“A” Journey Configuring SSL for TCPIP and Telnet and Performance ToolKit

Presented by:

The Earl

Abstract

There have been MANY presentations over the years at SHARE, at the VM Workshop and at User Groups about how to setup SSL servers including the ultimate authority Chapter 16. of the TCP/IP Planning & Customization manual.

Attend this session for an overview of z/VM's SSL, material “Borrowed” from other presentations, my discussions with friends from Endicott (I hope they still are), material posted on the IBMVM list. And find out who was finally able to help me.

Most Important though is HOW-TO create a certificate request AND send it to your company’s Security team to sign and HOW-TO find your company’s Trusted Primary and Intermediate Certificate's.

Agenda

- Introduction
- A bit of History
- My Journey and My Fails
- Create an Internal z/VM Certificate Database
- Update z/VM TCP/IP Configuration
- Update IBM PCOMM 3270 and IBM Performance Toolkit
- Thanx and some acknowledgements

Introduction

“ It is assumed that the reader has a good understanding of z/VM TCP/IP server configuration, SSL concepts and digital certificates. “

The above statement is common among the presentations I have read and tried to learn from, if not stated it is implied. That is the problem with not being able to attend the presentations, you missed the chance to ask questions. Not that I would have known enough to ask intelligent questions.

I tried to figure out how to secure our PC3270 telnet sessions. I e-mail’d and talked to IBM’rs in Endicott and I got a lot of great help, until they got tired of me, but they assumed I knew more than I did. I asked People and Company’s that are Partners for help and was told they would but they did not. I asked for someone to sit with me and walk me through it and no one would. I was sitting at an MVMUA meeting next to “the person that would ultimately help me” and as we were talking about my problem, it was 4/23/2019, a posting came across on the IBMVM list serv from Peter Webb of TTC that was a step by step instruction on how to create a Certificate Request. That was my first step to a new milestone. I used it and got a signed certificate from our Security Group but I could not load it to the data base. I took my error messages to the VM Workshop and showed it to my HERO and he took one look and told me I was missing the Signing Authority Certificate. Nobody here at my office had even told me about that. Yes it was in the multiple documentations, but very confusing, to me.

A bit of History

The Journey begins

- Late 2017 - Early 2018 – I start
  - I am going to be proactive and secure our PC3270 telnet sessions before they find out.
  - I put it in my z/VM 2018 Projects to do
- I read and look at SHARE , VM Workshop , WAVV, and MVMUA presentations
  - I am not really getting it but I press on and try to understand
- I use one presentation to create the Certificate Data Base
- I use the same presentation to update the System DTCPARMS file
- Another presentation had great information but I did not know enough to understand
  - I got bogged down in file type .p12 or .pem and bfsline none or bfsline nl
- Then on or about 4/26/2018 I got caught – flagged by Info Defense:
  - “Web Server Uses Plain-Text Form Based Authentication detected”

More History

PerfKit has been flagged as vulnerable, (not on my radar?)
It is now time for my lifelines

I contacted IBM , a Business Partner of IBM and my company , CA , a resource in Canada , and friends at other Companies.

Over the year or so I exchanged e-mail's with these resources

I will try and document these exchanges the best I can from saved e-mails and my memory .

Some helped me a lot (until they got tired of me - I do not blame them) some said they would help but did not, one did not answer back, and some sent me off on a different path

All the time I was asking for someone to sit next to me and walk me through the process – Finally Someone Did and it WORKED
Yes I needed someone to hold my hand

The Journey

4/26/2018 - I started by contacting IBM, 3 with Endicott in their e-mail and one in NJ

The answers were simple and informative and I did use them ,eventually

1) Add “SECURE <tlslabel>” to the line for PERFSVM in the PROFILE TCPIP - the problem was PERFSVM was not defined there

2) I then had to add this line to my PROFILE TCPIP “81 TCP PERFSVM NOAUTOLOG SECURE label”
    1) I had no idea at this time what – label was or meant

3) I was told to add this to my FCONX $PROFILE for PERFSVM “FC MONCOLL WEBSERV ON SSL TCPIP TCPIP 81”

4) I went back to a SHARE presentation that showed how to change the DTCPARMS and create a Certificate Database – very helpful J.M.

VIP - I made a mistake in the DTCPARMS and SSL00001-5 never came up , I did not find the error for another year.

More of the Journey

At the same time I contacted our Business Partner and an IBM business partner

I asked for someone to sit with me and help me

I asked if they had set up SSL there, I do not remember if they already had set it up or were planning to set up.

I did say if they were doing it , they could work it out using me as “THE” test dummy. We could do it at the same time , together , side by side. And we could make a presentation for the VM Workshop.

Neither one of these requests got off the ground

I also contacted a resource in the North, and I really do not remember hearing back , I was so confused .

