


Securing z/VM Connectivity

A discussion of TLS configuration and certificate management

Brian W. Hugenbruch, CISSP
IBM Z Security for Virtualization & Cloud
z/VM Development Lab: Endicott, NY
 @Bwhugen

© 2019 IBM Corporation

V7.1.4 – Last updated 09 October 2019 for z/VM V7.1+

you ^{IBM}

Agenda

Picking an appropriate security policy: what does it all mean?

Introducing the z/VM TLS/SSL Server

Configuring TLS for z/VM

- *Managing Digital Certificates*
- *Configuring the TLS Server*
- *Configuring a TN3270 Client for Secure Communication*

Validating an appropriate security policy: bringing it all together

Appendices

- *Frequently Asked Questions*
- *Being your own Certificate Authority*
- *Debugging the TLS/SSL Server*

Names of Configuration Files used in this Presentation

PROFILE TCPIP – controls TCP/IP operations and configuration

- Sits on the TCPMAINT.198 disk, usually accessed at Filemode D
- May have a different filename, will always be filetype TCPIP
- ASSORTEDPARMS, INTERNALCLIENTPARMS, PORT, HOME, OBEY ...

IBM DTCPARMS – controls configurations of **Service Virtual Machines**

- Often renamed as <yoursys>.DTCPARMS
- Also on TCPMAINT.198
- Different definitions for SSL configuration, what TLS protocols are allowed, explains where the certificate database is
- For FTP, enables/disables anonymous access, turns on RACF exits

Step 0: *Picking an appropriate security policy*

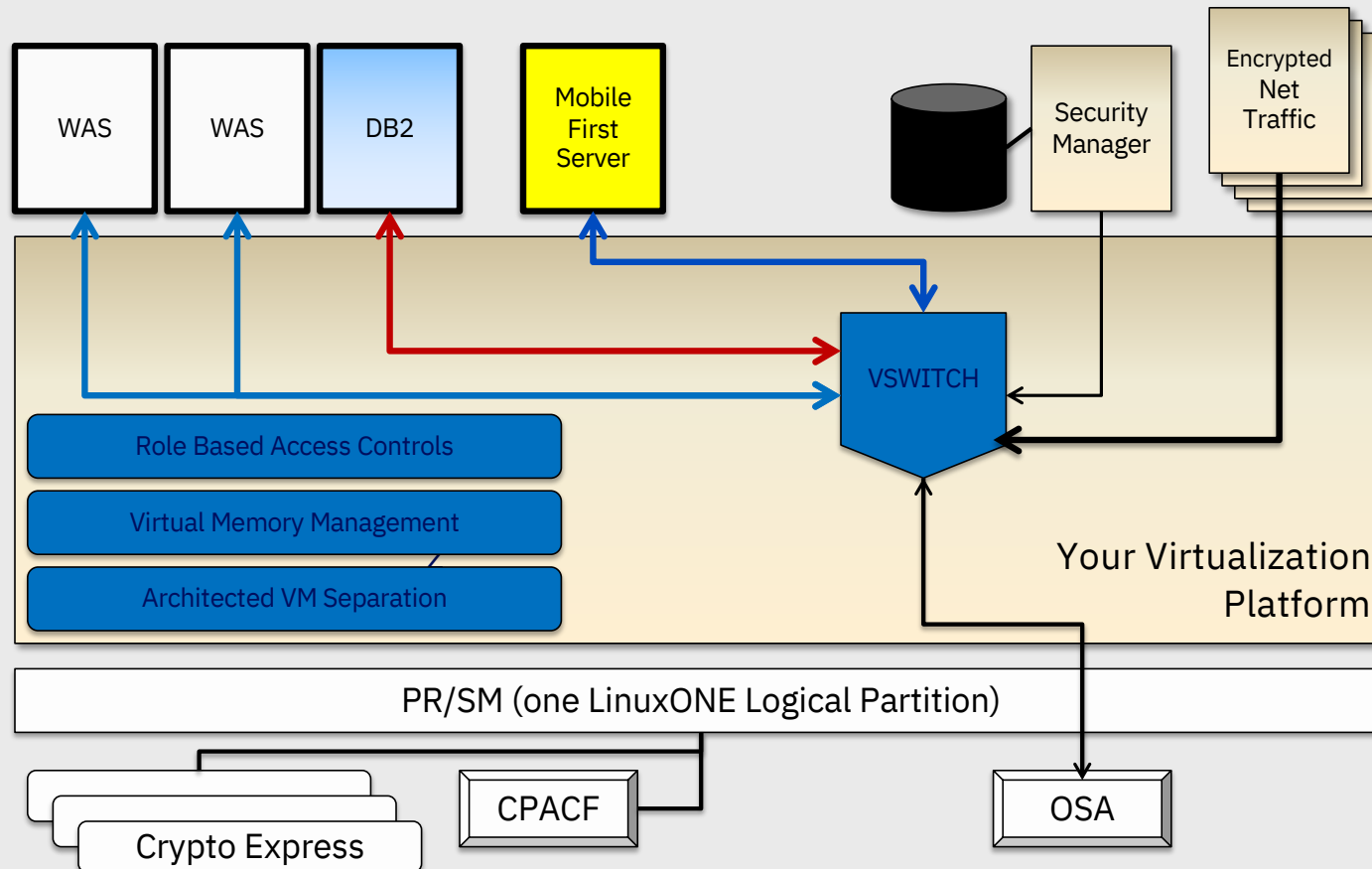
What are you trying to secure?

