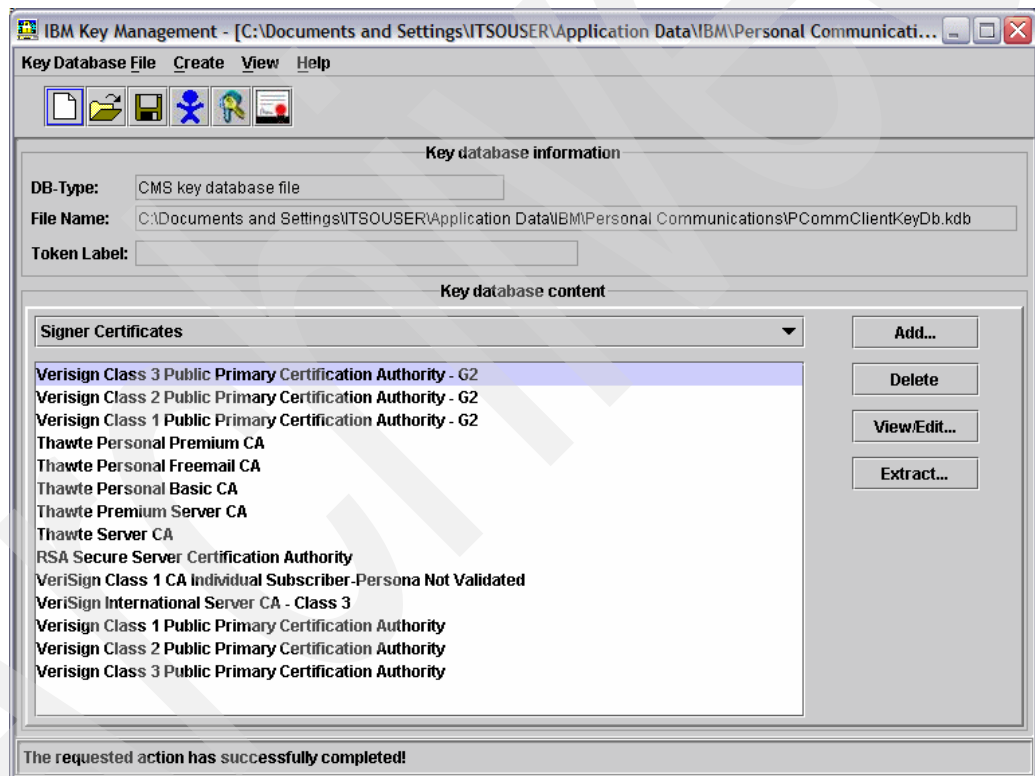


Figure 5-4 Adding a certificate

5. Select **Browse** to search for your certificate file (Figure 5-5).

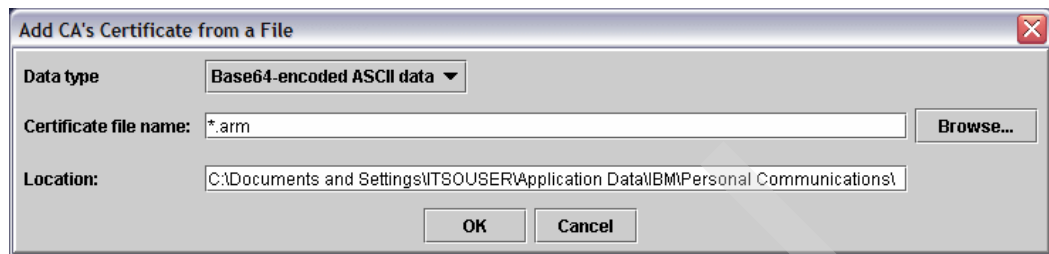


Figure 5-5 Looking for the certificate

6. Select **Files of type** and then select **All files (*.*)**, as shown in Figure 5-6.

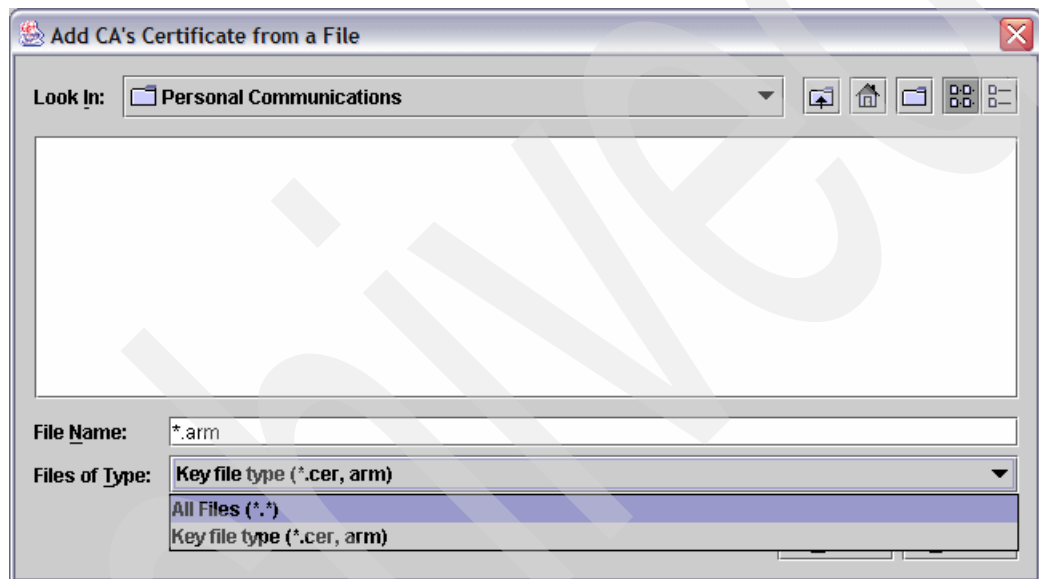


Figure 5-6 Searching for the certificate file

7. Then look for the appropriate folder where you have stored the certificate. Use the *Look In* area to locate and select your folder. See Figure 5-7.