During this time to FIX the “problem” and not get flagged I disabled the FC MONCOLL WEBSERV statement in the FCONX $PROFILE

More of the Journey

7/16/2018 - I was able to re connect with IBM

The IBM person in NJ started up a conversation with IBM in Endicott and Washington Systems Center again for me.

I stated that I could not find any SSL servers in my User Directory (like any other service virtual machine) ;-)

I was given instructions on where my SSL servers are defined;

```
PROFILE TCPSSLU
 IPL CMS PARM FILEPOOL VMSYS
 LOGONBY TCPMAINT GSKADMIN

IDENTITY SSL $$$PW$$$   160M  256M G
POOL LOW 1 HIGH 5 PROFILE TCPSSLU
```

I was given more information for the PROFILE TCPIP

```
SSLSERVERID * TIMEOUT 60
```


More of the Journey

7/18/2018 - I was able to re connect with IBM

It was suggested that I needed to read Chapter 16 of the TCP/IP Planning and Customization doc

I had 5 presentations I was looking through as well as Chapter 16
Still not understanding it very well at all

At the same time I was working on 2018 RSU (5/11/18 – 9/22/18)
It takes time to get permission to schedule and IPL all my LPARS

Also there were other z/VM things going on as well

I also decided to try CA around this time

More Journey more confusion

I contacted CA/Broadcom

I was given another suggestion – PEF needs to be installed

We had been using CA:VMSecure for years

I had installed it with encryption (but it was only the Data Base)

I had not installed the Password Encryption Facility

I spent a lot of time installing this on our systems (7/24/18 – 2/7/19) ,
it was a good thing to do , but it did not solve this problem

I went back to the manuals and my other work

More Journey more confusion

I went back to IBM on 2/28/2019

I was given some tasks and things to check;

Log on to GSKADMIN check for the .kdb file , and check permissions

Confirm the default BFS directory is /etc/gskadm

Check the log when SSL00001 does not come up , check for database does not exist, if another message it is not the data base

I sent him the screen shots of the first 2 , BUT I did not check the log for SSL00001 , BIG mistake

He asked for a look at my DTCPARMS and PROFILE TCPIP , I sent them

He also told me to look at console files again , and again I did not.

More Journey more confusion

I sent him the SYSTEM DTCPARMS file

```
:nick.SSLDCSSM :type.server
               :class.ssl_dcss_agent
               :stack.tcpip
               :for.sslserv
:nick.SSL      :type.class
               :name.SSL daemon
               :command.VMSSL
               :runtime.C
               :diskwarn.YES
               :Admin_ID_list.TCPMAINT GSKADMIN
               :memory.256M
               :mixedcaseparms.YES
               :mount. /../VMBFS:VMSYS:ROOT/     /     '
                       /../VMBFS:VMSYS:SSLSERV/  /tmp  '
                       /../VMBFS:VMSYS:GSKSSLDB/ /etc/gskadm
               :parms.KEYFile /etc/gskadm/TstCerts.kdb
```


More Journey more confusion

I sent him some console logs

```
DTCRUN1022I Console log will be sent to default owner ID: TCPMAINT
DTCRUN1046I Using TCP/IP data file: TCPIP DATA F1
DTCRUN1046I Using 'server' definition (SSL00001) from file: IBM DTCPARMS
E1
DTCRUN1046I Using 'class' definition (SSL) from file: SYSTEM DTCPARMS D1
DMSVML2060I VMSYS:TCPMAINT.SSLPOOL_SSL accessed FORCERW as
file mode A
DTCRUN1096I STORAGE = 256M
DTCRUN1040I SSL server cache segment attributes:
Space     Name      Location  Length    Loaded   Attribute
TCPIP         10000000  00100000  NO       USER
DMSPCL391E Unexpected operand(s):    /../VMBFS:VMSYS:GSKSSLDB/
/ETC/GSKADM
DTCRUN1001E "OPENVM MOUNT /../VMBFS:VMSYS:ROOT/ / '
/../VMBFS:VMSYS:SSLSERV/ /t
p ' /../VMBFS:VMSYS:GSKSSLDB/ /etc/gskadm" failed
          with return code 24
DTCRUN1099E Server not started - correct problem and retry
```


More Journey more confusion

At this point I dropped it , I had company work to do –
and MVMUA and VMWorkshop work

The error in my DTCPARMS was missed by both of us

I did not pay attention to the SSL00001 console message, it was there

I was also frustrated that I could not create a certificate in any form

We were scrambling to find a location for the next MVMUA meeting

We were hot in planning the VM Workshop in Richmond

In my spare time I had things to do at work as well, we were swapping our 3 z13's for 3 z14's and I had to prepare for that with service from IBM and our other Vendors

Finally the MVMUA meeting in JC at the Double Tree

More Journey less confusion

4/23/2019 – MVMUA meeting in JC

I was sitting next to a friend I had known for over 25 years

We were discussing my problems and he was sure he could help me, at least with my SSL problem, the others not so much