What rules / laws / regulations do you need to follow?

What features do you have underneath the hypervisor?

...am I even up to date on service?

This is your LinuxONE System On Lockdown.



Why Does Securing z/VM TCP/IP Matter to Me?

Managing security controls for the hypervisor is a fundamental part of enterprise security management

This includes connectivity to the hypervisor layer

- If your guests are secure, and your hypervisor is not ...
- *... your guests are not as secure as they should be.*

This line of thinking applies both to smaller shops and to larger shops

- Controlling potential damage
- Auditability of privileged commands
- Restrictions on access to data
- Enforcing scope of responsibility

Your compliance is (probably) required.

There are a lot of rules around network security

- Government rules (HIPAA, SOX, FIPS, etc.)
- Industry rules (PCI DSS)
- Internal rules – your company probably has a security policy to which you should (read: must) adhere

If you're lucky, they'll tell you about the problems (correct or not)

- “Security scans reported Port 23 was open on your z/VM LPAR, we can't have unencrypted traffic!”
- “Our BISO just declared no more using DES to encrypt stuff, please update your policies!”
- “Our certificate provider raised their rates; we need to cycle in new certificates for everything.”

Maybe you're not so lucky, and the questions are a bit more ...vague.

- “How can I tell who's using TLS 1.0 on your system or not?”
- “Have you disabled weak symmetric algorithms?”
- “Are you impacted by” [security thing someone heard about on Twitter] “?”

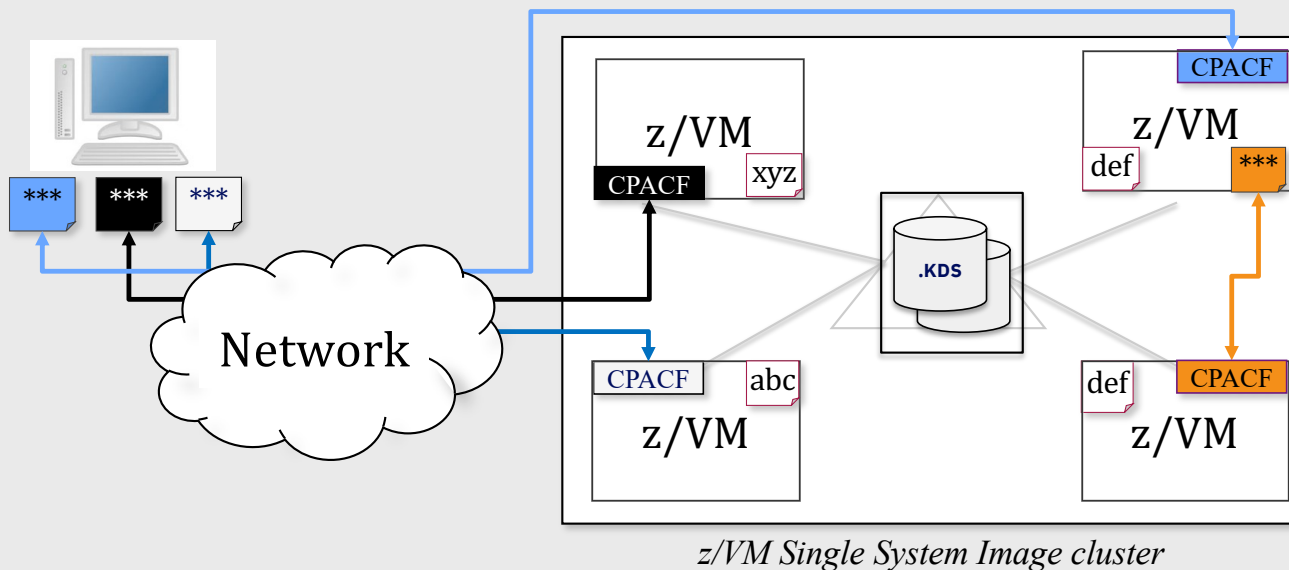
Pervasive Encryption // z/VM Network Security

Protection of data in-flight

z/VM 6.4
PTF for APAR PI72106

Legend:

*** - encrypted data
abc - unencrypted data



z/VM Secure Communications

- **Threat:** disclosure of sensitive data in flight to the hypervisor layer
- **Solution:** encrypt traffic in flight.

