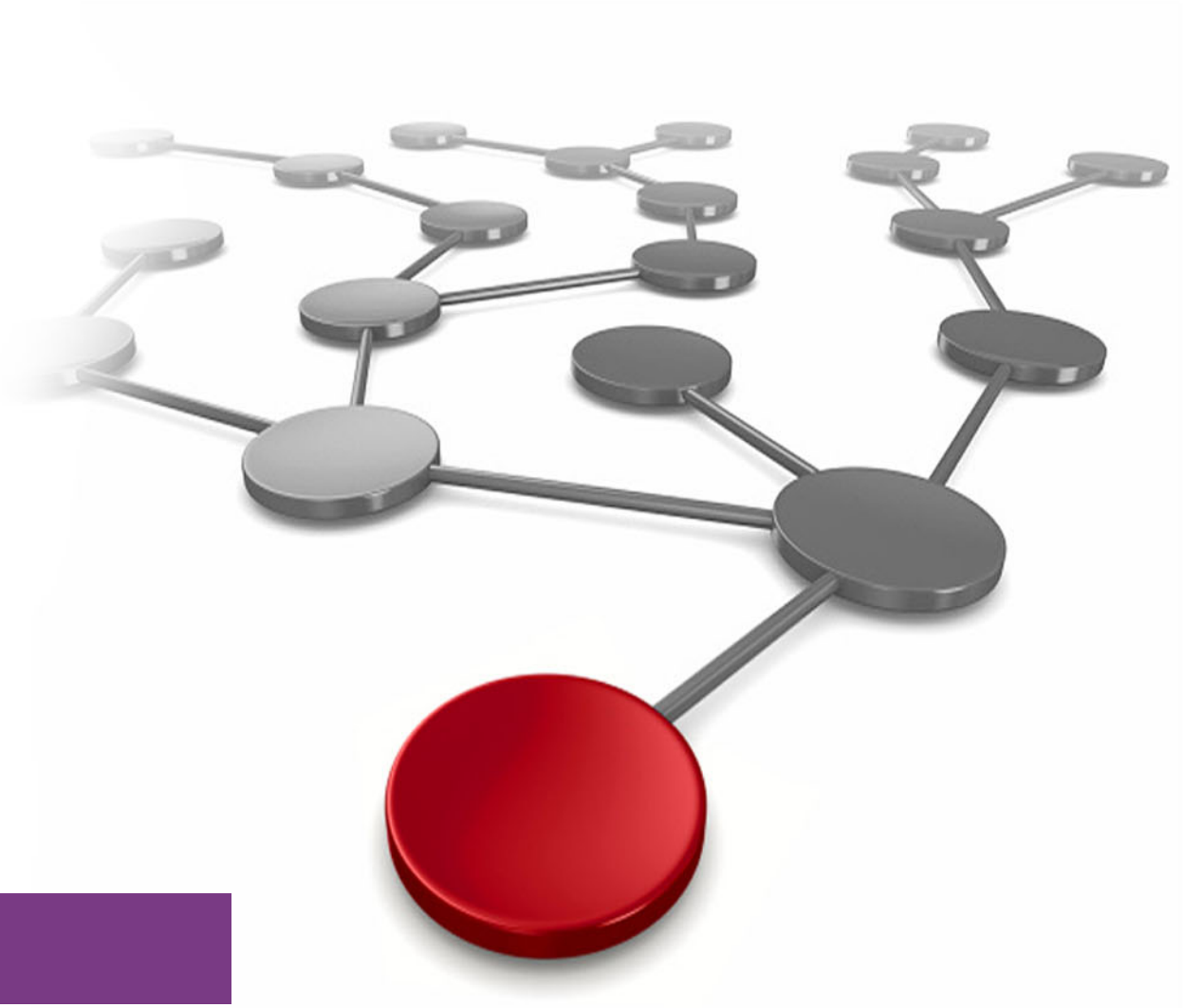
Redbooks
ibm.com/redbooks

IBM Personal Communications and IBM z/OS TTLS Enablement

Technical Enablement Series

Chris Van Wagner



IBM Z

IBM

IBM Systems Worldwide Client Experience Centers

Redpaper

IBM z/OS IBM Personal Communications TTLS Enablement

In this IBM Redpaper™ publication, we describe the process of introducing Transport Layer Security to IBM z/OS® so that IBM Personal Communications (PCOMM) uses TLS security.

This document describes enabling Tunneled Transport Layer Security (TTLS) on your IBM z/OS for use with a PCOMM TN3270 connection. When you complete this task, you need a certificate to access your TN3270 PCOMM session.

You work with the following products and components:

- TN3270
- TCP/IP
- PAGENT
- INET (maybe)
- IBM RACF®

We assume that the reader has extensive knowledge of z/OS security administration and of these products and components.

This document is part of the Technical Enablement Series that was created at the IBM Client Experience Centers.

Warning: Enabling PCOMM TTLS introduces the possibility that you lose access to your z/OS via PCOMM. Ensure that you have an alternative method to back out any changes that are made. In this study, the following back-door process was to be used if disaster occurs:

- Use an OSA-ICC connection to bypass TCP/IP/TN3270.
- For TN3270 changes, FTP configuration files that use native FTP were used. TCP/IP must be working to do this.
- Access to shared DASD from another z/OS combined with HMC access to issue console commands.

Overview

Figure 1 shows an overview of the steps that are described in this document.

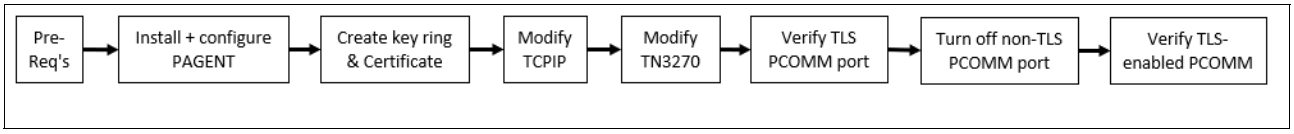


Figure 1 Steps to configuration

Figure 2 shows the changes that are introduced to your environment.

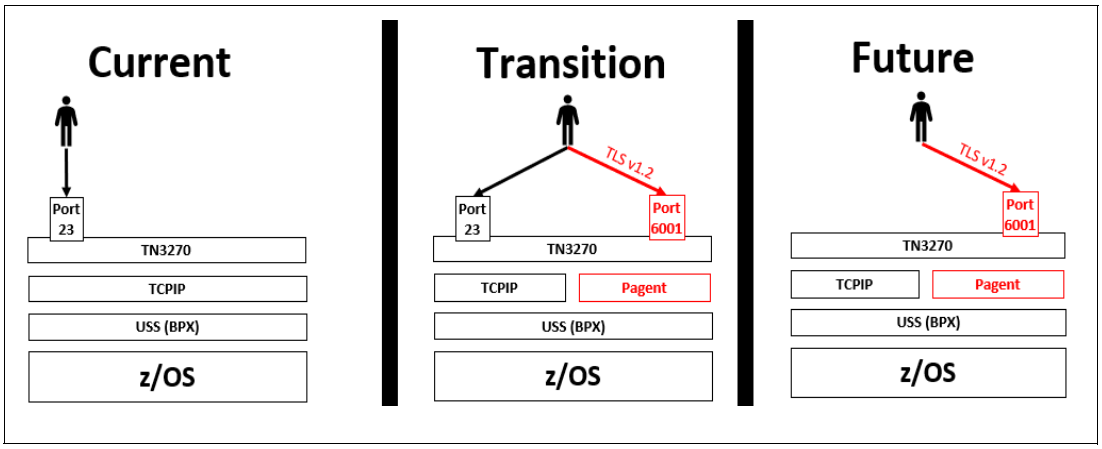


Figure 2 Updates to be made

Prerequisites

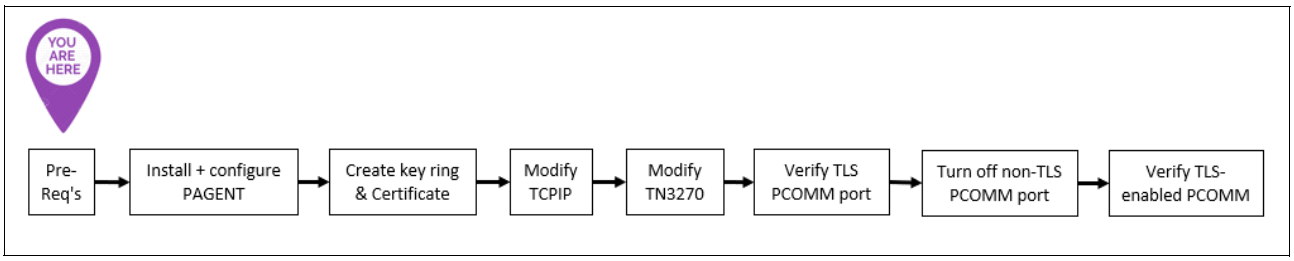


Figure 3 You are here: Prerequisites

You must have the following components successfully running:

- z/OS (this document was based on z/OS 2.3).
- UNIX System Services. This component of z/OS contains INET (you might have CINET).
- ICSF. You do not need a crypto card; instead, have ICSF running.
- TCP/IP is fully configured and successfully activated.
- TN3270 is fully configured and successfully serving a port to which you can connect with PCOMM.

You do not need to download any software or middleware. All of the instructions in this document are configuration-related.

Install and configure PAGENT

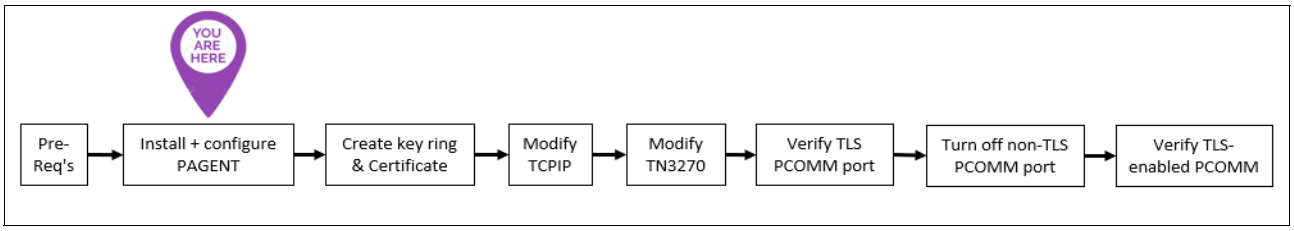


Figure 4 You are here: Install and configure PAGENT

Policy AGENT (PAGENT) is a started task that points to files that contain policy statements. PAGENT interacts with TCP/IP and INET. PAGENT uses a keyring and must be configured for TLS to work properly (see Figure 5).

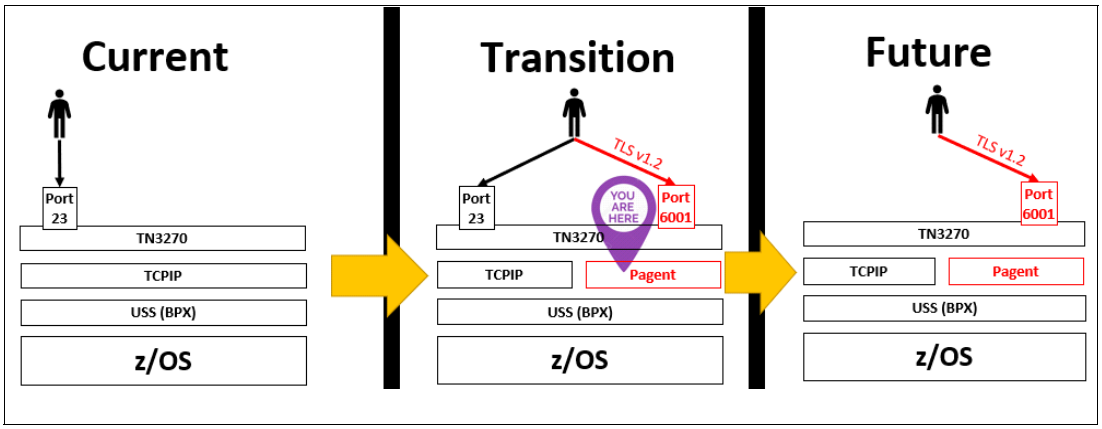


Figure 5 Transition stage

Creating the started task

The z/OS RES should include the PAGENT procedure. Copy `TCPIP.SEZAINST(PAGENT)` to `<hlq>.PROCLIB(PAGENT)`. The PAGENT PROC procedure is shown in Example 1.