I checked my phone for e-mails and saw one come across the IBMVM list serv subject “z/VM Security Certificate Management”

I know that is the same title of some of the presentations from IBM

But this one was different it was a 60 step process on how to generate a “Certificate Request”, how to get it signed , and how to load the “Signed Certificate” – it was created by Peter Webb of the Toronto Transit Commission – a frequent contributor to the VM community

Now I had something to work with that I sorta understood

More Journey less confusion

6/03/2019 I am busted again

The Information Defense Team prepared a list of open network ports across our internal network and found there are 183 devices with Telnet enabled

My 16 z/VM LPAR's were listed

My mangers response to me was:

"Why is telnet running? Can it be shut down permanently? Or telnet is required to run the mainframe?"

After explaining what telnet is used for on the MAINFRAME and that I was working on securing telnet already

I was told to secure it this week

I should mention at this time the z/VM LINUX team (both of us) had been transferred to the Distributed Group – VMWARE – WINTEL - RedHat

More Journey less confusion

6/03/2019 I create a CRQ

The document from Peter did state that what was needed for a successful operation of the z/VM SSL servers was;

- A server certificate with a label
- 2 certificates that form the chain of trust hierarchy

I came to find out I needed the same things , but I had no idea what a chain of trust hierarchy was

I used the DOC to create a Certificate Request - CRQ

I sent it off to my company's' Infostructure Defense team

They sent back a signed Certificate and nothing else

Once again it was assumed I knew what I was doing , WRONG

More Journey less confusion

6/13/2019 I reach out to IBM again

I had been trying to load the CERTIFICATE but failed

I asked if I could send him some printouts
- The document I was using from Peter
- What I had entered to create the CRQ
- The printout when I tried to load the certificate
- The CRQ and the CER

He sent back that I could send the document his way

He suggested I check the logs again and DTCPARMS

I sent a SNARKY reply back saying I only wanted to worry about the Certificates now and that is all , I sent it and the docs

I never heard back from him , not that I blame him , I am an A-H

More Journey less confusion

6/17/2019 I Finally do something right

I finally followed his suggestion and looked at SSL00001 when trying to come up

Here is the error message:

DMSWOV2141E Missing quote or quote specification is not valid
DTCRUN1001E "OPENVM MOUNT /../VMBFS:VMSYS:ROOT/ / '
/../VMBFS:VMSYS:GSKSSLDB/ /
etc/gskadm" failed with return code 24

Light bulb this time –
QUOTE what QUOTE there should be no stinking QUOTE ????

Went back to the DTCPARMS

More Journey less confusion

6/18/2019 I Fixed the DTCPARMS

AFTER

```
:nick.SSLDCSSM :type.server
               :class.ssl_dcss_agent
               :stack.tcpip
               :for.sslserv
:nick.SSL      :type.class
               :name.SSL daemon
               :command.VMSSL
               :runtime.C
               :diskwarn.YES
               :Admin_ID_list.TCPMAINT GSKADMIN
               :memory.256M
               :mixedcaseparms.YES
               :mount. /../VMBFS:VMSYS:ROOT/     /     ,
                     /../VMBFS:VMSYS:SSLSERV/  /tmp  ,
                      /../VMBFS:VMSYS:GSKSSLDB/ /etc/gskadm
               :parms.KEYFile /etc/gskadm/TstCerts.kdb
```


More Journey less confusion

6/18/2019 I Fixed the DTCPARMS

BEFORE

```
:nick.SSLDCSSM :type.server
               :class.ssl_dcss_agent
               :stack.tcpip
               :for.sslserv
:nick.SSL      :type.class
               :name.SSL daemon
               :command.VMSSL
               :runtime.C
               :diskwarn.YES
               :Admin_ID_list.TCPMAINT GSKADMIN
               :memory.256M
               :mixedcaseparms.YES
               :mount. /../VMBFS:VMSYS:ROOT/     /     '
                     /../VMBFS:VMSYS:SSLSERV/  /tmp  '
                      /../VMBFS:VMSYS:GSKSSLDB/ /etc/gskadm
               :parms.KEYFile /etc/gskadm/TstCerts.kdb
```


More Journey less confusion

6/18/2019 Now they come up

```
DTCRUN1046I Using TCP/IP data file: TCPIP DATA F1
DTCRUN1046I Using 'server' definition (SSL00001) from file: IBM DTCPARMS E1
DTCRUN1046I Using 'class' definition (SSL) from file: SYSTEM DTCPARMS D1
DMSVML2060I VMSYS:TCPMAINT.SSLPOOL_SSL accessed FORCERW as file
mode A
DTCRUN1096I STORAGE = 256M
DTCRUN1040I SSL server cache segment attributes:
Space     Name      Location  Length    Loaded   Attribute
TCPIP     TCPIP     10000000  00100000  NO       USER
DTCRUN1011I Server started at 12:02:25 on 18 Jun 2019 (Tuesday)
DTCRUN1011I Running server command: VMSSL
DTCRUN1011I Parameters in use:
DTCRUN1011I  KEYFile /etc/gskadm/TstCerts.kdb
DTCSSL2423I Using server module: SSLSERV MODULE E2 - 4/02/19 14:19:22
DTCSSL1048I SLVL service information for: SSLSERV MODULE E2
```