Notes:

- Automatic use of CPACF for symmetric algorithms
- One-line change to enable automatic use of Crypto Express features for acceleration of asymmetric algorithms
- Built on System SSL and ICSFLIB for z/VM

Client Value Proposition:

Not all organizations use host-based network encryption today ... reduced cost of encryption enables broad use of network encryption

What can we do to secure z/VM TCP/IP? (1 of 2)

Enable the TLS/SSL Server

- Allows (or requires) encrypted traffic to and from the hypervisor
- For TN3270 connections, it requires a client certificate

Enable z/VM service virtual machines (SVMs) to use TLS/SSL as well

- Telnet, FTP, SMTP, RSCS
- Port-based controls for other services (web servers, SMAPI...)

Apply service to TCP/IP

- Especially security-relevant PTFs
- Lack of currency means gaps in security may appear!
- Security-related service numbers, and CVSS scores, available at the IBM Z Security Portal:
<https://www.ibm.com/it-infrastructure/z/capabilities/system-integrity>

What can we do to secure z/VM TCP/IP? (2 of 2)

Adjust other controls as pertinent:

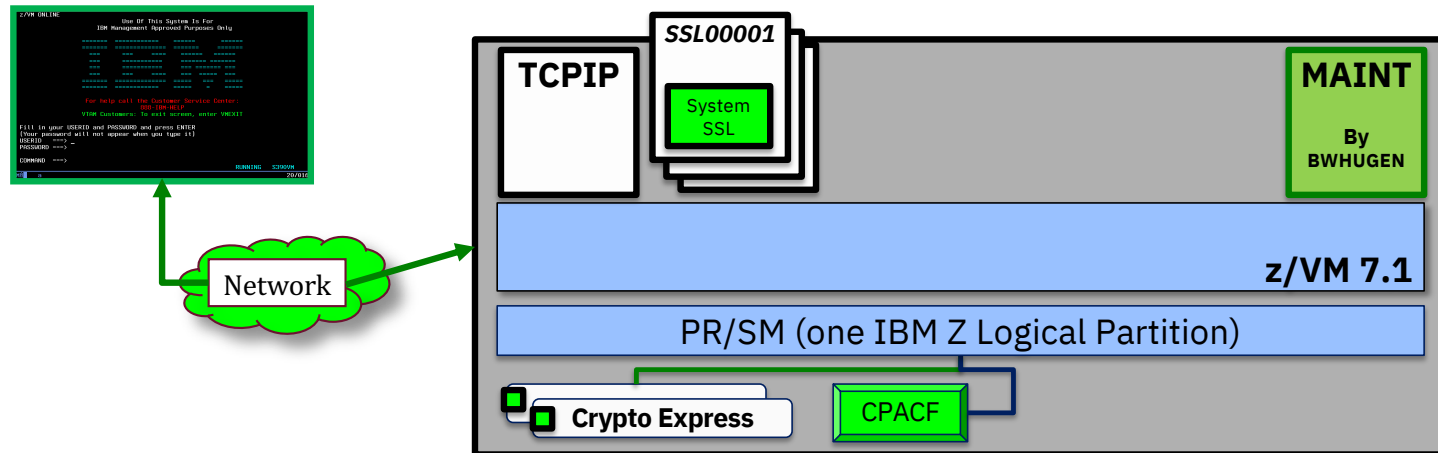
- **TIMEMARK** for timing out Telnet sessions (PROFILE TCPIP)
- Disable Anonymous FTP if appropriate (SRVRFTP.CONFIG)
- Make sure RESTRICTLOWPORTS is enabled (PROFILE TCPIP)
- SMTP FORWARDMAIL (disabled by default in z/VM 6.4)
- Remove unused TCP/IP SVMs (NOLOG in USER DIRECT)
- Enable services for RACFVM control
 - Security labeling for services if appropriate (or SYSNONE for TCPIP)
 - RACF configuration for SSLSERV available in the Appendix