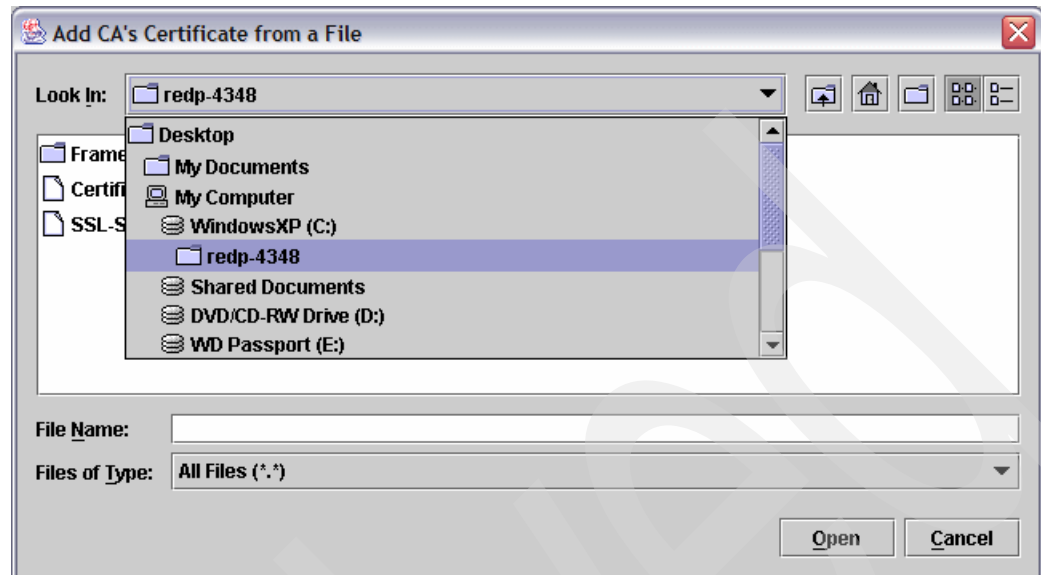


Figure 5-7 Selecting the certificate file

8. After you have selected the appropriate folder, select the file that includes the certificate (Figure 5-8).

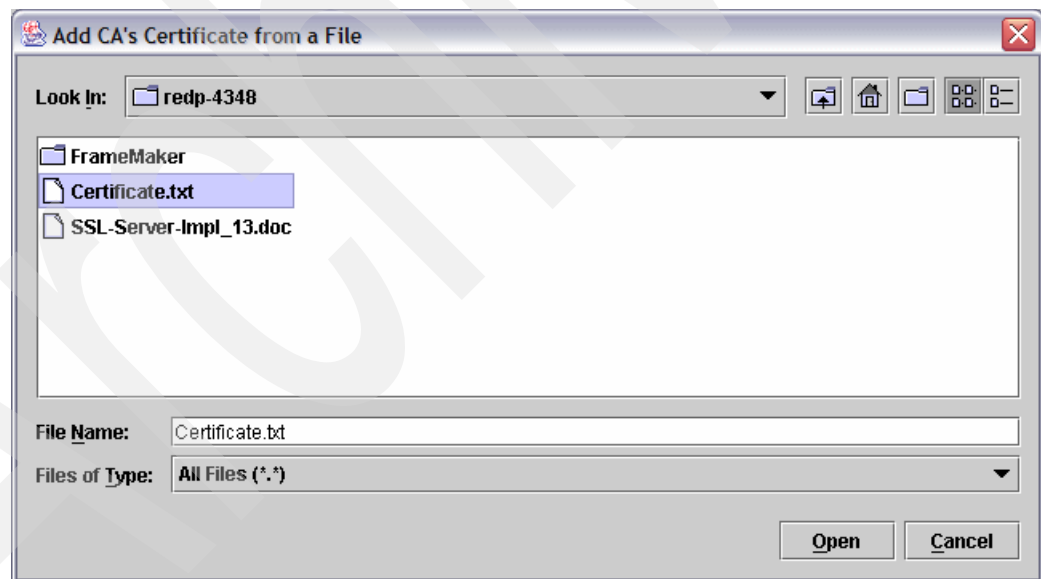


Figure 5-8 Certificate file to be imported

9. To start the import from this file, click **OK**. See Figure 5-9.

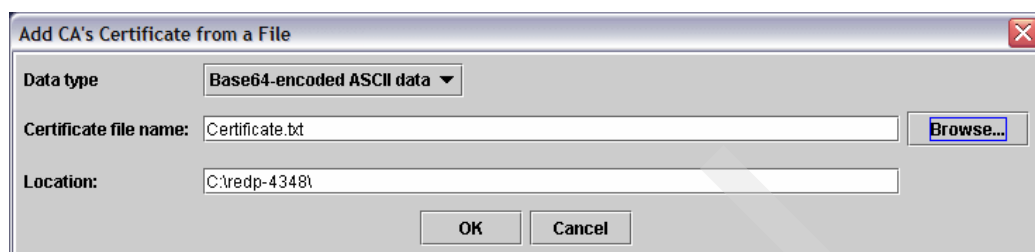


Figure 5-9 Importing the certificate

10. Provide a label for your certificate (Figure 5-10). In our example, we chose *ITSO certCC*. Then, click **OK**.



Figure 5-10 Labeling the certificate

11. The certificate is imported. Back in the main window, you see the imported certificate, including its label, as you specified. In addition, you find a success message in the bottom of the window. See Figure 5-11.