More Journey but getting closer

6/29/2019 Last day of the 2019 VM Workshop at VCU in Richmond

I finally get to sit with Arty

I show him my print out from trying to load the Certificate

Enter option number (press ENTER to return to previous menu):
5

Enter certificate file name (press ENTER to return to menu):
zvm01.cer

Unable to import certificate.
Status 0x03353024 - Issuer certificate not found.

“that is easy” you do not have the Primary Root certificate (Issuer certificate) – chain of trust issue

More Journey but getting closer

Back from the VM Workshop

I talk to my Manager to give him an update , I told him what I have been doing and what I learned from the VM Workshop

We go over to talk to the Manager of the Information Defense Team and I give him an update as well

I told him about creating the Certificate Request and the Certificate signed by a member of his team and how I was unable to import/load it to my data base

I told them about being told I did not have the Primary Root Certificate

I was not told of anything I had to do to get this ? blank stare I guess he will send it to me ?

More Journey a lot closer

7/17/2019 Back working on SSL

I text Arty and ask him if he has time to talk

He calls me back and we set up a time on Monday the 22nd for him to come over and “SIT WITH ME”

I told him I was waiting for the Root Certificate

He said we do not need them – “go to your Command Prompt” enter “certmgr” - (Windows 10 PC)

A whole new world opened up to me – I clicked through and found the Primary Certificate – Arty had to go (10 min call)

I down loaded the Primary Root certificate and imported it

More Journey a lot closer

7/22/2019 Arty is coming to JC

Arty arrives at 3:30 – he does not have to use any notes

We log on to GSKADMIN and look at what I have and I show him where I can still not import the CERT even with the Primary CERTIFICATE imported

He said there must be an Intermediate Cert that we need

We go back to “certmgr” and find the Intermediate Cert

I down load and import the Intermediate Cert

Now I successfully import my Signed Certificate - WOW

I now have the 3 certificate system Peter mentioned, Arty says he has/is working on systems that have 5 intermediates

More Journey a lot closer

7/22/2019 Arty is coming to JC

Now we make sure my Profile TCPIP is set up correctly,
I add this: PORT 992
TLSLABEL VMSSL02

I have already added all the needed lines and commented out port 23 for telnet and added port 81 for perfsvm

I have already fixed the System DTCParms

We bounced TCPIP , change the configuration for PCOMM 3270 and now have the lock in the lower left hand corner, Change the FCONX $PROFILE for the secure port 81 and now HTTPS works and the lock is visible in the heading

It is 4:59 and I have a SECURE LPAR in 90 minutes
And he took the time to try and explain what were doing

My Journey is Ending

7/22/2019 One down and 15 more to go

Now you know that Arty Ecock from CUNY was the one that bailed me out , after knowing me for over 25 years he did not assume I knew anything , he knew I did NOT know anything

He suggested I create a presentation of my Journey for the next VM Workshop and MVMUA , I worked on this while securing my Systems , I also made notes so I would not forget it

I looked for a template to use and remembered Dave Jones's presentation at the 2019 Workshop , it was very good

So I stole (borrowed) it to use for my presentation, the slides before this one are 99 44/100% mine , the slides after this one are slides I would have added but Dave's are much better
I did make changes where they were different from mine

SSL CONFIGURATION IN z/VM

SSL server environment in z/VM

At z/VM installation, a default SSL/TLS server environment is created with the following components

- TCP/IP server **TCPIP**
- SSL servers **SSL0000** n (n =1 to 5)
- DCSS agent **SSLDCSSM**

The SSL environments rely on certificates defined in Certificate and key databases. The databases and certificates management tasks (create, deletion, certificates exports and imports) are performed from the **GSKADMIN** virtual machine, by mean of a utility program called *gskkyman* .

A single database can be used by all SSL server environments.

A single certificate in a database can be used by all the SSL server environments sharing that database.

SSL CONFIGURATION IN z/VM

Concept of « pool »

z/VM has had for a long time the concept of a “pool” of virtual machines, all configured to work on the same type of workload, say, performing SSL/TS encryption.

A pool is defined in the USER DIRECT file via either a USER or IDENTITY statement followed by the “POOL” statement. An example:

```
IDENTITY SSL LBYONLY 160M 256M G
POOL LOW 1 HIGH 5 PROFILE TCPSSLU
```

Creates a set of 5 virtual machines (SSL00001...SSL00005), all having common characteristics (class G, 160M memory, surrogate logon only, and based on the TCPSSLU profile).