Introducing the z/VM TLS/SSL Server

A service virtual machine for z/VM guests on a particular LPAR,

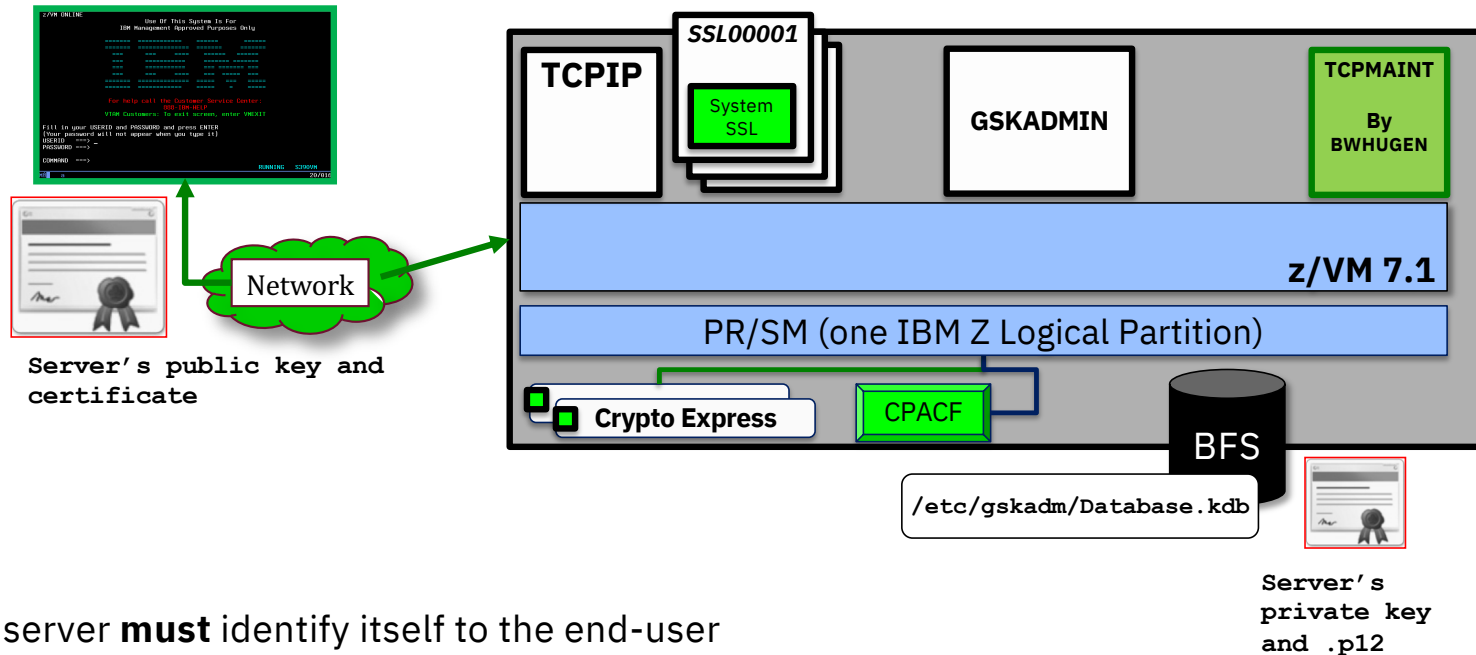
With a side discussion on certificate management

z/VM 7.1 TLS/SSL Server



- A CMS-based server associated with the TCP/IP stack
- Secures point-to-point traffic to your hypervisor
- Telnet, FTP and SMTP provide “dynamic” SSL traffic
- Port-based “static” SSL
- <http://www.vm.ibm.com/related/tcpip/tcsslspe.html>