Example 1 PAGENT PROC

```
//PAGENT   PROC
//PAGENT   EXEC PGM=PAGENT,REGION=OK,TIME=NOLIMIT,
// PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/-c /etc/pagent.conf'
//STDENV   DD PATH='/etc/pagent.env',PATHOPTS=(ORDONLY)
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

Creating the RACF STARTED profile

Ask your RACF administrator to create the PAGENT.** STARTED profile. Figure 6 and Figure 7 show how the RACF STARTED profile should look.

```
CLASS      NAME
-----      ----
STARTED    PAGENT.** (G)

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    SYS1            NONE             ALTER      NO

INSTALLATION DATA
```

Figure 6 RACF Started profile

```
USER      ACCESS
----      ------
STCGRP    ALTER
SYSPROG   ALTER

   ID     ACCESS  CLASS                E
-------- ------- -------- --------------
NO ENTRIES IN CONDITIONAL ACCESS LIST

STDATA INFORMATION
------------------
USER= STCSYS
GROUP= STCGRP
TRUSTED= YES
PRIVILEGED= NO
TRACE= NO
******************************** Bottom
```

Figure 7 RACF Started profile

Creating /etc/pagent.conf

A sample of the `/etc/pagent.conf` (see Example 2) is included with z/OS and can be copied by using the following commands:

```
cp /usr/lpp/tcpip/samples/pagent.conf /etc/pagent.conf
chown 775 /etc/pagent.conf
```

Example 2 /etc/pagent.conf

```
TTLSConfig /etc/pagent_TTLS.conf FLUSH PURGE
policyAction   networkcontrol
{
     policyScope    DataTraffic
     OutgoingTOS    11100000     # Precedence bits (first 3 bits)
}

policyAction   internetwork      # encapsulated network control
{
     policyScope    DataTraffic
     OutgoingTOS    11000000     #
}

policyAction   crit-realtime     # realtime data
{
     policyScope    DataTraffic
```

```
     OutgoingTOS    10100000     #
}

policyAction   interactive1
{
     policyScope    DataTraffic
     OutgoingTOS    10000000
}

policyAction   interactive2
{
     policyScope    DataTraffic
     OutgoingTOS    01100000
}
policyAction   batch1
{
     policyScope    DataTraffic
     OutgoingTOS    01000000
}

policyAction   batch2
{
     policyScope    DataTraffic
     OutgoingTOS    00100000
}
```

Creating /etc/pagent.env

Example 3 shows an example of `/etc/pagent.env`. The TZ variable defines the local time zone.

Example 3 /etc/pagent.env

```
PAGENT_CONFIG_FILE=/etc/pagent.conf
PAGENT_LOG_FILE=/tmp/pagent.log
LIBPATH=/usr/lib
TZ=CST6CDT5
```

Creating /etc/pagent_TTLS.conf

z/OS provides a sample file for pagent_TTLS.conf in `/usr/lpp/tcpip/samples/pagent_TTLS.conf`.

Copy this sample to `/etc/pagent_TTLS.conf` by using the following commands:

```
cp /usr/lpp/tcpip/samples/pagent_TTLS.conf /etc/pagent_TTLS.conf
chown 775 /etc/pagent_TTLS.conf
```

Next, modify `/etc/pagent_TTLS.conf` to add your key ring. There are two critical configuration items in this file: the port `6001` and the ring `TN3270_ring`.

Example 4 shows an example of `/etc/pagent_TTLS.conf`.

Example 4 /etc/pagent_TTLS.conf

```
TTLSRule                          TN3270~1
{
  LocalAddr                       0.0.0.0/0
  RemoteAddr                      0.0.0.0/0
  LocalPortRange                  6001
  RemotePortRange                 1024-65535
  Direction                       Inbound
  Priority                        255
  TTLSGroupActionRef              gAct1~TN3270
  TTLSEnvironmentActionRef        eAct1~TN3270
  TTLSConnectionActionRef         cAct1~TN3270
}
TTLSGroupAction                   gAct1~TN3270
{
  TTLSEnabled                     On
}
TTLSEnvironmentAction             eAct1~TN3270
{
  HandshakeRole                   Server
  EnvironmentUserInstance         0
  TTLSKeyringParms
    {
      Keyring                     TN3270_ring
    }
}
TTLSConnectionAction              cAct1~TN3270
{
  HandshakeRole                   Server
  TTLSCipherParmsRef              cipher1~TN3270
  TTLSConnectionAdvancedParmsRef  cAdv1~TN3270
  CtraceClearText                 Off
  Trace                           2
}
TTLSConnectionAdvancedParms       cAdv1~TN3270
{
  SSLv3                           Off
  TLSv1                           Off
  TLSv1.1                         Off
  ApplicationControlled           On
  SecondaryMap                    Off
  TLSv1.2                         On
}
TTLSCipherParms                   cipher1~TN3270
{
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_256_GCM_SHA384
  V3CipherSuites                  TLS_RSA_WITH_AES_256_CBC_SHA256
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DHE_DSS_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_DH_DSS_WITH_AES_256_CBC_SHA
  V3CipherSuites                  TLS_RSA_WITH_AES_256_CBC_SHA
```

```
  V3CipherSuites                  TLS_RSA_WITH_AES_128_GCM_SHA256
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_128_GCM_SHA256
  V3CipherSuites                  TLS_RSA_WITH_AES_128_CBC_SHA256
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_128_CBC_SHA256
  V3CipherSuites                  TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DHE_DSS_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DH_RSA_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_DH_DSS_WITH_AES_128_CBC_SHA
  V3CipherSuites                  TLS_RSA_WITH_AES_128_CBC_SHA
}
```

Granting access privileges

Use the following commands to grant access privileges to the files you created:

```
chmod 775 /etc/pagent.env
chmod 775 /etc/pagent.conf
chmod 775 /etc/pagent_TTLS.conf
```

Starting the PAGENT proc

Use the following command to start the PAGENT PROC:

```
/s pagent
```

The results should be similar to the results that are shown in Figure 8 on page 7.

```
VANWAG   00000290  S PAGENT
STC00198 000002B1  $HASP100 PAGENT   ON STCINRDR
STC00198 00000290  IEF695I START PAGENT   WITH JOBNAME PAGENT   IS ASSIGNED TO USER STCSYS
                    , GROUP STCGRP
STC00198 000002B1  $HASP373 PAGENT   STARTED
STC00198 00000090  EZZ8431I PAGENT STARTING
STC00198 00000090  EZZ8432I PAGENT INITIALIZATION COMPLETE
STC00006 00000090  EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP
                   KDEBEGRPACT
STC00198 00000090  EZD1579I PAGENT POLICIES ARE NOT ENABLED FOR TCPIP : TTLS
STC00198 00000090  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : QOS
STC00198 00000090  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
STC00198 00000090  EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP
STC00006 00000090  EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP
                   XDEBEGRPACT
```

Figure 8 PAGENT startup

The task should remain up. Check SYSLOG for RACF errors (see Figure 9).

```
 STATUS DISPLAY ALL CLASSES
AND INPUT ===>
 JOBNAME  JobID    Owner    Prty Queue      C Max-R
 PAGENT   STC00198 STCSYS     15 EXECUTION
```

Figure 9 SYSLOG

To see if the startup was successful, review the `/tmp/pagent.log` file. An example of a successful PAGENT startup is shown in Example 5.

Example 5 Successful PAGENT startup

```
04/24 12:20:07 LOG    :000: .main: EZZ8431I PAGENT STARTING
```

```
04/24 12:20:07 INFO   :000: .main: Compiled on Sep 26 2016 at 18:37:59
04/24 12:20:07 INFO  :000: .main: Use environment PAGENT_CONFIG_FILE = '//'SYSL.ZLP7.TCPPARMS(PAGCNF)''
04/24 12:20:07 INFO   :000: .main: List all environment variables:
04/24 12:20:07 INFO   :000: .main:   EXPORT '_CEE_ENVFILE_S=DD:STDENV'
04/24 12:20:07 INFO  :000: .main:  EXPORT 'PAGENT_CONFIG_FILE=//'SYSL.ZLP7.TCPPARMS(PAGCNF)''
04/24 12:20:07 INFO   :000: .main:   EXPORT 'PAGENT_LOG_FILE=/tmp/pagent.log'
04/24 12:20:07 INFO   :000: .main:   EXPORT '_BPXK_SETIBMOPT_TRANSPORT=TCPIP'
04/24 12:20:07 INFO   :000: .main: using code page 'IBM-1047'
04/24 12:20:07 INFO   :000: .main: Using log level 3
04/24 12:20:07 LOG   :000: main: EZZ8432I PAGENT INITIALIZATION COMPLETE

04/24 12:20:07 LOG   :005: pzos_install_A_ServiceClass: increase varsize for new gsk advanced parms
04/24 12:20:07 LOG   :005: pzos_install_A_ServiceClass: increase varsize for new gsk advanced parms
04/24 12:20:07 LOG   :005: pzos_install_A_ServiceClass: increase varsize for new gsk advanced parms
04/24 12:20:07 LOG   :005: pzos_install_A_ServiceClass: increase varsize for new gsk advanced parms
04/24 12:20:07 LOG    :005: instantiate_policies: EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR
TCPIP : TTLS

04/24 12:20:07 LOG    :005: instantiate_policies: EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR
TCPIP
```

Stopping and modifying the proc: To stop the proc, use the following command:

```
/p pagent
```

To modify the proc, use the following command:

```
/f pagent,refresh
```

INET or CINET start up errors

You might encounter errors when PAGENT is activated, as shown in the following example:

```
EZZ4248E TCPIP WAITING FOR PAGENT TTLS POLICY
```

If you encounter this type of error, go to UNIX and the `/etc/pagent.log` and browse for error messages. These messages often provide useful information.

The following messages indicate a problem that is related to INET:

```
SYSERR :001: plfm_kernel_init: socket(INET, DGRAM, 0) failed, errno=EDC5112I
Resource temporarily unavailable., errno2=112B00B6

OBJERR:001:init_PEP_and_kernel:Kernelinitializationfailedforimage'TCPIP',

OBJERR :001: check_main_config_file: PEP/kernel initialization failed for image
'TCPIP', config processing thread NOT created
```

INET is configured in `<hlq>.PARMLIB(BPXPRMxx)`. The change to BPXPRMxx is shown in Figure 10 and an IPL often corrects the problem.

```
BROWSE    SYSL.ZLP7.PARMLIB(BPXPRM00) - 01.04      Line 0000000114 Col 0(
Command ===> ____________________________________________ Scroll ===
  FILESYSTYPE TYPE(INET) ENTRYPOINT(EZBPFINI) /* TCP remote sockets */
  SUBFILESYSTYPE NAME(&TCPIPROC) TYPE(INET)  ENTRYPOINT(EZBPFINI)
  NETWORK DOMAINNAME(AF_INET)
          DOMAINNUMBER(2)
          MAXSOCKETS(64000)
          TYPE(INET)
          INADDRANYPORT(4901)
          INADDRANYCOUNT(100)
/* CVW - 2019-04-24 - Commented the following.                        */
/*NETWORK DOMAINNAME(AF_INET6)                                        */
/*        DOMAINNUMBER(19)                                            */
/*        MAXSOCKETS(64000)                                           */
/*        TYPE(INET)                                                  */
```

Figure 10 BPXPRM00 changes for INET

Verifying success

You are looking for two things at this point:

- No glaring errors in the PAGENT started task output.
- No errors in `/tmp/pagent.log`.

Figure 11 on page 9 shows an example of a successful PAGENT started task.