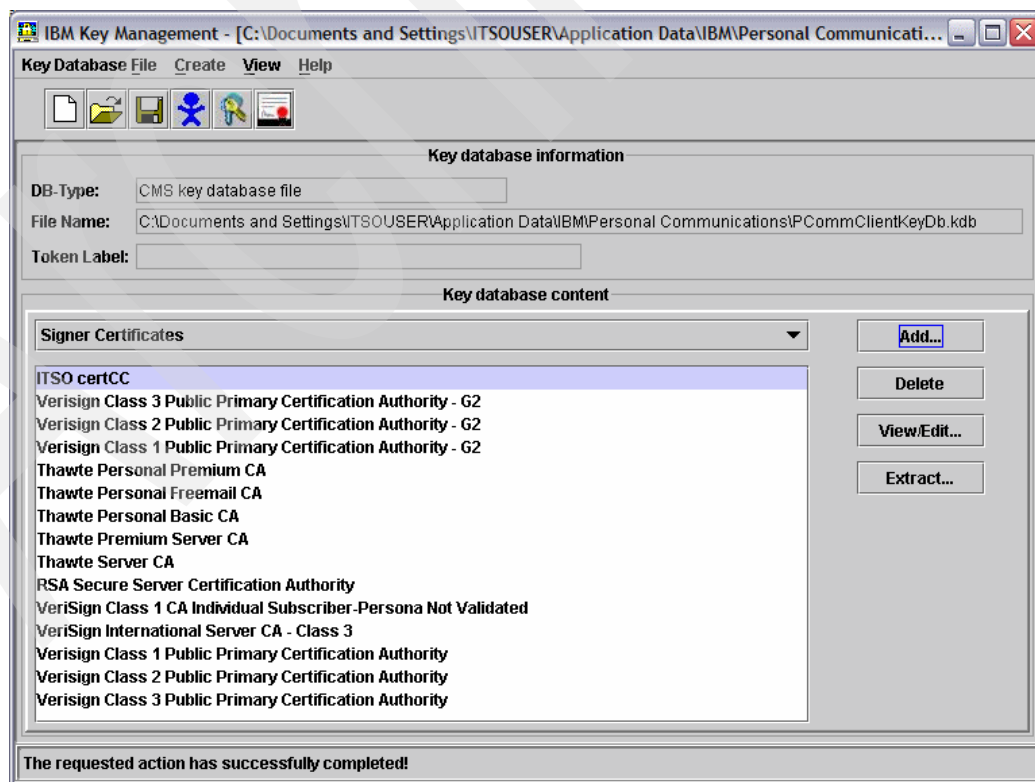


Figure 5-11 Certificate imported in the database

12. To check the result, verify the content of the certificate. Select the certificate and click **View/Edit**. In the resulting window, you can verify the key information including the fingerprint of the certificate, as shown in Figure 5-12.



Figure 5-12 Certificate content

13. You can check for more detailed information by selecting **Show Details**. You can check for any contained information like the general name or check the expiration date of the certificate, or check for the public key as shown in the example. See Figure 5-13.