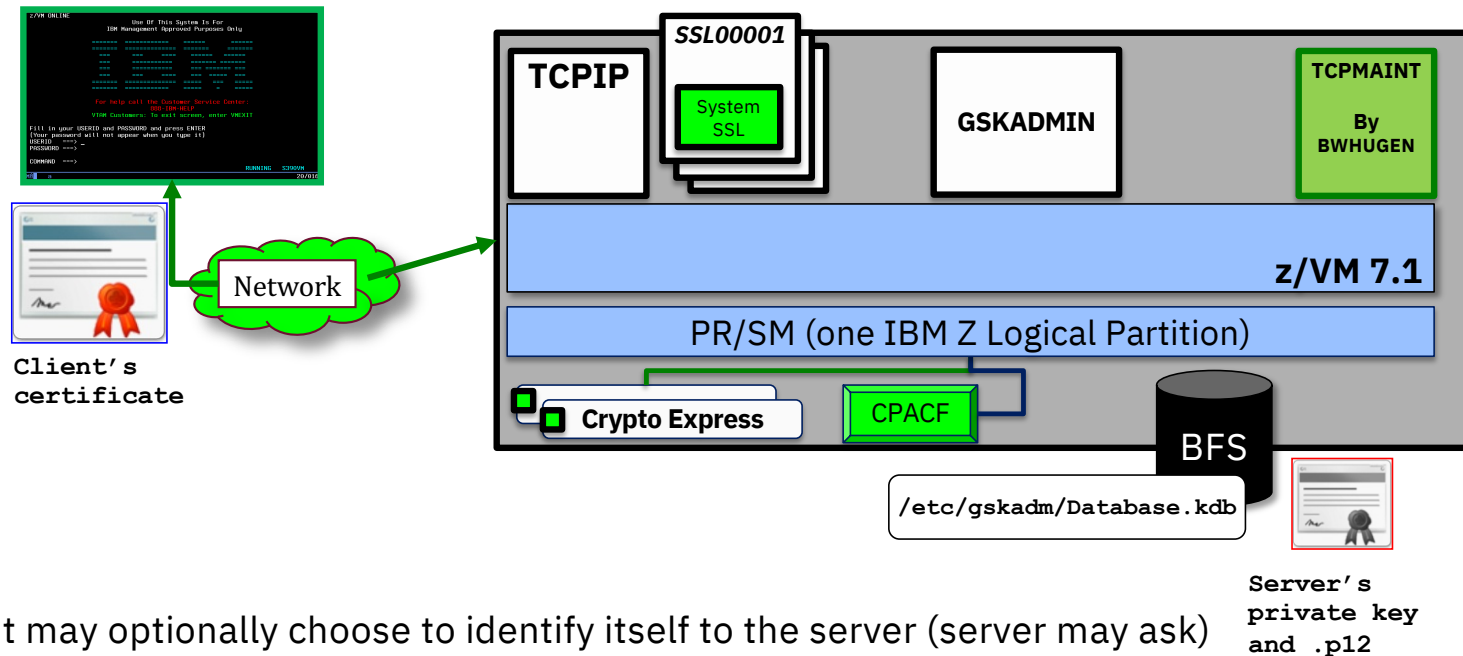
The server authenticates itself to the user ...



- The server **must** identify itself to the end-user
- Otherwise, how can you trust this connection?

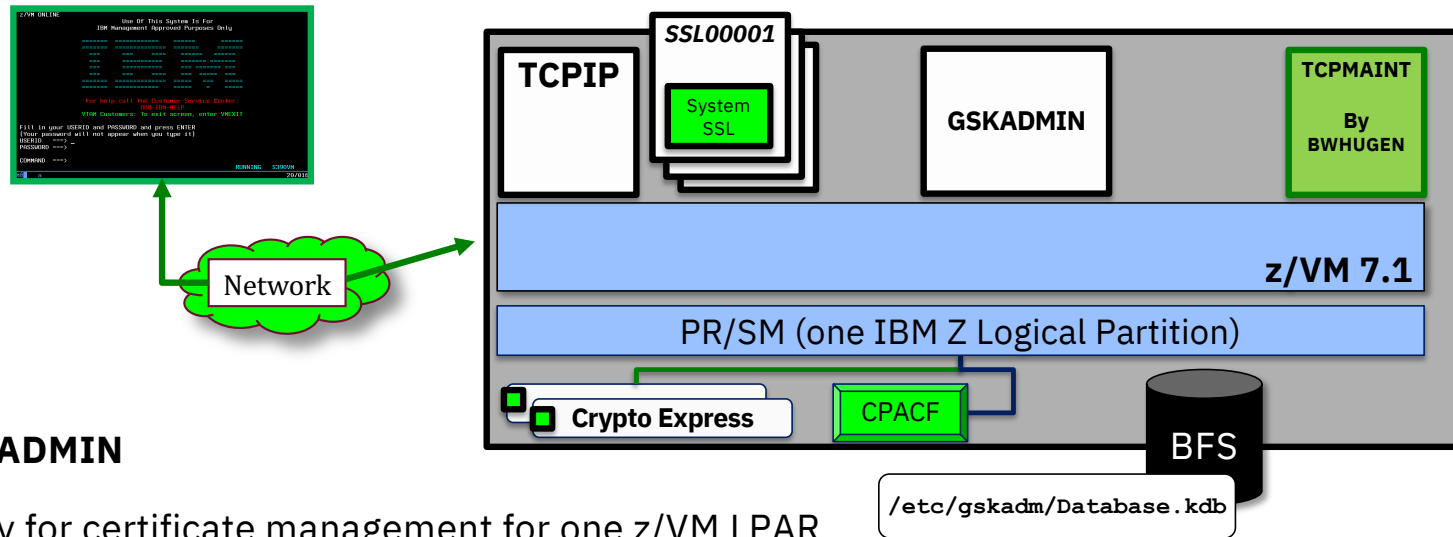
The client authenticates itself to the server