The default SSL server pool (5 servers shown above) is designed to serve a maximum of 3000 connections, with a maximum of 600 sessions per server.

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Topics

- **GSKADMIN** and *gskkyman*
- Create the database
- Grant read access
- Create the Certificate Request
- Load the Signed server certificate
- Display certificate information

CREATE INTERNAL z/VM CERTIFICATE DATABASE

GSKADMIN and *gskkyman*

To create and manage the database, the z/VM user id GSKADMIN is available.

The utility program *gskkyman* is used to perform management tasks against the certificate database.

The GSKADMIN user owns both the BFS file space where the key database resides and the BFS file space used as SSL server temporary work space.

GSKADMIN also serves as the SSL server administrative user ID, as well.

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the database

The following information is required to create the database:

- database name – use “Database.kdb”
- database password – user defined
- password expiration – 365 days (one year)
- database record length – use default value 5000
- Comply to FIPS 6 standard – enter 1

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the database

gskkyman

Database Menu

1 - Create new database
2 - Open database
3 - Change database password
4 - Change database record length
5 - Delete database
6 - Create key parameter file
7 - Display certificate file (Binary or Base64 ASN.1 DER)

0 - Exit program

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the database

Enter option number:
1

Enter key database name (press ENTER to return to menu):
Database.kdb
Enter database password (press ENTER to return to menu):

Re-enter database password:

Enter password expiration in days (press ENTER for no expiration):
365

Enter database record length (press ENTER to use 5000):

Enter 1 for FIPS mode database or 0 to continue:
1

Key database /etc/gskadm/Database.kdb created.

The database has now been created.

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the database

Once the database has been created, the database password must be stored to allow the SSL server to work with the database with automatic login. On the main menu, select option 10:

```
      Expiration: 2020/06/18 10:30:29
      Type: FIPS

  1 - Manage keys and certificates
  2 - Manage certificates
  3 - Manage certificate requests
  4 - Create new certificate request
  5 - Receive requested certificate or a renewal certificate
  6 - Create a self-signed certificate
  7 - Import a certificate
  8 - Import a certificate and a private key
  9 - Show the default key
 10 - Store database password
 11 - Show database record length

  0 - Exit program

Enter option number (press ENTER to return to previous menu):
10

Database password stored in /etc/gskadm/Database.sth.

Press ENTER to continue.
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Grant read access

First, Select option **0** to exit from the **GSKKYMAN** program.

The POSIX statement in the TCPSSLU profile used to generate the default SSL pool sets the SSL server group ownership to security.

At this point, only the GSKADMIN user has access to the files in r/w mode. We want users from the same group (security) be able to access the files in read mode. The SSL servers are part of the security group.

Execute the following **openvm** commands to grant the read authority for the security group to the kdb and sth files:

```
Ready;
openvm permit /etc/gskadm/Database.kdb rw- r-- ---
Ready;
openvm permit /etc/gskadm/Database.sth rw- r-- ---
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the Certificate Request

From the Key Management Menu, select option 4 – Manage keys and certificates

```
  1 - Manage keys and certificates
  2 - Manage certificates
  3 - Manage certificate requests
  4 - Create new certificate request
  5 - Receive requested certificate or a renewal certificate
  6 - Create a self-signed certificate
  7 - Import a certificate
  8 - Import a certificate and a private key
  9 - Show the default key
 10 - Store database password
 11 - Show database record length

  0 - Exit program
4
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the Certificate Request (cont.)

```
 Certificate Key Algorithm

   1 - Certificate with an RSA key
   2 - Certificate with a DSA key
   3 - Certificate with an ECC key

Select certificate key algorithm (press ENTER to return to menu):
1
       RSA Key Size

   1 - 1024-bit key
   2 - 2048-bit key
   3 - 4096-bit key

Select RSA key size (press ENTER to return to menu):
2
       Signature Digest Type

   1 - SHA-1
   2 - SHA-224
   3 - SHA-256
   4 - SHA-384
   5 - SHA-512

Select digest type (press ENTER to return to menu):
1
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Create the Certificate Request (cont.)

```
Enter request file name (press ENTER to return to menu):
zvm01.crq

Enter label (press ENTER to return to menu):
ZVM01

Enter subject name for certificate
  Common name (required):
vmlpar.testlpar.com

  Organizational unit (optional):
systems

  Organization (required):
zVM

  City/Locality (optional):

  State/Province (optional):

  Country/Region (2 characters - required):
US

Enter 1 to specify subject alternate names or 0 to continue:
0

Please wait .....

Certificate created.
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Move the Certificate Request to a text file on the 191 mdisk