```
************************* TOP OF DATA ***************************************************
                 J E S 2  J O B  L O G  --  S Y S T E M  Z L P 7  --  N O D E  N 1

 STC00744 ---- WEDNESDAY, 24 APR 2019 ----
 STC00744  IEF695I START PAGENT   WITH JOBNAME PAGENT   IS ASSIGNED TO USER STCSYS  , GROU
 STC00744  $HASP373 PAGENT   STARTED
 STC00744  EZZ8431I PAGENT STARTING
 STC00744  EZZ8432I PAGENT INITIALIZATION COMPLETE
 STC00744  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : QOS
 STC00744  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
 STC00744  EZD1586I PAGENT HAS INSTALLED ALL LOCAL POLICIES FOR TCPIP
 STC00744  EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : TTLS
1 //PAGENT   JOB MSGLEVEL=1                                                STC00744
2 //STARTING EXEC PAGENT
3 XXPAGENT   PROC
4 XXPAGENT   EXEC PGM=PAGENT,REGION=0K,TIME=NOLIMIT,
  XX PARM='ENVAR("_CEE_ENVFILE=DD:STDENV")/-c /etc/pagent.conf'
5 XXSTDENV   DD PATH='/etc/pagent.env',PATHOPTS=(ORDONLY)
6 XXSYSPRINT DD SYSOUT=*
7 XXSYSOUT   DD SYSOUT=*
8 XXCEEDUMP  DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
  MESSAGE
2 IEFC001I PROCEDURE PAGENT WAS EXPANDED USING SYSTEM LIBRARY SYSL.ZLP7.PROCLIB
START PAGENT   WITH JOBNAME PAGENT   IS ASSIGNED TO USER STCSYS  , GROUP STCGRP
 PAGENT IS USING THE FOLLOWING JOB RELATED SETTINGS:
 SWA=ABOVE,TIOT SIZE=32K,DSENQSHR=DISALLOW,GDGBIAS=JOB
ALLOC. FOR PAGENT PAGENT
SMS HFS FILE ALLOCATED TO DDNAME STDENV
JES2 ALLOCATED TO SYSPRINT
JES2 ALLOCATED TO SYSOUT
JES2 ALLOCATED TO CEEDUMP
7C01 ALLOCATED TO SYS00001
  SYSL.ZLP7.PARMLIB                          KEPT
  VOL SER NOS= L7MCAT.
7C00 ALLOCATED TO SYS00004
  SYS1.TCPPARMS                              KEPT
  VOL SER NOS= L7RESA.
7C01 ALLOCATED TO SYS00005
  SYSL.ZLP7.PARMLIB                          KEPT
  VOL SER NOS= L7MCAT.
7C00 ALLOCATED TO SYS00007
  TCPIP.STANDARD.TCPXLBIN                    KEPT
  VOL SER NOS= L7RESA.
************************ BOTTOM OF DATA *****************************************************
```

Figure 11 Successful PAGENT started task

Check `/tmp/pagent.log` for the following key messages:

```
04/24 10:11:29 LOG    :000: .main: EZZ8431I PAGENT STARTING
```

```
04/24 10:11:29 LOG    :000: main: EZZ8432I PAGENT INITIALIZATION COMPLETE

04/24 10:11:30 LOG    :005: instantiate_policies: EZZ8771I PAGENT CONFIG POLICY
PROCESSING COMPLETE FOR TCPIP : QOS

04/24 10:11:30 LOG    :005: instantiate_policies: EZZ8771I PAGENT CONFIG POLICY
PROCESSING COMPLETE FOR TCPIP : TTLS
```

Rings, certificates, and certificate authorities

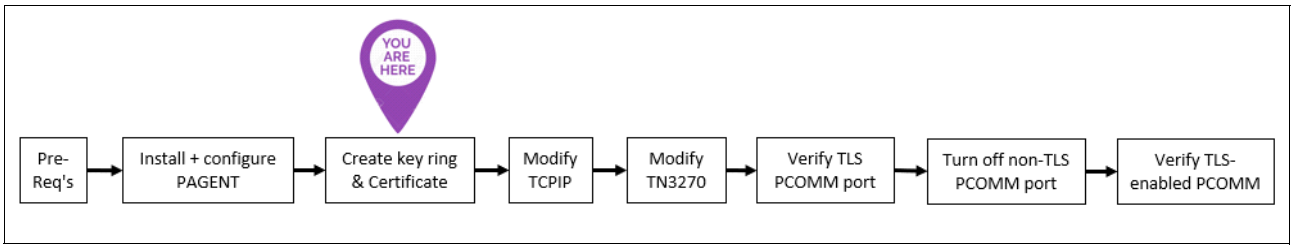


Figure 12 You are here: Ring administration

This section shows how to create a keyring, a certificate authority (CA) certificate that is connected to the keyring, and a personal certificate that is signed with the CA certificate, which also is connected to the keyring.

Creating a key ring, CA certificate, and a personal certificate

The job that is shown in Example 6 can be run to create the necessary key ring, a CA certificate as default, and a personal certificate that is signed with a CA certificate.

Warning: Use caution because this process deletes objects. Adjust the JCL as necessary to fit your system's configuration.

Example 6 JCL to create a key ring, CA certificate and personal certificate

```
//MAKECER2 JOB ,,MSGLEVEL=1,MSGCLASS=H,CLASS=A,REGION=0M
/*JOBPARM SYSAFF=*
//*********************************************************************
//* WARNING!  This job deletes rings and certificates!!!              *
//* ----------------------------------------------------------------- *
//* Job instructions:                                                 *
//*   1. Enter valid jobcard above.                                   *
//*   2. Change ++MY_KEYRING++ to your key ring name. Ex: TN3270_ring *
//*   3. Change ++MY_CA_CERT++ to your CA cert name. Ex: ZLP6_CA_cert *
//*   4. Change ++MY_CERT++    to your non-CA cer. Ex: ZLP6_cert      *
//*   5. Change ++HLQ++        to your personal HLQ on system.        *
//*   6. Change ++NOTBEFORE++  to a not-before date YYYY-MM-DD.       *
//*   7. Change ++NOTAFTER++   to a not-after  date YYYY-MM-DD.       *
//*   8. Submit. You should recieve RC=0 for every step.              *
//* ----------------------------------------------------------------- *
//* At the end of this job you should have the following:             *
//*    Keyring    : ++MY_KEYRING++                                    *
//*    CA Cert    : ++MY_CA_CERT++ (Connected to ring)                *
//*    Non-CA Cert: ++MY_CERT++    (Connected to ring)                *
```

```
//*    Data set   : ++HLQ++.CERTB64.CERT                              *
//* ---------------------------------------------------------------- *
//* C. Van Wagner  2019-05-03 Initial create.                         *
//*********************************************************************
//*********************************************************************
//* Delete CA Cert if it exists.                                      *
//*********************************************************************
//STEP010  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
  RACDCERT CERTAUTH DELETE(LABEL('++MY_CA_CERT++')) ID(STCSYS)

  SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
  SETROPTS RACLIST(FACILITY) REFRESH
/*
//*********************************************************************
//* Create CA Cert.                                                   *
//*********************************************************************
//STEP020  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
  RACDCERT CERTAUTH GENCERT -
  SUBJECTSDN( o('IBM Corporation') -
  ou('zBMC Certificate Authority') -
  C('US')) -
  NOTBEFORE(DATE(++NOTBEFORE++)) -
  NOTAFTER(DATE(++NOTAFTER++)) -
  KEYUSAGE(CERTSIGN) -
  WITHLABEL('++MY_CA_CERT++')

  SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
  SETROPTS RACLIST(FACILITY) REFRESH
/*
//*********************************************************************
//* Delete a non-CA Cert.                                             *
//*********************************************************************
//STEP030  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
  RACDCERT ID(STCSYS) DELETE(LABEL('++MY_CERT++')

  SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
  SETROPTS RACLIST(FACILITY) REFRESH
/*
//*********************************************************************
//* Create a non-CA certificate and reference the CA cert above.      *
//*********************************************************************
//STEP040  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT GENCERT ID(STCSYS) +
 SUBJECTSDN(CN('TN3270 Server')  +
 O('International Business Machines Corporation') C('US')) +
 SIZE(2048) NOTBEFORE(DATE(++NOTBEFORE++) TIME(11:00:00)) +
 NOTAFTER(DATE(++NOTAFTER++) TIME(11:00:00)) +
```

```
 WITHLABEL('++MY_CERT++') +
 RSA KEYUSAGE(CERTSIGN DATAENCRYPT HANDSHAKE) +
 SIGNWITH(CERTAUTH LABEL('++MY_CA_CERT++'))

 SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
 SETROPTS RACLIST(FACILITY) REFRESH
/*
//*********************************************************************
//* List the CA cert.                                                 *
//*********************************************************************
//STEP050  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT CERTAUTH LIST(LABEL('++MY_CA_CERT++'))
/*
//*********************************************************************
//* List the non-CA cert.                                             *
//*********************************************************************
//STEP060  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
  RACDCERT LIST(LABEL('++MY_CERT++')) ID(STCSYS)
/*
//*********************************************************************
//*********************************************************************
//* At this point, you should have two certificates:                  *
//*    1. CA cert                                                     *
//*    2. Non-CA cert which references the CA cert.                   *
//* Next, we will create a key ring and connect those certs.          *
//*********************************************************************
//*********************************************************************
//*********************************************************************
//* Delete key ring if it exists.                                     *
//*********************************************************************
//STEP070  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT ID(STCSYS) DELRING(++MY_KEYRING++)
/*
//*********************************************************************
//* Create a key ring.                                                *
//*********************************************************************
//STEP080  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT  ID(STCSYS) ADDRING(++MY_KEYRING++)
/*
//*********************************************************************
//* List the key ring.                                                *
//*********************************************************************
//STEP090  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT LISTRING(++MY_KEYRING++) ID(STCSYS)
/*
```

```
//*********************************************************************
//* CONNECT THE non-CA Cert TO THE RING.                              *
//*********************************************************************
//STEP100  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=0M
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT ID(STCSYS) CONNECT(LABEL('++MY_CERT++') -
          RING(++MY_KEYRING++) DEFAULT)
/*
//*********************************************************************
//* CONNECT THE CA Cert to the ring.                                  *
//*********************************************************************
//STEP110  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=0M
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT ID(STCSYS) CONNECT(CERTAUTH -
  LABEL('++MY_CA_CERT++') -
  RING(++MY_KEYRING++) -
   USAGE(CERTAUTH))

  SETROPTS RACLIST(DIGTCERT DIGTRING) REFRESH
  SETROPTS RACLIST(FACILITY) REFRESH
/*
//*********************************************************************
//* Display the key ring which should now have 2 certs connected.     *
//*********************************************************************
//STEP120  EXEC PGM=IKJEFT01,DYNAMNBR=30,REGION=4096K
//SYSTSPRT DD  SYSOUT=*
//SYSTSIN  DD  *
 RACDCERT LISTRING(++MY_KEYRING++) ID(STCSYS)
/*
//*********************************************************************
//*********************************************************************
//* At this point, you should have your key ring and certs connected. *
//* If you don't something went wrong.  Start over. Don't proceed.    *
//*********************************************************************
//*********************************************************************
//*********************************************************************
//* Export a non-CA cert to a file so it can be sent to your PC/MAC.  *
//* After you make TCPIP / TN3270 changes, this is the magic key that *
//* will permit you to authenticate with TN3270 (PCOMM).              *
//* Make sure you FTP this file to your PC in ASCII mode.  You can    *
//* also just copy/paste it.  It is small.                            *
//*********************************************************************
//STEP130  EXEC PGM=IKJEFT01,DYNAMNBR=50
//SYSLBC   DD   DSN=SYS1.BRODCAST,DISP=SHR
//SYSPRINT DD   SYSOUT=*
//SYSTSPRT DD   SYSOUT=*
//SYSTSIN  DD   *
  RACDCERT CERTAUTH   EXPORT(LABEL('++MY_CA_CERT++'))     -
     FORMAT(CERTB64) DSN('++HLQ++.CACERT.EXPORT') -
     PASSWORD('WELCOME')
/*
```

At the end of this job, you should have a key ring with the certificates as shown in Figure 13.

> **Important:** Be sure to review the results of the `RACDCERT LISTRING` command. Pay special attention to ensure that the CA cert is DEFAULT. This part of the process is critical.