(TN3270 only)



- Client may optionally choose to identify itself to the server (server may ask)
- Updates in progress by the z/VM team (2019)
- Want to be a sponsor user?
 - <http://www.vm.ibm.com/newfunction/#ssl-cert-ver>

z/VM TLS/SSL Server – Certificate Management



- Userid **GSKADMIN**

- Specifically for certificate management for one z/VM LPAR
- PROFILE enrolls in and accesses appropriate filepools and directories
- *Gskkyman* command-line application runs here
 - Manages databases stored in a Byte-File System (BFS)
 - TLS Servers and LDAP Servers can share databases and certificates

Certificate Management for z/VM TLS

Logging onto GSKADMIN:

```
Profile...: Setting up BFS environment...
Profile...: Determining what is currently mounted...
Nothing is mounted

Profile...: Mounting root file system...
Profile...: Mounting GSKSSLDB file space at: /etc/gskadm/
Profile...: Setting working directory to: /etc/gskadm/
Profile...: (for direct access to key database files)...
Profile...: Checking mounts...
Mount point = '/etc/gskadm'
Type Stat Mounted
BFS R/W '/../VMBFS:VMSYS:GSKSSLDB/'
Mount point = '/'
Type Stat Mounted
BFS R/W '/../VMBFS:VMSYS:ROOT/'

Profile...: Checking current directory content...
Directory = '/etc/gskadm'
[.....]
Profile...: Setup complete; Environment prepared for use of GSKKYMAN
```


GSKADMIN > Looking around

```
openvm listf
```

```
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links      Bytes Path name component
02/02/2013 02:41:00   F      1         651 'certfips.arm'
01/31/2013 19:45:47   F      1        1497 'mct210s1.cert'
01/31/2013 19:46:09   F      1       120080 'Database_tcpip10.kdb'
01/31/2013 19:46:09   F      1         80 'Database_tcpip10.rdb'
01/31/2013 15:44:32   F      1        129 'Database_tcpip10.sth'
02/06/2013 11:12:43   F      1       60088 'FipsDatabase_tcpip10.kdb'
02/01/2013 08:23:04   F      1         88 'FipsDatabase_tcpip10.rdb'
02/01/2013 08:22:55   F      1        129 'FipsDatabase_tcpip10.sth'
01/31/2013 19:20:46   F      1       1112 'Mct2root.cert'
01/31/2013 19:39:56   F      1       5109 'MCT210BH.cert'
Ready; T=0.01/0.01 11:37:27
```

GSKADMIN > Using gskkyman

`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

Enter option number:

GSKADMIN > Using gskkyman

Creating a Certificate Database

- 1. Create new Database

```
Enter key database name (press ENTER to return to menu):  
ForThisPresentation.kdb  
Enter database password (press ENTER to return to menu):  
Re-enter database password:  
  
Enter password expiration in days (press ENTER for no expiration):  
1000  
  
Enter database record length (press ENTER to use 5000):  
  
Enter 1 for FIPS mode database or 0 to continue:  
1  
  
Key database /etc/gskadm/ForThisPresentation.kdb created.  
  
Press ENTER to continue.
```

GSKADMIN > Modifying Permissions

```
openvm listf (own
```

```
gskadmin  security  rw- --- --- F 'ForThisPresentation.kdb'  
gskadmin  security  rw- --- --- F 'ForThisPresentation.rdb'  
gskadmin  security  rw- --- --- F 'ForThisPresentation.sth'
```

```
openvm permit Database.kdb rw- r-- --- (replace
```

```
gskadmin  security  rw- r-- --- F 'ForThisPresentation.kdb'  
gskadmin  security  rw- r-- --- F 'ForThisPresentation.rdb'  
gskadmin  security  rw- r-- --- F 'ForThisPresentation.sth'
```

Certificate Management for z/VM TLS

Default database location: `/etc/gskadm`

GSKADMIN automatically mounts and accesses the database's directory

Database should be located at mount point

May require manual configuration if you decide not to use the defaults

GSKADMIN > Using gskkyman

Opening a Certificate Database

- 2. Open Database (enter database name, e.g. Database.kdb, and pwd)

Key Management Menu

Database: /etc/gskadm/ForThisPresentation.kdb

Expiration: 2015/12/15 15:49:12

- 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):

GSKADMIN > Importing Certificates

Importing certificates

Certificates can be imported into the certificate database through gskkyman.

But first they need to be placed in the appropriate BFS directory.