```
  openvm list
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links        Bytes Path name component
06/03/2019 16:05:05   F       1         1098 ‘zvm01.crq’

 openvm get zvm01.crq zvm01 crq a (bfsline NL

filel
     ZVM01  CRQ     W1 V       64       18        1  6/03/19 16:07:33
```

send this off to Info Defense group

While waiting go to the Command Prompt on your windows 10 PC - enter “certmgr”

GO TO TRUSTED ROOT CERTIFICATION AUTHORITIES
pull down " Primary Certificate Authority "
GO TO TRUSTED INTERMEDIATE CERTIFICATION AUTHORITIES
pull down " Intermediate Certificate Authority “

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Move the Primary and Intermediate Certs to the Database

openvm putbfs primary cer a /etc/gskadm/primary.cer (bfsline none

openvm putbfs intermed cer a /etc/gskadm/intermed.cer (bfsl none

```
 openvm list
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links         Bytes Path name component
07/17/2019 11:53:00   F       1          2000 ‘primary.cer'
07/22/2019 15:55:41   F       1          1984 ‘intermed.cer’
```

gskkyman

Open Database

Key Management Menu

Enter option number - 7

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Import the Primary and Intermediate Certs

Enter import file name (press ENTER to return to menu):
primary.cer

Enter label (press ENTER to return to menu):
PRIMARY

Certificate imported.

Press ENTER to continue.

Key Management Menu

Enter option number (press ENTER to return to previous menu):
7

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Import the Primary and Intermediate Certs

Enter import file name (press ENTER to return to menu):
intermed.cer

Enter label (press ENTER to return to menu):
INTERMED

Certificate imported.

Press ENTER to continue.

0 - Exit program

enter 0

CREATE INTERNAL z/VM CERTIFICATE DATABASE

If/When we receive the Signed Certificate back from INFO DEFENSE

Place the Signed Certificate on your 191 mdisk (action – send file to host)
(IND$FILE PUT ZVM01 CER A (ASCII CRLF RECFM V LRECL 133)
Move the Signed Certificate to the database

openvm putbfs zvm01 cer a /etc/gskadm/zvm01.cer (bfsl none

```
   openvm list
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links        Bytes Path name component
07/17/2019 11:53:00   F       1         2000 'primary.cer'
07/22/2019 15:55:41   F       1         1984 'intermed.cer'
06/03/2019 16:05:05   F       1         1098 'zvm01.crq'
06/10/2019 16:14:57   F       1         2427 'zvm01.cer'

  filel
INTERMED    CER     Z1 V       64        33        1  7/22/19 15:54:05
PRIMARY     CER     Z1 V       64        33        1  7/17/19 11:45:32
ZVM01       CER     Z1 V       64        39        1  6/10/19 14:50:23
ZVM01       CRQ     Z1 V       64        18        1  6/03/19 16:07:33
```

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Import the Signed Certificate

Move the Signed Certificate to the database

open data base

Key Management Menu

5 - Receive requested certificate or a renewal certificate

Enter option number (press ENTER to return to previous menu):
5

Enter certificate file name (press ENTER to return to menu):
/etc/gskadm/zvm01.cer

Certificate received.

Press ENTER to continue.

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Display certificate information

Information about certificates stored in the database can be displayed using Option 1 from the menu:

```
  Key and Certificate Menu

  Label: ZVM01

 1 - Show certificate information
 2 - Show key information
 3 - Set key as default
 4 - Set certificate trust status
 5 - Copy certificate and key to another database
 6 - Export certificate to a file
 7 - Export certificate and key to a file
 8 - Delete certificate and key
 9 - Change label
10 - Create a signed certificate and key
11 - Create a certificate renewal request

 0 - Exit program

Enter option number (press ENTER to return to previous menu):

1
```


CREATE INTERNAL z/VM CERTIFICATE DATABASE

Display certificate information