```
RACDCERT LISTRING(TN3270_ring) ID(STCSYS)

Digital ring information for user STCSYS:

  Ring:
       >TN3270_ring<
  Certificate Label Name                Cert Owner     USAGE      DEFAULT
  ----------------------------------    ------------   --------   -------
  ZLP6_cert                             ID(STCSYS)     PERSONAL     YES

  ZLP6_CA_cert                          CERTAUTH       CERTAUTH     NO
```

Figure 13 Ring with connected certificates

Exporting the CA certificate

As shown in Example 6, you created a user certificate that is signed with a CA certificate and export the CA certificate to a flat file. Now, you must get that CA certificate to your PC where you can import it into a certificate management application. The certificate must be in the correct format. The exported file should look like the example that is shown in Figure 14.

```
BROWSE     VANWAG.CACERT.EXPORT                          Line 00000000
Command ===> ____________________________________________________________ Sc
******************************** Top of Data ******************************
-----BEGIN CERTIFICATE-----
MIIDmDCCAoCgAwIBAgIBADANBgkqhkiG9w0BAQsFADBMMQswCQYDVQQGEwJVUzEY
MBYGA1UEChMPSUJNIENvcnBvcmF0aW9uMSMwIQYDVQQLExp6Qk1DIENlcnRpZmlj
YXRlIEF1dGhvcml0eTAeFw0xOTA1MDEwNDAwMDBaFw00MDA1MDIwMzU5NTlaMEwx
CzAJBgNVBAYTAlVTMRgwFgYDVQQKEw9JQk0gQ29ycG9yYXRpb24xIzAhBgNVBAsT
GnpCTUMgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEA4GuNTYbIKLXjMzISoAFp80fu3UFJEz0n6sozJMQ2nPKupI2u
ST1Uag1uNLI2f+2becwgN5BmOtwu3qztqviNqbki8qj554+JhAijadSvNaL/iKBX
msezavO5BUdV63Sm3wkxnzF0TQtcJBnIU3xqgj8lM8c8IWCkiwEdTlbiyLIXWmkU
Lv/O2vf+DF4zfIatpZMGwERqAoHrSoLpmCEk1pkuXosA3hIlL/TBgiawZlZe0QCv
VhjTRfsfyny1G23wOW6nYSKHaTm1cqrBvnnga695WCypAniLHqpRf1XdVn5k1Kk8
xflu8MLsWS+LDC0VPzt7uz50s9P74l2mE7/WxwIDAQABo4GEMIGBMD8GCWCGSAGG
+EIBDQQyFjBHZW5lcmF0ZWQgYnkgdGhlIFNlY3VyaXR5IFNlcnZlciBmb3Igei9P
UyAoUkFDRikwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFFZA6/mqta1cC8komHTiHJysLeOFMA0GCSqGSIb3DQEBCwUAA4IBAQC+UOB4
dNnUW79IxoBhTIze6hPMy35hPth5C/odzRCwBuouaTPaEH5RpMOPDJL9iPg6N6Kz
fIef0U6DlYilASmsKGTT0UbdGYOD15UJqfHYnd7iH4t5SzATBgLeqCVEAmm5aZnQ
ivvfajASbckzN3RSezbsHpyh6/q/eJpzrA2E5zDcOe2miiT3O2WVbM43QIgYmiLS
rAMwobvOCR2nE8wCzTKOdJUg/QlhSMdRtM0DpFkpQWL3/zOOGn5mrUtNLH7LRcNQ
6Z1GL6pEZeTyr19fUQ1qvvgWFFbPzamjiO0d3v9sNPBmuSc/h0Q14e/WzkAyB3SH
n7kIo5i1sz6yoPZb
-----END CERTIFICATE-----
******************************** Bottom of Data ***************************
```

Figure 14 Exported CA certificate

Now, you can FTP that file in ASCII mode to your PC. You can also paste it into a notepad. Figure 15 shows the FTP of the file to the PC in ASCII format (not BIN).

```
ftp> open
To 129.40.110.225
Connected to 129.40.110.225.
220-FTP1 IBM FTP CS V2R3 at ex237n01.pbm.ihost.com, 18:00:21 on 2019-05-13.
220 Connection will close if idle for more than 5 minutes.
501 command OPTS aborted -- no options supported for UTF8
User (129.40.110.225:(none)): vanwag
331 Send password please.
Password:
230 VANWAG is logged on.  Working directory is "/u/vanwag".
ftp> get 'VANWAG.CACERT.EXPORT' C:\tmp\ZLP6_CA_cert.cer
200 Port request OK.
125 Sending data set VANWAG.CACERT.EXPORT
250 Transfer completed successfully.
ftp: 1328 bytes received in 0.00Seconds 1328000.00Kbytes/sec.
ftp> quit
```

Figure 15 FTP the flat file to the PC

The file is saved with a `.cer` extension. Verify that the file arrived successfully to the PC.

Importing the certificate to the PC

The next step is to import the certificate into your certificate database as a trusted certificate. Complete the following steps:

1. Click **Start** →**IBM® Personal Communication** →**Certificate Management.**

   This process starts a new window that is called IBM Key Management.

2. Open the Key Database file by clicking **Key Database File** →**Open** →**OK.**
3. Enter the password.
4. Click the **Add** button (see Figure 16).

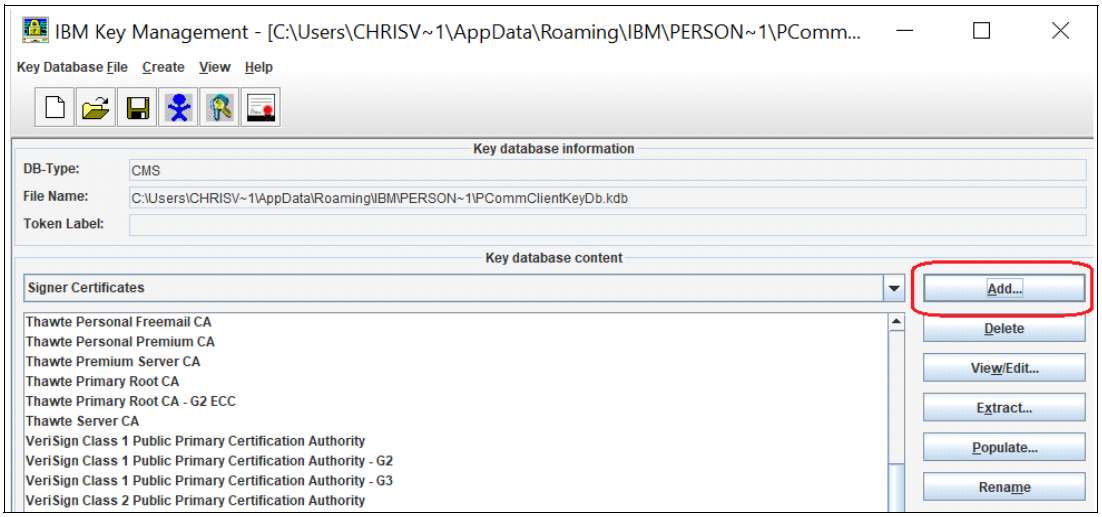


Figure 16 IBM Key Management

5. Find the `.cer` file that you transferred to your PC. Enter a name for the key when prompted. This name can be anything you want. In our example, we used `ZLP6_CA_cert` (see Figure 17). You receive a message that it was added successfully. Verify that the certificate is in the list.

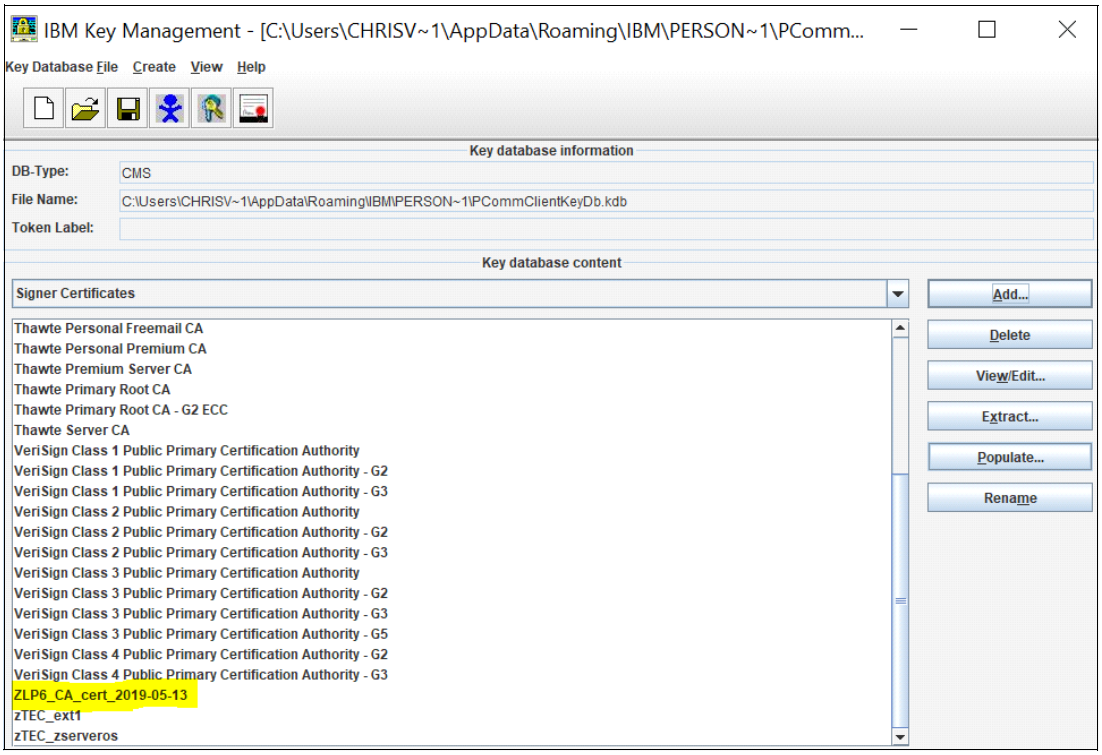


Figure 17 The new certificate is added

6. After you verify that the certificate is in the list, close the window. The configuration is automatically saved.

> **Tip:** If you encounter any errors with the Certificate Management application, restart your PC and attempt the import process again.

Checkpoint

At this time, you should have the following procedures and elements in place:

- PAGENT installed and running with no errors
- TN3270 running with no changes made
- TCP/IP running with no changes made
- A new key ring
- A new personal certificate and CA certificate created and connected to your key ring
- The new CA certificate on your PC and in your Certificate Management application

Modify TCP/IP

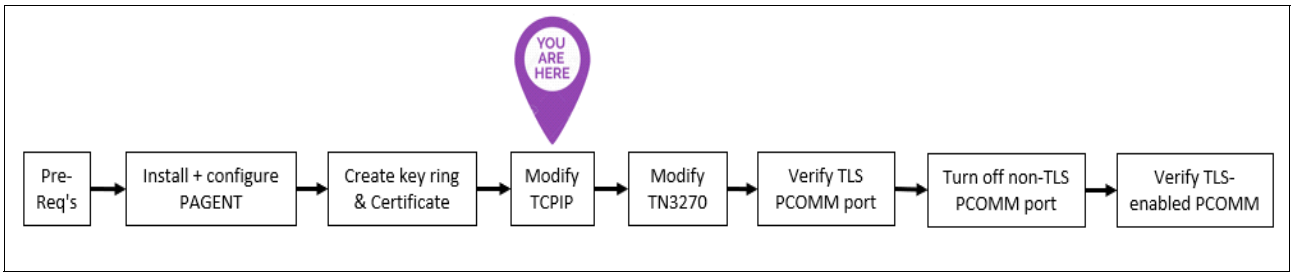


Figure 18 You are here: Modify TCP/IP

Warning: Use caution when you changing the TCP/IP. You should have a back out plan in case you make a change that prevents you from accessing the configuration. It is suggested that you have a back door to the system so that you can undo any changes.

In the test environment that is described in this document, we accessed the DASD from another z/OS and accessed the HMC. This combination permitted changes to be made to the system and recycle TCP/IP, if needed.

Identify your TCP/IP procedure and all associated configuration files. For this exercise, the examples that are shown in Example 7, Example 8 on page 17, Example 9 on page 18, Example 10 on page 19, and Example 11 on page 19 contain the TCP/IP procedure and files.

Example 7 <hlq>.PROCLIB(TCPIP)