If possible, FTP directly into the BFS

- `cd ../../VMBFS:VMSYS:GSKSSLDB/`

If not, transfer the certificate to GSKADMIN and then issue the following command ... selecting a bfsline option based on file format.

```
openvm putbfs TESTCERT P12 A /etc/gskadm/testcert.p12 (bfsline none
```

or

```
openvm putbfs MYCACERT PEM A /etc/gskadm/mycacert.pem (bfsline nl
```

GSKADMIN > Importing Certificates

Standard certificates can be either Base64 or binary format – and **bfsline none** is for binary format only. *If you can open it and read **any** of it, it's in Base64!*

```
-----BEGIN CERTIFICATE-----
MIIEOTCCA+OgAwIBAgIDEAAHMA0GCSqGSIb3DQEEBQUAMIGcMQswCQYDVQQGEwJV
UzERMA8GA1UECBMTmV3IFlvcmsxETAPBgNVBACtCEVuZGljb3R0MRgwFgYDVQQK
Ew96Vk0gRGV2ZWxvcG1lbnQxDDAKBgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4g
Vy4gSHVnZW5icnVjaDEhMB8GCSqGSIb3DQEJARYSYndodWdlbkB1cy5pYm0uY29t
MB4XDTEzMDMyNzE3NTMwOV0xNDTE0MDMyNzE3NTMwOVowZjE1MAkGA1UEBhMCVVMx
ETAPBgNVBAGTCE5ldyBZb3JrMRgwFgYDVQQKEw96Vk0gRGV2ZWxvcG1lbnQxDDAK
BgNVBAsTA1NTTDEcMBoGA1UEAxMTQnJpYW4gVy4gSHVnZW5icnVjaDCCAiIwDQYJ
KoZIhvcNAQEBBQADggIPADCCAgoCggIBAPb/rg0V3++X7lJ2N7xDcktOeSxjvlkA
2n1HRnb3VCO5HlROket1Oxd4QhBoLWL+GJgo2vY1jBM3fP/KX6lFYcCXj+zwUMIu
+eGOB+DRmVfL4cZnVYEKWTgBnEKRLQEIJ+KmgGnJgtJYRjdZ54kaXlgB2obupCui
099iYZDVkzdiiizu/SlrM0dP3jz3p6MRWMRN4f9uf6a4bNd+bCI7HnVLsLvfp3wCW
MUTKjAx6snZPAgMBAAGjezB5MAkGA1UdEwQCAAwLAYJYIZIAyb4QgENBB8WHU9w
ZW5TU0wgR2VuZXJhdGVkIENlcnRpZmljYXRlMB0GA1UdDgQWBBTWiatA5nzhUruN
ds9/TJPz/F3PnTAfBgNVHSMEGDAWgBT7hRhg6eCiBsJPY2+4DBIzqS8CEzANBgkq
hkiG9w0BAQUFAANBAAwic+Z/IvzFImTcgVNC3PH99c9u8J0u5KiAT39c6ia+FuZZ
i3tBDKoSBCfy2kBBc4k6CQNYazovVSUtJrJquQU=
-----END CERTIFICATE-----
```

```
"b"Ñ""""b""""fçf7""""µb""""b""""b""""b""""fçf7""""µb""""b""""b""""fçf7 ...
```


Certificate Management for z/VM TLS

Standard certificates (.pem, .pfx) **tend** to be Base64

.p12 files, the PKCS #12 format for a Certificate With Private Key, is binary only.

Once the key is in the BFS directory, access *gskkyman*.
Open the database and select either:

8. Import a certificate and a private key

or

1. Manage keys and certificates

7. Import a certificate

Certificate Management for z/VM TLS

A few thoughts:

When making changes to a certificate database in use by a running TLS Server virtual machine, be sure to issue an SSLADMIN REFRESH from a privileged userid.

The server will reload its environment **without interrupting existing secure connections.**

Important for when certificates need to be renewed, replaced or removed.

SSLADMIN REFRESH will automatically be transmitted to all SSL servers in an SSL Pool.