```
                    Certificate Information

                Label: ZVM01
            Record ID: 11
     Issuer Record ID: 11
              Trusted: Yes
              Version: 3
        Serial number: 5d0a8f8000087035
          Issuer name: company name
                       dom01
                       systems
                       US
         Subject name: lparname.dns
                       domo1
                       systems
                       US
       Effective date: 2019/06/19
      Expiration date: 2020/06/18
  Signature algorithm: sha512WithRsaEncryption
    Issuer unique ID: None
   Subject unique ID: None
Public key algorithm: rsaEncryption
     Public key size: 2048
          Public key: 30 82 01 0A 02 82 01 01 00 A1 26 8F 88 5F EC 6C
                      47 10 E6 2B DF 31 3D 7C C9 CE 31 EE 32 4B 44 13
                      8D 7F 77 F6 FC 97 B5 79 2B C9 BB 90 97 0E FA C2
                      C3 69 43 0B A0 0E 61 BB 50 CA BA 89 65 40 7B A7
                      71 C3 DD E3 02 93 87 24 F3 05 62 16 83 B8 67 B0
                      BC BF FE DF 07 02 80 3F 52 44 7A 70 DE CE 6F C7
                      E1 EA 69 0D 75 23 49 C7 C2 27 EB A7 81 A1 14 9A
                      EE C7 C6 1D CE E1 1A 90 24 7B 46 9F E2 6B 97 EE
                      CB 85 65 96 32 38 0F F1 B2 57 8C 26 BA 55 3E 4C
                      3D 00 83 4F 26 61 58 36 91 D9 15 09 7D DD 3B 28
                      B1 04 3A EB 8D 36 1D C2 6B 0F F7 EF 5A 64 DE C3
                      58 92 37 1A C5 84 97 96 A9 E0 B1 F7 4B FC 68 D0
                      E6 F3 D5 72 E2 4E 54 A6 5F A1 4E BE 87 2E 17 C6
                      FE 83 A0 BC D7 C5 8C 73 A8 A6 BB F5 AA CE 47 F8
                      7C CE 22 17 8E 8F DF AB F4 B4 5F 22 77 8C 3B 97
                      96 A5 31 A3 9F BA 51 77 82 BE 43 50 20 39 65 17
```

CREATE INTERNAL z/VM CERTIFICATE DATABASE

Display certificate information

```
                    10 FD 4B 08 DF D5 CF 36 A1 02 03 01 00 01
  Number of extensions: 4

Enter 1 to display extensions, 0 to return to menu:

1

      Certificate Extensions List

   1 - subjectKeyIdentifier
   2 - authorityKeyIdentifier
   3 - keyUsage (critical)
   4 - basicConstraints (critical)

Enter extension number (press ENTER to return to previous menu):
1

 49 DA C1 22 5E D6 FB 60 E3 74 C4 0D FE F4 25 85
 08 4D 9B 47

Press ENTER to continue.


      Certificate Extensions List

   1 - subjectKeyIdentifier
   2 - authorityKeyIdentifier
   3 - keyUsage (critical)
   4 - basicConstraints (critical)

Enter extension number (press ENTER to return to previous menu):
2

Key identifier:
 49 DA C1 22 5E D6 FB 60 E3 74 C4 0D FE F4 25 85
 08 4D 9B 47

Press ENTER to continue.
```


UPDATE z/VM TCP/IP CONFIGURATION

Topics

- Update the SYSTEM DTCPARMS file
- Update the PROFILE TCPIP file
- Restart TCPIP
- Check log file
- QUERY NAMES

UPDATE z/VM TCP/IP CONFIGURATION

Update the SYSTEM DTCPARMS file

Log onto the TCPMAINT user id. Insure that the TCPMAINT 198 mdisk is accessed R/W and file mode D.

Edit the SYSTEM DTCPARMS file and change/add the following

XEDIT SYSTEM DTCPARMS D

```
.*************************************************
.* SYSTEM DTCPARMS created by DTCIPWIZ EXEC on 26 Dec 2016
.* Configuration program run by MAINT640 at 18:09:59
.*************************************************
:nick.TCPIP    :type.server
                :class.stack
.=➔            :DCSS_Parms.<DEFAULT>
```


UPDATE z/VM TCP/IP CONFIGURATION

Update the SYSTEM DTCPARMS file - continued

Edit the SYSTEM DTCPARMS file and add the following lines

```
:nick.SSLDCSSM :type.server
               :class.ssl_dcss_agent
               :stack.tcpip
               :for.sslserv
 :nick.SSL     :type.class
               :name.SSL daemon
               :command.VMSSL
               :runtime.C
               :diskwarn.YES
               :Admin_ID_list.TCPMAINT GSKADMIN
               :memory.256M
               :mixedcaseparms.YES
               :mount. /../VMBFS:VMSYS:ROOT/     /     ,
                       /../VMBFS:VMSYS:SSLSERV/  /tmp  ,
                       /../VMBFS:VMSYS:GSKSSLDB/ /etc/gskadm
               :parms.KEYFile /etc/gskadm/zVMCerts.kdb ← your DB name
```


UPDATE z/VM TCP/IP CONFIGURATION

Update the PROFILE TCPIP file

Edit the PROFILE TCPIP file and add the following lines.

XEDIT PROFILE TCPIP D

```
SSLSERVERID * TIMEOUT 60
SSLLIMITS MAXSESSIONS 3000 MAXPERSSLSERVER 600
```

- The “*” wildcard is used to tell the TCP/IP server that the SSL servers are taken for the SSL server pool associated to the TCP/IP stack. This is the default pool with prefix SSL. Note that the prefix must not be specified in the statement, only the wildcard. The association between the TCP/IP server and the SSL server pool is established in the DTCPARMS file
- The timeout is the number of seconds to wait for the TCP/IP server before starting the other TCP/IP servers specified in the AUTOLOG statement. The default value is 30.

UPDATE z/VM TCP/IP CONFIGURATION

Update the PROFILE TCPIP file - continued

Edit the PROFILE TCPIP file and add/change the following lines.