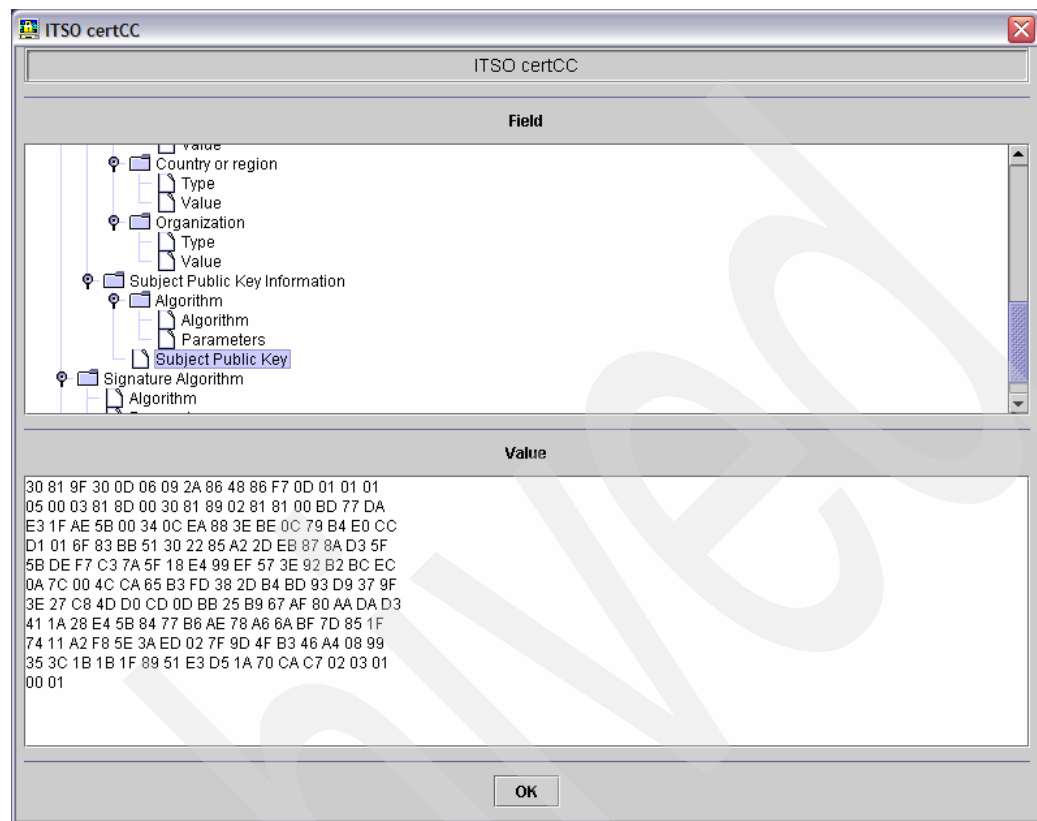


Figure 5-13 Certificate details

14. After selecting **OK** several times, you return to the main window of the utility. You can now close the key database and exit the program.

5.2 Configuring 3270 sessions for SSL use

After you have imported the certificate in your key database of IBM Personal Communications, you can configure a 3270 session to use for connecting to your z/VM system. To configure a session for use with SSL, click **Start** → **All Programs** → **IBM Personal Communications** → **Start or Configure