```
//TCPIP    PROC PARMS='CTRACE(CTIEZB00)'
//TCPIP    EXEC PGM=EZBTCPIP,REGION=0M,TIME=1440,
//        PARM='&PARMS'
//STEPLIB  DD DSN=SYS9.VTAMLIB,DISP=SHR
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//ALGPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CFGPRINT DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSOUT   DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CEEDUMP  DD SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSERROR DD SYSOUT=*
//PROFILE  DD DISP=SHR,DSN=SYSL.&PROJECT..PARMLIB(PELPROF)
//SYSTCPD  DD DISP=SHR,DSN=SYSL.&PROJECT..PARMLIB(PELDATA)
//SYSFTPD  DD DISP=SHR,DSN=SYSL.&PROJECT..PARMLIB(FTPDAT)
```

Example 8 SYSL.&PROJECT..PARMLIB(PELPROF)

```
INCLUDE  SYSL.COMMON.DATA(PELBASE)
INTERFACE &TCPLINK
 DEFINE IPAQENET
 IPADDR 129.40.&IPADDRS./&TCPMASK
 PORTNAME &TCPDEVC
 INBPERF DYNAMIC
 VLANID  &TCPVLAN
 PRIROUTER
HOME
  129.40.&IPADDRS &TCPLINK
```

```
PRIMARYINTERFACE &TCPLINK
BEGINROUTES
  Route 129.40.&IPROUTE/&TCPMASK = &TCPLINK         MTU 1500
  Route Default 129.40.&TCPGATE  &TCPLINK         MTU 1500
ENDROUTES
ITRACE OFF
START &TCPLINK
```

Example 9 SYSL.COMMON.DATA(PELBASE)

```
SOMAXCONN 1024
ARPAGE 20
IPCONFIG         PATHMTUDISCOVERY
TCPCONFIG        UNRESTRICTLOWPORTS
                 TCPSENDBFRSIZE 65535  ; 256-256K (default 16K)
                 TCPRCVBUFRSIZE 65535  ; 256-256K (default 16K)
                 DELAYACKS
UDPCONFIG        UNRESTRICTLOWPORTS
AUTOLOG 5
    FTP JOBNAME FTP1     ; FTP Server
ENDAUTOLOG
PORT
     7 UDP MISCSERV            ; Miscellaneous Server
     7 TCP MISCSERV
     9 UDP MISCSERV
     9 TCP MISCSERV
    19 UDP MISCSERV
    19 TCP MISCSERV
    20 TCP OMVS      NOAUTOLOG ; FTP Server
    21 TCP OMVS                ; FTP Server
    25 TCP SMTP                ; SMTP Server
    53 TCP NAMESRV             ; Domain Name Server
    53 UDP NAMESRV             ; Domain Name Server
    80 TCP OMVS                ; WebServer
   111 TCP PORTMAP             ; Portmap Server
   111 UDP PORTMAP             ; Portmap Server
   135 UDP LLBD                ; NCS Location Broker
   161 UDP OSNMPD              ; SNMP Agent
   162 UDP SNMPQE              ; SNMP Query Engine
   397 TCP VTAM44              ; VTAM AnyNet Support (TCP/IP over SNA)
   443 TCP OMVS                ; WebServer SSL support
   446 TCP * DELAYACKS         ; DRDA DB2 SQL port
   447 TCP * DELAYACKS         ; DRDA DB2 SQL port
   448 TCP * DELAYACKS         ; DRDA DB2 Security SQL port
   512 TCP OMVS                ; Remote Execution Server
   513 TCP OMVS                ; Rlogin
   514 TCP OMVS                ; Rshell
   515 TCP LPSERVE             ; LPD Server
   520 UDP OROUTED             ; RouteD Server
   580 UDP NCPROUT             ; NCPROUTE Server
   623 TCP OMVS                ; Otelnet Server (OMVS stack)
   750 TCP MVSKERB             ; Kerberos
   750 UDP MVSKERB             ; Kerberos
   751 TCP ADM@SRV             ; Kerberos Admin Server
   751 UDP ADM@SRV             ; Kerberos Admin Server
```

```
  900 TCP SYSMGT01            ; Component Broker
 3000 TCP CICSTCP             ; CICS Socket
 3010 TCP CICSTCP             ; CICS Listener
 5020 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5021 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5022 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5023 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5024 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5025 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5026 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5027 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5028 TCP OMVS                ; Resync port for DB2 DRDA (DDF)
 5555 TCP DAEMON01            ; Component Broker
```

Example 10 SYSL.&PROJECT..PARMLIB(PELDATA)

```
TCPIPJOBNAME TCPIP
&TCPLINK.:  HOSTNAME  &TCPLINK
DOMAINORIGIN  PBM.IHOST.COM
NSINTERADDR  129.40.106.1
NSPORTADDR 53
RESOLVEVIA UDP
RESOLVERTIMEOUT 30
RESOLVERUDPRETRIES 1
DATASETPREFIX TCPIP
  LOADDBCSTABLES JIS78KJ JIS83KJ SJISKANJI EUCKANJI HANGEUL KSC5601
```

Example 11 SYSL.&PROJECT..PARMLIB(FTPDAT)

```
SPACETYPE     TRACK          ; New data set allocation space type
PRIMARY       10             ; New data set allocation primary space
SECONDARY     5              ; New data set allocation secondary space
DIRECTORY     10             ; New data set allocation directory blocks
RECFM         FB             ; New data set allocation record format
LRECL         80             ; New data set allocation logical record length
BLOCKSIZE     3120           ; New data set allocation blocksize
JESLRECL      80             ; LRECL of JES jobs
JESRECFM      F              ; RECFM of JES jobs
JESPUTGETTO   600            ; Timeout for remote job submission put/get
JESINTERFACEL 2              ; Allows to switch JESOWNER
FILETYPE      SEQ            ; File transfer mode (JES/SEQ/SQL)
AUTOMOUNT     TRUE           ; Automatic mount of unmounted volume
AUTORECALL    TRUE           ; Automatic recall of migrated data sets
CONDDISP      CATLG          ; Data sets cataloged if transfer fails
DIRECTORYMODE FALSE          ; Directorymode vs. data set mode
INACTIVE      300            ; Inactive time out
STARTDIRECTORY HFS           ; Use HFS directory at connect time
WRAPRECORD    FALSE          ; Data is NOT wrapped to next record
```

Modifying TCP/IP

Make the following updates to the TCP/IP configuration in PARMLIB:

- Add `TTLS` to the TCPCONFIG section.
- Add `PAGENT` to the AUTOLOG section.

In the example that is shown in Figure 19, the changes were made to the PELBASE member in PARMLIB.

```
EDIT        SYSL.ZLP7.PARMLIB(PELBASE) - 01.05
Command ===>
****** ******************************** Top of Data ******
000001 ; ------------------------------------------------
000002 ; Set Maximum connection queue
000003 ;
000004 SOMAXCONN 1024
000005 ;
000006 ARPAGE 20
000007 ; ------------------------------------------------
000008 ; Set config
000009 ;
000010 IPCONFIG          PATHMTUDISCOVERY
000011 TCPCONFIG         UNRESTRICTLOWPORTS
000012                   TTLS
000013                   TCPSENDBFRSIZE 65535  ; 256-256K (c
000014                   TCPRCVBUFRSIZE 65535  ; 256-256K (c
000015                   DELAYACKS
000016 UDPCONFIG         UNRESTRICTLOWPORTS
000017 ; ------------------------------------------------
000018 AUTOLOG 5
000019     PAGENT                  ; Policy Agent
000020     FTP JOBNAME FTP1        ; FTP Server
000021 ;   TN3270                  ; TN3270 Server
000022 ;   LPSERVE                 ; LPD Server
000023 ;   NAMESRV                 ; Domain Name Server
000024 ;   NCPROUT                 ; NCPROUTE Server
000025 ;   PORTMAP                 ; Portmap Server
000026 ;   OROUTED                 ; RouteD Server
000027 ;   RXSERVE                 ; Remote Execution Server
000028 ;   SMTP                    ; SMTP Server
000029 ;   OSNMPD                  ; SNMP Agent Server
000030 ;   SNMPQE                  ; SNMP Client
000031 ;   TCPIPX25                ; X25 Server
000032 ENDAUTOLOG
```

Figure 19 Update the TCP/IP configuration in PARMLIB

Running the RACF commands

Complete the following steps:

1. Create `CLASS(SERVAUTH) EZB.INITSTACK.<sysname>.TCPIP` with STCGRP(UPDATE).
2. Permit user STCSYS to CLASS(OPERCMDS) profile IBM MVS™.** access(UPDATE). STCSYS is the user ID that runs the TCP/IP procedure. You can validate this process, as shown in Figure 20 on page 20.

```
STATUS DISPLAY ALL CLASSES
AND INPUT ===>
JOBNAME  JobID    Owner    Prty Queue
TCPIP    STC00759 STCSYS     15 EXECUTION
```

Figure 20 Validate the user ID for TCP/IP

Figure 21 shows the resulting SERVAUTH class.

```
CLASS       NAME
-----       ----
SERVAUTH    EZB.INITSTACK.ZLP7.TCPIP

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    SYS1            READ              ALTER     NO

INSTALLATION DATA
-----------------
NONE

APPLICATION DATA
----------------
NONE

SECLEVEL
--------
NO SECLEVEL

CATEGORIES
----------
NO CATEGORIES

SECLABEL
--------
NO SECLABEL

AUDITING
--------
FAILURES(READ)

NOTIFY
------
NO USER TO BE NOTIFIED

USER       ACCESS    ACCESS COUNT
----       ------    ------ -----
VANWAG     ALTER        000000
SYSPROG    ALTER        000000
STCGRP     UPDATE       000000

   ID      ACCESS   ACCESS COUNT  CLASS                    ENTIT
-------- -------  ------------ -------- --------------------
NO ENTRIES IN CONDITIONAL ACCESS LIST
```

Figure 21 The new SERVAUTH class

Recycle PAGENT, TCP/IP, and TN3270 by using the following commands:

- `/p tn3270`
- `/p tcpip`
- `/p pagent`

Wait until everything is successfully down. Then, issue the following commands:

- `/s pagent`
- `/s tcpip`
- `/s tn3270`

Figure 22 shows the results of the commands that are used to stop TN3270 and TCP/IP.

```
CNZ4105I 09.52.18 DISPLAY ACTIVITY 381
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00002    00018    00000      00033    00054    00000/00020      00009
  VTAM     NET      VTAM     NSW  S  LLA      LLA      LLA      NSW  S
  TCPIP    TCPIP    TCPIP    NSW  SO VTAMTSO  VTAMTSO  VTAMTCAS OWT  S
  VLF      VLF      VLF      NSW  S  RMF      RMF      IEFPROC  NSW  S
  APPC     APPC     APPC     NSW  S  ASCH     ASCH     ASCH     NSW  S
  TN3270   TN3270   TN3270   NSW  SO SDSF     SDSF     SDSF     NSW  S
  ICSF     ICSF     ICSF     NSW  S  JES2     JES2     IEFPROC  NSW  S
  RACF     RACF     RACF     NSW  S  OPCA     OPCA     OPCA     NSW  S
  SDSFAUX  SDSFAUX  SDSFAUX  NSW  S  INETD    STEP1    STCSYS   OWT  AO
  FTP1     STEP1    STCUSR   OWT  AO TRK      TRK      TRK      NSW  S
  RRS      RRS      RRS      NSW  S  PAGENT   PAGENT   PAGENT   OWT  SO
EZZ6008I TN3270 STOPPING   /p tn3270
EZZ6010I TN3270 SERVER ENDED FOR PORT    23
EZZ6009I TN3270 SERVER STOPPED
EZZ3205I SNMP SUBAGENT: SHUTDOWN IN PROGRESS   /p tcpip
BPXF024I (STCSYS) Apr 22 13:52:34 M2SubA 16777235 : EZZ3205I SNMP
```

Figure 22 Stopping TN3270 and TCP/IP

Figure 23 shows that the TCP/IP and TN3270 were removed.