```
  XEDIT PROFILE TCPIP D

PORT
 992   TCP INTCLIEN NOAUTOLOG SECURE ZVM01
; 23   TCP INTCLIEN            ; TELNET Server
  81   TCP PERFSVM NOAUTOLOG SECURE ZVM01

INTERNALCLIENTPARMS
;    PORT        23
     PORT       992
  TLSLABEL     ZVM01
```


UPDATE z/VM TCP/IP CONFIGURATION

Restart the TCPIP server

From the OPERATOR user id
(I use SYSG on the HMC)

FORCE TCPIP
XAUTOLOG TCPIP

UPDATE z/VM TCP/IP CONFIGURATION

Check the log file

```
.........
TCPIP  :  DTCRUN1038I Server is configured to support secure connections
TCPIP  :  DTCRUN1034I Associated SSL server pool: SSL*
.........
.........
TCPIP  :  DTCRUN1043I Initiating XAUTOLOG of server SSLDCSSM
.........
.........
SSLDCSSM:  HCPNSD440I Saved segment TCPIP was successfully defined in file
SSLDCSSM:  HCPNSS440I Saved segment TCPIP was successfully saved in file
.........
.........
TCPIP   :  11:02:10 DTCSSL044I SSL Server SSL00001 is available to handled secure connections
:

TCPIP : 11:02:13 DTCSSL044I SSL Server SSL00003 is available to handle secure connections
TCPIP : 11:02:13 DTCSSL044I SSL Server SSL00004 is available to handle secure connections
TCPIP : 11:02:13 DTCSSL044I SSL Server SSL00002 is available to handle secure connections
TCPIP : 11:02:13 DTCSSL044I SSL Server SSL00005 is available to handle secure connections
```


UPDATE z/VM TCP/IP CONFIGURATION

QUERY NAMES

```
query names
xxxx     - 0200, XXXXXXX  -L0005, xxxxx    - DSC , PERFSVM  - DSC
MONWRITE - DSC , BATCH    - DSC , RSCSAUTH - DSC , RSCS     - DSC
RSCSDNS  - DSC , IPGATE   - DSC , GCS      - DSC , SSL00005 - DSC
SSL00004 - DSC , SSL00003 - DSC , SSL00002 - DSC , WEB390   - DSC
VMNFS    - DSC , REXECD   - DSC , PORTMAP  - DSC , FTPSERVE - DSC
ZVMSFS   - DSC , SSL00001 - DSC , SSLDCSSM - DSC , TCPIP    - DSC
DATAMOVE - DSC , DIRMAINT - DSC , DTCVSW4  - DSC , DTCVSW3  - DSC
DTCVSW2  - DSC , DTCVSW1  - DSC , VMSERVP  - DSC , VMSERVR  - DSC
VMSERVU  - DSC , VMSERVS  - DSC , OPERSYMP - DSC , DISKACNT - DSC
EREP     - DSC , OPERATOR - 0020, MAINT    -L0004
VSM      - TCPIP
Ready; T=0.01/0.01 07:22:36
```


Update PC3270 and PerfKit configuration

For PERFSVM

Change this line in the FCONX $PROFILE

FC MONCOLL WEBSERV ON SSL TCPIP TCPIP 81

Bounce PERFSVM

Change the URL

Was http://vmlpar.testlpar.com:8081/
Now https://vmlpar.testlpar.com:81/

Now you will see the Closed Lock next to the URL

Update PC3270 and PerfKit configuration

For PC3270

Change Configuration

Link Parameters	change to PORT 992 from 23
Security Setup	enable Security

Communication
Configure
Link Parameters
change Port Number from 23 to 992
Apply
Security Setup
check Enable Security
Apply
OK

Now you will see the closed lock in the lower left hand corner

I asked an IBM friend what he thought

Here is my take on the subject.

“As a seasoned zVM systems programmer you still can not know everything.
You were taking on a project that was on a subject that was completely new to you.
You did what any experienced person would do. You asked for help.
The IBM global support (FREE) resources did what they could within the scope of their jobs.
No billable resources were asked for.
You continued to seek the assistance of peer resources and ultimately found a resource that was willing to provide the direct guidance that you needed.
Your project is complete.
Sounds like a success with you learning additional skills ultimately making you a more valuable resource.

Ignorance in a particular subject is not stupidity
Not asking for help sounds stupid to me.

I ask for help and provide help almost every day. It is what we do. SHARE!!!!!!!”

Thank you for your time!

Questions?

Thanks to Arty Ecock
For pushing me up the hill

Thanks to Dave Jones
For letting me use his template and some of his examples

Thanks to Paul Johnson and
Thanks to IBM for being patient with me till they had enough of me