Sessions**. In the Session Manager, select **New Session** and the Customize Communication dialog box opens, as shown in Figure 5-14.

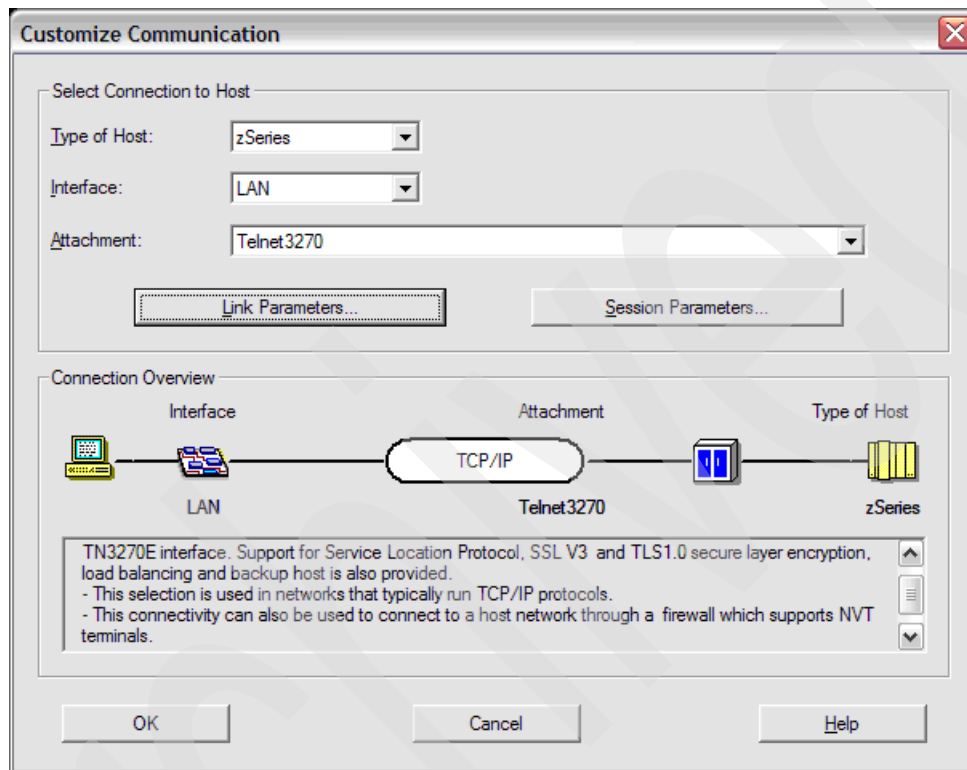


Figure 5-14 Customizing the communication session

Select **Link Parameters** and provide the host name or IP address of the z/VM server. Do not forget to select **Enable Security** so that this session uses Transport Layer Security (TLS) 1.0 or Secure Sockets Layer (SSL) V3 encryption. The telnet server to which the session connects must have SSL configured for this session.