```
EZZ4201I TCP/IP TERMINATION COMPLETE FOR TCPIP
CNZ4105I 09.54.31 DISPLAY ACTIVITY 418
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00001    00016    00000      00033    00054    00000/00020      00007
  VTAM     NET      VTAM     NSW  S  LLA      LLA      LLA      NSW  S
  VTAMTSO  VTAMTSO  VTAMTCAS OWT  S  VLF      VLF      VLF      NSW  S
  RMF      RMF      IEFPROC  NSW  S  APPC     APPC     APPC     NSW  S
  ASCH     ASCH     ASCH     NSW  S  SDSF     SDSF     SDSF     NSW  S
  ICSF     ICSF     ICSF     NSW  S  JES2     JES2     IEFPROC  NSW  S
  RACF     RACF     RACF     NSW  S  OPCA     OPCA     OPCA     NSW  S
  SDSFAUX  SDSFAUX  SDSFAUX  NSW  S  INETD    STEP1    STCSYS   OWT  AO
  TRK      TRK      TRK      NSW  S  RRS      RRS      RRS      NSW  S
  PAGENT   PAGENT   PAGENT   OWT  SO
```

Figure 23 Termination complete

After the tasks are restarted, you see them again in the Activity list, as shown in Figure 24.

```
CNZ4105I 09.55.37 DISPLAY ACTIVITY 496
  JOBS     M/S    TS USERS    SYSAS    INITS   ACTIVE/MAX VTAM     OAS
 00002    00018    00000      00033    00054    00000/00020      00009
  VTAM     NET      VTAM     NSW  S  LLA      LLA      LLA      NSW  S
  VTAMTSO  VTAMTSO  VTAMTCAS OWT  S  VLF      VLF      VLF      NSW  S
  RMF      RMF      IEFPROC  NSW  S  APPC     APPC     APPC     NSW  S
  ASCH     ASCH     ASCH     NSW  S  SDSF     SDSF     SDSF     NSW  S
  ICSF     ICSF     ICSF     NSW  S  JES2     JES2     IEFPROC  NSW  S
  RACF     RACF     RACF     NSW  S  OPCA     OPCA     OPCA     NSW  S
  SDSFAUX  SDSFAUX  SDSFAUX  NSW  S  INETD    STEP1    STCSYS   IN   AO
  TRK      TRK      TRK      NSW  S  RRS      RRS      RRS      NSW  S
  PAGENT   PAGENT   PAGENT   OWT  SO TCPIP    TCPIP    TCPIP    NSW  SO
  FTP1     STEP1    STCUSR   OWT  AO TN3270   TN3270   TN3270   NSW  SO
```

Figure 24 TN3270 and TCP/IP have been restarted

Verification

Log in to PCOMM by using TN3270. If you cannot log in, *stop*. You did something wrong and you must start over.

Examine the TCP/IP started task output and look for messages about PAGENT. You should see the messages that are shown in Example 12.

Example 12 TCP/IP started task output

```
IEF695I START TCPIP    WITH JOBNAME TCPIP    IS ASSIGNED TO USER STCSYS  , GROUP STCGRP
 $HASP373 TCPIP    STARTED
 IEE252I MEMBER CTIEZB00 FOUND IN SYSL.ZLP7.PARMLIB
```

```
 IEE252I MEMBER CTIIDS00 FOUND IN SYSL.ZLP7.PARMLIB
 IEE538I CTINTA00 MEMBER NOT FOUND IN PARMLIB
 EZZ4210I CTRACE DEFINE FAILED FOR CTINTA00  RETURN CODE: 0000000C  REASON CODE: 00000401  COMPONE
 EZZ0162I HOST NAME FOR TCPIP IS EX238N01
 EZZ0300I OPENED INCLUDE FILE 'SYSL.COMMON.DATA(PELBASE)'
 EZZ0300I OPENED PROFILE FILE DD:PROFILE
 EZZ0309I PROFILE PROCESSING BEGINNING FOR DD:PROFILE
 EZZ0309I PROFILE PROCESSING BEGINNING FOR SYSL.COMMON.DATA(PELBASE)
 EZZ0655I PORT 5555 TCP DAEMON01 IS ALREADY RESERVED
 EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE 'SYSL.COMMON.DATA(PELBASE)'
 EZZ0304I RESUMING PROCESSING OF FILE DD:PROFILE
 EZZ0328I LINK NAME EX238N01 ON LINE 35 HAS NOT BEEN DEFINED OR HAS BEEN DELETED
 EZZ0316I PROFILE PROCESSING COMPLETE FOR FILE DD:PROFILE
 EZZ0303I INITIAL PROFILE FILE CONTAINS ERRORS
 EZZ0623I PATH MTU DISCOVERY SUPPORT IS ENABLED
 EZZ0338I TCP PORTS 1 THRU 1023 ARE NOT RESERVED
 EZZ0338I UDP PORTS 1 THRU 1023 ARE NOT RESERVED
*EZZ4248E TCPIP WAITING FOR PAGENT TTLS POLICY
 EZZ4202I Z/OS UNIX - TCP/IP CONNECTION ESTABLISHED FOR TCPIP
 EZZ4340I INITIALIZATION COMPLETE FOR INTERFACE EX238N01
 EZB6473I TCP/IP STACK FUNCTIONS INITIALIZATION COMPLETE.
 EZAIN11I ALL TCPIP SERVICES FOR PROC TCPIP ARE AVAILABLE.
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP grp_Diagnostic
 EZZ4250I AT-TLS SERVICES ARE AVAILABLE FOR TCPIP
 EZD1176I TCPIP HAS SUCCESSFULLY JOINED THE TCP/IP SYSPLEX GROUP EZBTCPCS
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP gAct1~TN3270_SHARE
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP TouchTokenMutualGroupAction
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP TouchTokenServerGroupAction
 S FTP
 EZZ0621I AUTOLOG FORCING PAGENT, REASON: TCP/IP HAS BEEN RESTARTED
 CANCEL PAGENT,A=0030
 IEE301I PAGENT            CANCEL COMMAND ACCEPTED
 S PAGENT
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP grp_Diagnostic
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP gAct1~TN3270_SHARE
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP TouchTokenMutualGroupAction
 EZD1289I TCPIP ICSF SERVICES ARE CURRENTLY AVAILABLE FOR AT-TLS GROUP TouchTokenServerGroupAction
```

The TCP/IP configuration is complete.

Checkpoint

At this time, you should have:

- Access to the z/OS through PCOMM
- PAGENT installed and running with no errors
- TN3270 running
- TCP/IP running successfully, reflecting PAGENT and with keyword TTLS
- A new key ring
- A new CA certificate as the default and connected to your key ring
- A new personal certificate that is signed with the CA certificate and connected to your key ring
- The CA certificate on your PC and in your Certificate Management application

Updating TN3270 to use the secure port

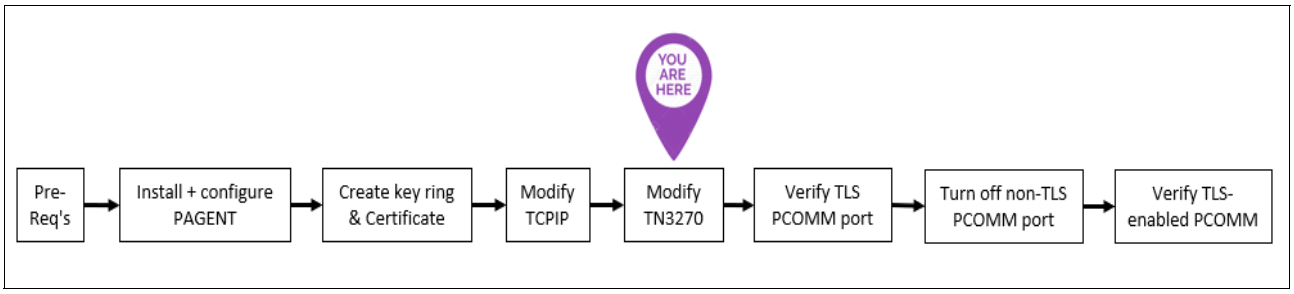


Figure 25 You are here: Modify TN3270

Warning: Be careful with this process. You should have a back-out plan in case you make a change to TN3270 that prevents you from accessing the configuration. Have a back door to the system so you can undo any changes. We had access to the DASD from another z/OS and access to the HMC. This combination permitted changes to be made to the system and to recycle TN3270, if needed.

In this section, we describe how to alter the z/OS TN3270 task to add a port that is served by TN3270. This new port is the secure port. Consider the following points:

- Port 23 is the current port for TN3270.
- Port 6001 is the new secure port we are creating.

As a reminder, the personal and CA certificates are attached to a ring called TN3270_ring, which is currently on the z/OS (see Figure 26).

```
 RACDCERT CERTAUTH LIST(LABEL('ZLP6_CA_cert'))

Digital certificate information for CERTAUTH:

  Label: ZLP6_CA_cert
  Certificate ID: 2QiJmZmDhZmjgenT1/Ztw8Ftg4WZo0BA
  Status: TRUST
  Start Date: 2019/05/01 00:00:00
  End Date:   2040/05/01 23:59:59
  Serial Number:
       >00<
  Issuer's Name:
       >OU=zBMC Certificate Authority.O=IBM Corporation.C=US<

  Subject's Name:
       >OU=zBMC Certificate Authority.O=IBM Corporation.C=US<

  Signing Algorithm: sha256RSA
  Key Usage: CERTSIGN
  Key Type: RSA
  Key Size: 2048
  Private Key: YES
  Ring Associations:
    Ring Owner: STCSYS
    Ring:
       >TN3270_ring<
```

Figure 26 Certificates and key ring on z/OS

Verifying the TN3270 current configuration

Issue the **TSO NETSTAT** command and confirm that TN3270 is serving port 23 only, as shown in Figure 27.

```
TN3270   00000014 Listen
  Local Socket:    ::..23
  Foreign Socket:  ::..0
TN3270   00002740 Establsh
  Local Socket:    ::ffff:129.40.110.65..23
  Foreign Socket:  ::ffff:9.63.20.253..53143
```

Figure 27 Display of TN3270 port

Example 13 shows the TN3270 procedure that is in `<hlq>.PROCLIB(TN3270)`.

Example 13 TN3270 procedure

```
//TN3270   PROC PARMS='CTRACE(CTIEZBTN)'
//TN3270   EXEC PGM=EZBTNINI,REGION=0M,PARM='&PARMS'
//STEPLIB  DD   DISP=SHR,DSN=SYS9.VTAMLIB
//SYSPRINT DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//SYSOUT   DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//CEEDUMP  DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
//PROFILE  DD   DISP=SHR,DSN=SYSL.COMMON.DATA(TN3270)
```

Example 14 shows the original `SYSL.COMMON.DATA(TN3270)` before any changes were made.

Example 14 SYSL.COMMON.DATA(TN3270)

```
TELNETGLOBALS
    TCPIPJOBNAME TCPIP
ENDTELNETGLOBALS
TELNETPARMS
    PORT 23
    INACTIVE 86400
    TIMEMARK 600
    SCANINTERVAL 120
    SMFINIT STD
    SMFTERM STD
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-2   D4B32782,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3   D4B32783,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4   D4B32784,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5   D4B32785,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3279-2-E NSX32702
TELNETDEVICE 3279-2   D4B32782
TELNETDEVICE 3279-3-E NSX32703
TELNETDEVICE 3279-3   D4B32783
TELNETDEVICE 3279-4-E NSX32704
TELNETDEVICE 3279-4   D4B32784
TELNETDEVICE 3279-5-E NSX32705
TELNETDEVICE 3279-5   D4B32785
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE DYNAMIC          ,D4C32XX3    ;dynamic Lmode for 3270-E
LUSESSIONPEND
```

```
ENDTELNETPARMS
BEGINVTAM
   Port 23
  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS
ENDVTAM
```

Modifying the TN3270 configuration

Make the changes that are shown in Example 15 to your TN3270 configuration in `SYSL.COMMON.DATA(TN3270)`.

Example 15 SYSL.COMMON.DATA(TN3270) modified

```
TELNETGLOBALS
    TCPIPJOBNAME TCPIP
ENDTELNETGLOBALS
TELNETPARMS
    PORT 23
    INACTIVE 86400
    TIMEMARK 600
    SCANINTERVAL 120
    SMFINIT STD
    SMFTERM STD
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-2   D4B32782,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3   D4B32783,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4   D4B32784,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5   D4B32785,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3279-2-E NSX32702
TELNETDEVICE 3279-2   D4B32782
TELNETDEVICE 3279-3-E NSX32703
TELNETDEVICE 3279-3   D4B32783
TELNETDEVICE 3279-4-E NSX32704
TELNETDEVICE 3279-4   D4B32784
TELNETDEVICE 3279-5-E NSX32705
TELNETDEVICE 3279-5   D4B32785
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE DYNAMIC          ,D4C32XX3    ;dynamic Lmode for 3270-E
LUSESSIONPEND

ENDTELNETPARMS
TELNETPARMS
  TTLSPort   6001
ENDTELNETPARMS
BEGINVTAM
```

```
   Port 23
  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS

ENDVTAM
BEGINVTAM PORT 6001

  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS
ENDVTAM
```

Remember that port number 6001 is the port that you added to the PAGENT policy statement.

Recycle

Recycle PAGENT, TCP/IP, and TN3270 by using the following commands:

- `/p tn3270`
- `/p tcpip`
- `/p pagent`

Wait until everything is successfully down. Then, issue the following commands:

- `/s pagent`
- `/s tcpip`
- `/s tn3270`

Verifying the TN3270 changes

When TN3270 is back up, review the TN3270 started task output. You should see another message about the new port 6001, as shown in Figure 28.