You can use TLS and SSL security with or without the Service Location Protocol (SLP). If you enable both the SLP and Security, the session connects only if the SLP returns a telnet server on which Security is configured.

A valid site certificate, signed by a CA or self-signed, must reside on the workstation. If it does not, the session will not connect.

IBM Personal Communications has a keyring database in the application data directory specified when IBM Personal Communications is installed. The keyring database contains certificates from several trusted CAs. If the server is using a self-signed certificate or a certificate from an unknown CA, a copy of the self-signed certificate or of the CA's root certificate must be added to the client's database.

To save your settings, press **Apply** and then **OK** (Figure 5-15).

The screenshot shows the 'Telnet3270' dialog box with the 'Advanced Security Setup' tab selected. The dialog is divided into several sections:

- Host Definition:** Contains a table with columns 'Host Name or IP Address', 'LU or Pool Name', and 'Port Number'. It lists 'Primary', 'Backup 1', and 'Backup 2' hosts. The 'Primary' host has the IP address '9.152.123.14' and port '23'. 'Backup 1' and 'Backup 2' have empty fields and port '23'.
- Connection Options:** Includes a 'Connection Timeout' set to '6' seconds, an unchecked 'Auto-reconnect' checkbox, and a checked 'Try connecting to last configured host infinitely' checkbox.
- Printer Association (only valid for TN3270E Display sessions):** Features an 'Associated Printer Session' dropdown menu (currently empty) with a 'Browse...' button. Below it are two checked checkboxes: 'Start Associated Printer Minimized' and 'Automatically close the associated printer session with this session'.
- Enable Security:** A checked checkbox at the bottom of the main configuration area.
- Buttons:** 'OK', 'Cancel', 'Apply', and 'Help' buttons are located at the bottom right of the dialog.

Figure 5-15 Configuring the session

Using these definitions, you can now securely connect to your z/VM system (see Figure 5-16).

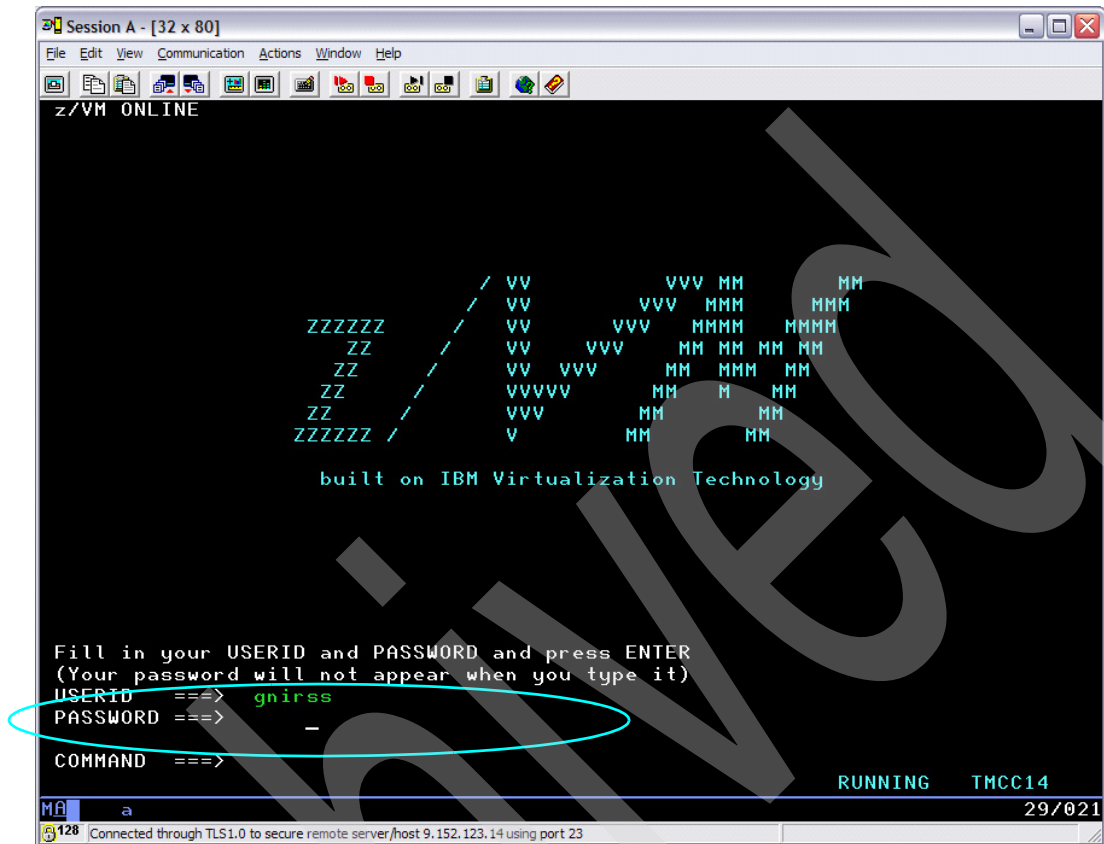


Figure 5-16 Connecting to the z/VM system

After connecting the server, the 3270 connection is already established in a secure mode, even before you have specified a user ID and password for your session. This can be seen in the status line at the bottom of the 3270 session window.

The z/VM administrator can verify with the **netstat co** command that the 3270 telnet sessions are routed via the service machine SSLSERV for encryption. Figure 5-17 is an example of the result of **netstat co** command.

VM TCP/IP Netstat Level 520				
Active IPv4 Transmission Blocks:				
User Id	Conn	Local Socket	Foreign Socket	State
INTCLIEN	1021	*..TELNET	*..*	Listen
INTCLIEN	1007	TMCC14..TELNET	9.152.140.126..1389	Established
PORTMAP	UDP	*..PMAP	*..*	UDP
PORTMAP	1001	*..PMAP	*..*	Listen
VSMERVE	1027	*..999	*..*	Listen
VSMERVE	1002	TMCC14..999	9.152.123.185..665	Established
VSMERVE	1023	TMCC14..999	9.152.123.185..801	Established
SSLSERV	1003	127.0.0.0..9999	*..*	Listen
SSLSERV	1030	*..1024	*..*	Listen
SSLSERV	1014	TMCC14..1024	9.152.140.126..1389	Established
SSLSERV	1026	TMCC14..4429	TMCC14..TELNET	Established
PERFSVM	1000	*..41785	*..*	Listen
PERFSVM	1009	TMCC14..41785	TMCC01..20518	Established
PERFSVM	1010	TMCC14..41785	9.152.123.12..45870	Established
PERFSVM	1028	TMCC14..41785	9.152.123.40..1025	Established
PERFSVM	1012	TMCC14..41785	9.152.123.16..1027	Established
PERFSVM	1008	TMCC14..41785	9.152.123.30..1156	Established
PERFSVM	1016	TMCC14..1027	TMCC01..41785	Established
PERFSVM	1020	TMCC14..1031	9.152.123.12..41785	Established
PERFSVM	1019	TMCC14..3799	9.152.123.16..41785	Established
PERFSVM	1022	TMCC14..4267	9.152.123.30..41785	Established
PERFSVM	1011	TMCC14..4268	9.152.123.30..41785	Established
MORE...				TMCC14

Figure 5-17 netstat co result

5.3 Using FTP client for secure file transfer

You can also configure FTP traffic to be encrypted through SSL by an appropriate definition in the TCP/IP server configuration (PROFILE TCPIP).

We performed our first tests successfully with the z/VM FTP client for secure file transfer to a z/VM Server. In addition, we used the WS_FTP client (in passive mode) from a Windows workstation to exchange data securely with the z/VM server.