```
********************************** TOP OF DATA ***********************************
                 J E S 2   J O B   L O G   --   S Y S T E M   Z L P 7   --   N O D E   N 1

STC00760 ---- THURSDAY,  25 APR 2019 ----
STC00760  IEF695I START TN3270   WITH JOBNAME TN3270   IS ASSIGNED TO USER STCSYS  , (
STC00760  $HASP373 TN3270   STARTED
STC00760  IEE538I CTIEZBTN MEMBER NOT FOUND IN PARMLIB
STC00760  EZZ4210I CTRACE DEFINE FAILED FOR CTIEZBTN  RETURN CODE: 0000000C  REASON C
STC00760  IEE252I MEMBER CTIEZB00 FOUND IN SYSL.ZLP7.PARMLIB
STC00760  EZZ6001I TN3270 SERVER STARTED
STC00760  EZZ6044I TN3270 PROFILE PROCESSING BEGINNING FOR FILE  513
                   SYSL.COMMON.DATA(TN3270)
          EZZ6045I TN3270 PROFILE PROCESSING COMPLETE FOR FILE
                   SYSL.COMMON.DATA(TN3270)
STC00760  EZZ6003I TN3270 LISTENING ON PORT  6001
STC00760  EZZ6003I TN3270 LISTENING ON PORT    23
STC00760  EZZ6034I TN3270 CONN 00000010 LU TCPP701  CONN DROP  TIMEMARK  597
            IP..PORT: 9.63.20.253..50245
  //TN3270   JOB MSGLEVEL=1                                          STC00760
  //STARTING EXEC TN3270
  XXTN3270   PROC PARMS='CTRACE(CTIEZBTN)'
  XXTN3270   EXEC PGM=EZBTNINI,REGION=0M,PARM='&PARMS'
  IEFC653I SUBSTITUTION JCL - PGM=EZBTNINI,REGION=0M,PARM='CTRACE(CTIEZBTN)'
  XXSTEPLIB  DD   DISP=SHR,DSN=SYS9.VTAMLIB
  XXSYSPRINT DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
  XXSYSOUT   DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
  XXCEEDUMP  DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
  XXPROFILE  DD   DISP=SHR,DSN=SYSL.COMMON.DATA(TN3270)
  MESSAGE
  IEFC001I PROCEDURE TN3270 WAS EXPANDED USING SYSTEM LIBRARY SYSL.ZLP7.PROCLIB
START TN3270   WITH JOBNAME TN3270   IS ASSIGNED TO USER STCSYS  , GROUP STCGRP
 TN3270 IS USING THE FOLLOWING JOB RELATED SETTINGS:
 SWA=ABOVE,TIOT SIZE=32K,DSENQSHR=DISALLOW,GDGBIAS=JOB
ALLOC. FOR TN3270 TN3270
C00 ALLOCATED TO STEPLIB
ES2 ALLOCATED TO SYSPRINT
ES2 ALLOCATED TO SYSOUT
ES2 ALLOCATED TO CEEDUMP
C01 ALLOCATED TO PROFILE
  SYSL.ZLP7.PARMLIB                                KEPT
  VOL SER NOS= L7MCAT.
  SYS1.PARMLIB                                     KEPT
  VOL SER NOS= L7RESA.
  SYSL.ZLP7.PARMLIB                                KEPT
  VOL SER NOS= L7MCAT.
  SYS1.PARMLIB                                     KEPT
  VOL SER NOS= L7RESA.
********************************* BOTTOM OF DATA *********************************
```

Figure 28 TN3270 started task job log

> **Note:** If TN3270 did not restart, review your back-door access to undo your change. Log on to the system and review the log of the TN3270 task output to troubleshoot the problem.

Issue the **TSO NETSTAT** command and confirm that ports 23 and 6001 are in listen state, as shown in Example 16.

Example 16 TSO NETSTAT output

```
User Id  Conn     Local Socket           Foreign Socket         State
-------  ----     ------------           --------------         -----
BPXOINIT 00000014 0.0.0.0..10007         0.0.0.0..0             Listen
FTP1     0000000F 0.0.0.0..21            0.0.0.0..0             Listen
INETD    00000019 0.0.0.0..512           0.0.0.0..0             Listen
INETD    0000001C 0.0.0.0..623           0.0.0.0..0             Listen
INETD    0000001A 0.0.0.0..513           0.0.0.0..0             Listen
INETD    0000001B 0.0.0.0..514           0.0.0.0..0             Listen
TN3270   0000000D 0.0.0.0..6001          0.0.0.0..0             Listen
TN3270   0000000E 0.0.0.0..23            0.0.0.0..0             Listen
TCPIP    00000048 0.0.0.0..1067          *..*                   UDP
```

Using PCOMM TLSv1.2 to connect

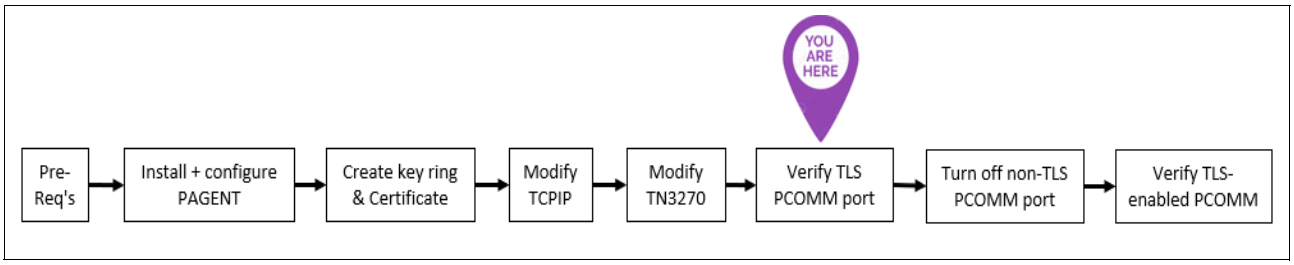


Figure 29 You are here: Verify TLS PCOMM port

The certificate that you imported to your PC as described in “Importing the certificate to the PC” on page 15 is now used. Complete the following steps to configure your PCOMM:

1. Select **Communication** →**Configure** →**Link Parameters.** Update the port number to use 6001, as shown in Figure 30.

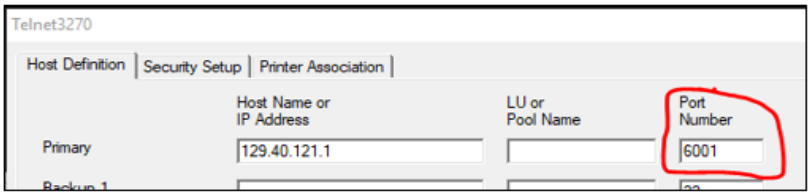


Figure 30 Configure the PCOMM port number

2. Go to the Security Setup tab and make the changes that are shown in Figure 31.

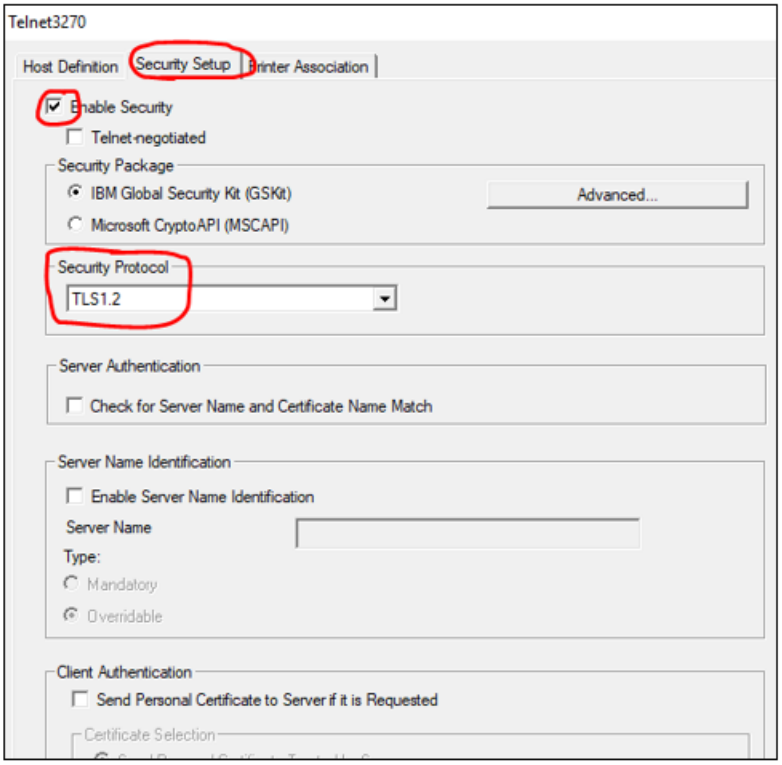


Figure 31 Configure the PCOMM security settings

If you do not see an option for TLS1.2, ensure that your PCOMM is at least version 12.0.

After these configuration changes are made, attempt to connect to z/OS. If your connection is working, you see a pad lock icon with “256” next to it at the bottom left of your secure PCOMM session. This icon indicates that your session is locked, as shown in Figure 32.

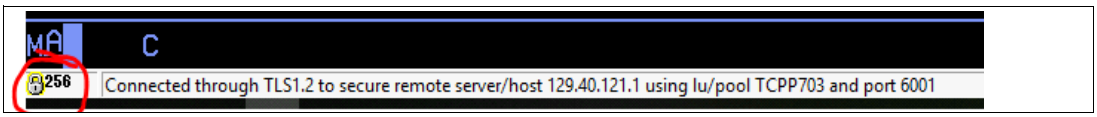


Figure 32 Working connection

If PCOMM does not connect, review the TN3270 started task output and check for messages.

If you see the message `EZZ6034I` with a CONN DROP action, you are successfully reaching TN3270, but you are not authenticating (see Figure 33).

```
EZZ6034I TN3270 CONN 00000067 LU **N/A**  CONN DROP  ERR 100B  423
 IP..PORT: 9.63.20.253..58108                              EZBTTRCV
```

Figure 33 TN3270 error message

Check the TCP/IP started task output for messages. If you see the message `EZD1286I` with a RC 428 (see Figure 34) or a RC 414 (see Figure 35), a problem exists with your certificate.