When using specific FTP clients with SSL encryption and passive mode on a Linux or Windows workstations, you might face some issues (for example not being able to connect to the FTP server on z/VM). Most likely these issues are because z/VM 5.2 behaves according to RFC1123 and the client relies on RFC959. This situation might occur with clients that are working successfully with non-z/VM FTP servers. You can details on these issues in PMR 32063,075,724. If the issues persist, try a different FTP client.

Archived



Miscellaneous

This appendix describes additional tips that we noticed during the set up of our environment and that can be interesting for your installation.

A.1 Determine cipher suites

You can use the `ssladmin query status` command to verify which cipher suites are allowed for an SSL connection. Not all available cipher suites provide a high degree of security. Thus, we recommend that you consider carefully which suites to allow.

You might want to exempt individual cipher suites, such as NULL, NULL_SHA, or NULL_MD5, or you might want to instruct the SSL server to operate in Federal Information Processing Standard (FIPS) mode. For details, refer to *TCP/IP Planning and Customization*, Chapter 23 *VMSSL*, and `SSLADMIN` command.

A.2 Hardware encryption support

IBM System z also provides hardware support for encryption (CPACF for symmetric encryption and CryptoExpress 2 for RSA asymmetric encryption). This support can be used generally by Linux for System z servers. Today, the SSL server of z/VM does not use this capability.

Related publications

We consider the publications that we list in this section particularly suitable for a more detailed discussion of the topics that we cover in this paper.

Publications

This publication is also relevant as a further information source:

- ▶ *TCP/IP Planning and Customization*, SC24-6125

Online resources

This Web site is also relevant as a further information source:

- ▶ TCP/IP for VM Secure Socket Layer Server - Configuration Information and Requirements
<http://www.vm.ibm.com/related/tcpip/vmsslinf.html>

How to get IBM Redbooks publications

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Archived

Index

Numerics

5TCPIP20 7

C

certificate database 15, 21–22
 just created certificate 18
Certifying Authorities (CA) 15

E

example EHCERT 19

F

FTP Session 6

I

IBM Personal Communications
 Version 5.7 21
IP address 30

L

Linux 2.6 9
Linux distribution 3
Linux space 8
Linux system 6
 general networking support 9
Locality city 18

N

netstat co
 command 33
 result 33

O

OSA Adapter 6

P

Personal Communication (PC) 21
Port value 19
PROFILE TCPIP 12, 18, 33

R

Redbooks Web site 37
 Contact us viii

S

Secure Socket Layer (SSL) 1
Secure Sockets Layer (SSL) 30
server machine 19

 Reserve ports 19
Service Location Protocol (SLP) 30
SSL server 2, 5–6, 11, 15–16, 36
 configuration process 10
SSL session 15
SSLADMIN command 16, 36
SSLADMIN QUERY command 18
ssladmin query status 16
SUSE SLES 8 5
SUSE SLES8
 Configuration 7
System z
 server 36

T

TELNET client 19
telnet/ssh connection 10, 19
Transport Layer Security (TLS) 30

U

user TCPMAINT 18, 22

V

VMSSL command 10

Z

z/VM SSL 9
 daemon program 9
 server 3, 10
 Server configuration Web site 3
 server user ID SSLSERV 10
z/VM system 11, 30, 32

Archived



Redpaper™

SSL Server Implementation for z/VM 5.2

**Setting up the SSL
server**

**Protecting z/VM
communications with
an easy method**

**Increasing the
security and
protection of z/VM
systems**

This IBM Redpaper publication gives a broad understanding of how to set up and configure the SSL server of z/VM 5.2 in a short time frame. It also provides an easy method to protect the communication to z/VM server, especially for administrative tasks, thus increasing the total security and protection of the z/VM system. Sensitive information such as passwords from administrators are protected when accessing the system independently from the network.

This paper is designed for IT architects and system programmers that need clarification on how to use and set up this type of configuration.

**INTERNATIONAL
TECHNICAL
SUPPORT
ORGANIZATION**

**BUILDING TECHNICAL
INFORMATION BASED ON
PRACTICAL EXPERIENCE**

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

**For more information:
ibm.com/redbooks**

REDP-4348-00