```
BPXF024I (STCSYS) Apr 24 14:44:41 TTLSÝ25¨: 10:44:41 TCPIP  217
EZD1286I TTLS Error GRPID: 00000002 ENVID: 00000001 CONNID: 00000015
LOCAL: 129.40.121.1..6001 REMOTE: 9.63.20.253..58556 JOBNAME: TN3270
USERID: STCSYS RULE: SHARE~1  RC:  428 Initial Handshake 0000000000000
000 00000050CC522750 0000000000000000 00000000
```

Figure 34 TCP/IP error message RC 428

```
BPXF024I (STCSYS) May  6 17:18:26 TTLSÝ45¨: 13:18:26 TCPIP  962
EZD1286I TTLS Error GRPID: 00000006 ENVID: 00000003 CONNID: 00000CE9
LOCAL: 129.40.110.225..6001 REMOTE: 9.12.65.253..53992 JOBNAME:
TN3270 USERID: STCSYS RULE: SHARE~1  RC:  414 Initial Handshake
0000000000000000 00000053B8522750 0000000000000000 00000000
```

Figure 35 Error message RC 414

If a problem occurred, verify the following issues:

- Your certificate is a CA certificate.
- Your certificate is connecting to ring TN3270_ring.
- You exported your certificate to a flat file correctly.
- You FTP’ed your certificate to your PC using ASCII and not option BIN.
- Your certificate is in your Certificate Management database on your PC. Review the certificate to ensure that the format is correct.
- Your PCOMM settings are correct.
- Check `/tmp/pagent.log` for messages.
- The INET changes were made in BPXPRMxx.

If the problem cannot be determined, attempt another IPL.

If the problem persists, look for messages and errors in the following components: PAGENT, TN3270, and TCP/IP.

Checkpoint

At this time, you should have access to the z/OS through the following ports:

- PCOMM non-TLS port
- PCOMM TLS port 6001

Next, we describe how to turn off the non-TLS port.

Turn off the TN3270 non-TLS port

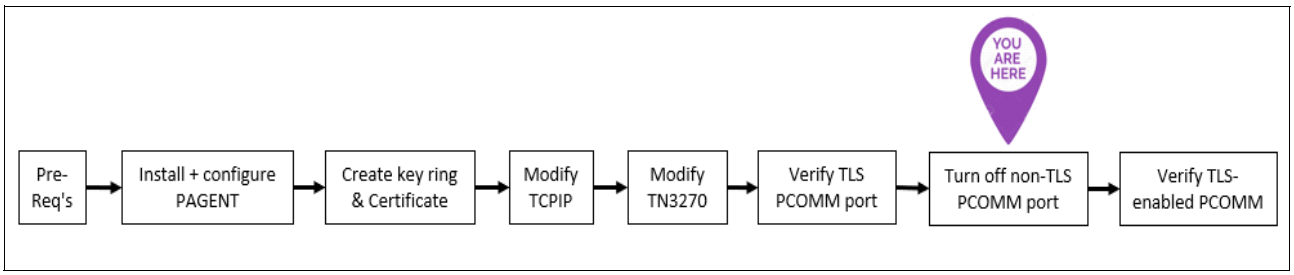


Figure 36 You are here: Turn off non-TLS port

> **Warning:** You should be able to successfully login to your z/OS through PCOMM port 6001. If you cannot log in, stop and review the previous steps.

Complete the following steps to configure TN3270 to remove the non-TLS port. Port 23 is removed, which leaves only port 6001:

1. Make the changes to your TN3270 configuration, `SYSL.COMMON.DATA(TN3270)`, that are shown in Example 17.

Example 17 Updates to TN3270 to remove port 23

```
TELNETGLOBALS
    TCPIPJOBNAME TCPIP
ENDTELNETGLOBALS
TELNETPARMS
    PORT 23
    INACTIVE 86400
    TIMEMARK 600
    SCANINTERVAL 120
    SMFINIT STD
    SMFTERM STD
TELNETDEVICE 3278-2-E NSX32702,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-2   D4B32782,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3-E NSX32703,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-3   D4B32783,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4-E NSX32704,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-4   D4B32784,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5-E NSX32705,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3278-5   D4B32785,D4C32XX3    ;dynamic Lmode for 3270-E
TELNETDEVICE 3279-2-E NSX32702
TELNETDEVICE 3279-2   D4B32782
TELNETDEVICE 3279-3-E NSX32703
```

```
TELNETDEVICE 3279-3   D4B32783
TELNETDEVICE 3279-4-E NSX32704
TELNETDEVICE 3279-4   D4B32784
TELNETDEVICE 3279-5-E NSX32705
TELNETDEVICE 3279-5   D4B32785
TELNETDEVICE LINEMODE INTERACT
TELNETDEVICE DYNAMIC          ,D4C32XX3    ;dynamic Lmode for 3270-E
LUSESSIONPEND
```

```
ENDTELNETPARMS
TELNETPARMS
  TTLSPort   6001
ENDTELNETPARMS
BEGINVTAM
   Port 23
  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS
```

```
ENDVTAM
BEGINVTAM PORT 6001

  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS
ENDVTAM
```

The configuration should look like the example that is shown Example 18 after the changes are made.

Example 18 Updated TN3270 configuration

```
TELNETGLOBALS
    TCPIPJOBNAME TCPIP
ENDTELNETGLOBALS
TELNETPARMS
  TTLSPort   6001
ENDTELNETPARMS
BEGINVTAM PORT 6001
  DEFAULTLUS
      TCP&SYSCLONE.01..TCP&SYSCLONE.30
  ENDDEFAULTLUS
  LINEMODEAPPL TSO
  ALLOWAPPL TSO* DISCONNECTABLE
  ALLOWAPPL *
  USSTCP ZLTVUSS
```

```
ENDVTAM
```

2. Recycle TN3270.
3. You should not have only one port that is serving from TN3270, port 6001. Check the TN3270 started task output and confirm. It should look like the example that is shown in Figure 37.

```
************************ TOP OF DATA ************************************************************
                 J E S 2  J O B  L O G  --  S Y S T E M  Z L P 7  --  N O D E  N 1

 STC00766 ---- THURSDAY,  25 APR 2019 ----
 STC00766  IEF695I START TN3270   WITH JOBNAME TN3270   IS ASSIGNED TO USER STCSYS  , GROUP S
 STC00766  $HASP373 TN3270   STARTED
 STC00766  IEE538I CTIEZBTN MEMBER NOT FOUND IN PARMLIB
 STC00766  EZZ4210I CTRACE DEFINE FAILED FOR CTIEZBTN  RETURN CODE: 0000000C  REASON CODE: 00
 STC00766  IEE252I MEMBER CTIEZB00 FOUND IN SYSL.ZLP7.PARMLIB
 STC00766  EZZ6001I TN3270 SERVER STARTED
 STC00766  EZZ6044I TN3270 PROFILE PROCESSING BEGINNING FOR FILE  638
                    SYSL.COMMON.DATA(TN3270)
           EZZ6045I TN3270 PROFILE PROCESSING COMPLETE FOR FILE
                    SYSL.COMMON.DATA(TN3270)
 STC00766  EZZ6003I TN3270 LISTENING ON PORT  6001
1 //TN3270   JOB MSGLEVEL=1                                                STC00766
2 //STARTING EXEC TN3270
3 XXTN3270   PROC PARMS='CTRACE(CTIEZBTN)'
4 XXTN3270   EXEC PGM=EZBTNINI,REGION=0M,PARM='&PARMS'
  IEFC653I SUBSTITUTION JCL - PGM=EZBTNINI,REGION=0M,PARM='CTRACE(CTIEZBTN)'
5 XXSTEPLIB  DD   DISP=SHR,DSN=SYS9.VTAMLIB
6 XXSYSPRINT DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
7 XXSYSOUT   DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
8 XXCEEDUMP  DD   SYSOUT=*,DCB=(RECFM=VB,LRECL=132,BLKSIZE=136)
9 XXPROFILE  DD   DISP=SHR,DSN=SYSL.COMMON.DATA(TN3270)
. MESSAGE
2 IEFC001I PROCEDURE TN3270 WAS EXPANDED USING SYSTEM LIBRARY SYSL.ZLP7.PROCLIB
START TN3270   WITH JOBNAME TN3270   IS ASSIGNED TO USER STCSYS  , GROUP STCGRP
 TN3270 IS USING THE FOLLOWING JOB RELATED SETTINGS:
 SWA=ABOVE,TIOT SIZE=32K,DSENQSHR=DISALLOW,GDGBIAS=JOB
ALLOC. FOR TN3270 TN3270
7C00 ALLOCATED TO STEPLIB
JES2 ALLOCATED TO SYSPRINT
JES2 ALLOCATED TO SYSOUT
JES2 ALLOCATED TO CEEDUMP
7C01 ALLOCATED TO PROFILE
  SYSL.ZLP7.PARMLIB                          KEPT
  VOL SER NOS= L7MCAT.
  SYS1.PARMLIB                               KEPT
  VOL SER NOS= L7RESA.
  SYSL.ZLP7.PARMLIB                          KEPT
  VOL SER NOS= L7MCAT.
  SYS1.PARMLIB                               KEPT
  VOL SER NOS= L7RESA.
************************ BOTTOM OF DATA *********************************************************
```

Figure 37 TN3270 startup

4. Issue a **TSO NETSTAT** command. The results should show TN3270 on port 6001 (see Example 19).

Example 19 TSO NETSTAT command output

```
User Id  Conn     Local Socket           Foreign Socket         State
-------  ----     ------------           --------------         -----
BPXOINIT 00000014 0.0.0.0..10007         0.0.0.0..0             Listen
FTP1     0000000F 0.0.0.0..21            0.0.0.0..0             Listen
INETD    0000001C 0.0.0.0..623           0.0.0.0..0             Listen
INETD    0000001A 0.0.0.0..513           0.0.0.0..0             Listen
INETD    0000001B 0.0.0.0..514           0.0.0.0..0             Listen
INETD    00000019 0.0.0.0..512           0.0.0.0..0             Listen
TN3270   0000005A 0.0.0.0..6001          0.0.0.0..0             Listen
TN3270   0000005B 129.40.121.1..6001     9.63.20.253..50738     Establ
```

Verify TLS-Enabled PCOMM

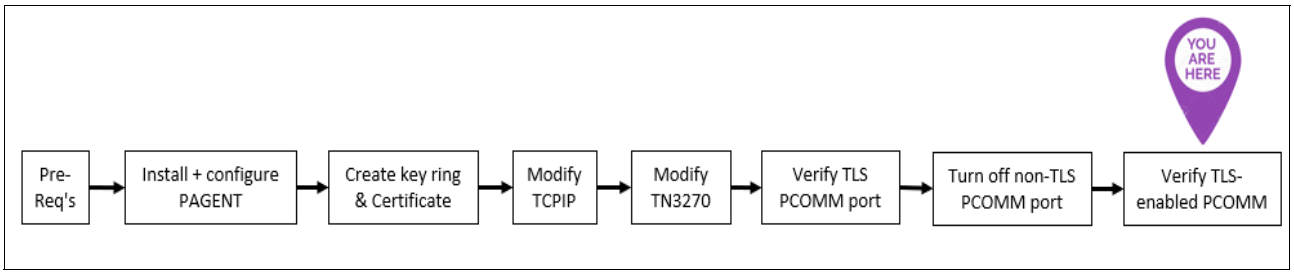


Figure 38 You are here: Verify TLS-enabled PCOMM

Your TN3270 is now using a single TLS-secured port 6001.

The real test now is to remove your certificate from the Certificate Management application on your PC and then attempt to connect to the secure PCOMM. This process should fail. If you can still connect to the secure PCOMM, something is wrong.

Another test is to have a colleague attempt to log in to your z/OS through PCOMM port 6001 (or any other port) without the certificate. They should not be able to access the z/OS.

Then, give them the certificate to add to their PC. You can send this certificate by using email. When they add the certificate to their PC and Certificate Management application, they should be able to access the secure PCOMM.

References

For more information about configuring and activating PAGENT, see in IBM Knowledge Center.

Author

This paper was produced as a result of experiences at the IBM Worldwide Client Experience Center, Mainframe Benchmark Center in Poughkeepsie, NY.

Chris Van Wagner is a Z Systems Programmer at the IBM Worldwide Client Experience Centers. He has extensive knowledge with the z/OS platform. Chris is a Z advocate and loves enabling use of the platform. Chris has a teacher's spirit and hopes to help others like him to avoid the pain points that were experienced throughout this exercise. If you read through this document and have suggestions or corrections, contact Chris.

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

Wai Choi
Linda Harrison
Carla Sadtler
IBM US

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks® residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

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

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:

  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm
- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

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 jurisdictions 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

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

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

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.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

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 actual people or business enterprises 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

REDP-5538-00

ISBN 0738457744

Printed in U.S.A.