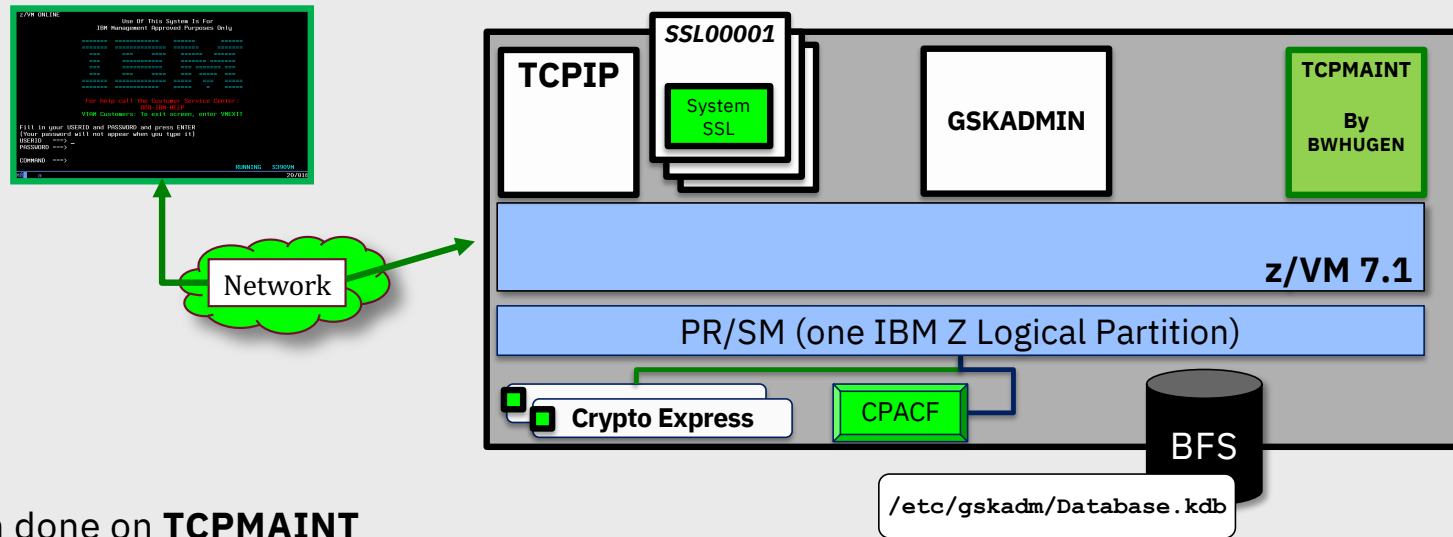
Configuring TLS for z/VM

Using Digital Certificates

Configuring the TLS Server

Configuring a TN3270 Client for Secure Communication

z/VM TLS/SSL Server – Policy Management



- Configuration done on **TCPMAINT**
- Privileged maintenance userid (**LOGON-BY** in **z/VM 7.1**)
- Covers operations for all the TCP/IP Service Virtual Machines
- Not necessarily authorized for certificate management, though

z/VM TLS/SSL Server >> DTCPARMS Options

(Machine configuration)

:Admin_ID_list.	Userids authorized to execute privileged commands – e.g., SSLADMIN commands
:Mixedcaseparms.	Parameters are supported in mixed case
:Mount.	Certificate database location. Default is /etc/gskadm/
:Parms.	As per the VMSSL command (see next slide)
:Stack.	Associated TCPIP virtual machine <i>This tag is required; otherwise, the SSL server / pool cannot be identified during stack initialization!</i>
:Timestamp.	On/Off for timestamps on terminal messages and cmd responses
:Timezone.	Set timezone of server
:Vmlink.	Sets a Pool member's SFS space

z/VM TLS/SSL Server >> Policy Configuration Parameters

Specified either on VMSSL (command-line exec) or DTCPARMS

Persists for the run-time for a server or server pool. Must be consistent for all members of a server pool

- KEYFILE - BFS location of the certificate database
- CACHELIFE - for secure connections, in hours, minutes, seconds
- CACHECLEANUP - processed every n connections
- MODE - sets a cryptographic compliance mode
 - MODE FIPS-140-2
 - MODE NIST-800-131A
- PROTOCOL - enable or disable SSL/TLS levels.
 - TLS 1.2 and TLS 1.1 enabled by default << different from earlier VM releases
 - Available protocols change based on MODE
- EXEMPT|ENABLE - disable or enable particular cipher suites
- GSKTRACE - enable System SSL tracing
- TRACE/NOTRACE - enable SSL Server tracing
 - Can be dynamically manipulated via authorized commands

z/VM TLS/SSL Server >> Mode Selection

MODE NIST-800-131A

- Minimum Protocol of TLS 1.2
- Minimum key exchange value of 2048
- Minimum hash of SHA2
- No certificate database requirements
 - Integrity checking only (HMAC-SHA256)
- Supersedes FIPS-140-2 where applicable

MODE FIPS-140-2

- Replaces the old 'FIPS' keyword
- Minimum Protocol of TLS 1.0
- Export ciphers restricted
- Minimum key exchange value of 1024
- FIPS-compliant database required
 - Integrity checking (HMAC-SHA256):
Digitally signs the crypto modules and database against tampering
 - Known Answer Tests – verify integrity after initialization

*When running in either mode, the cipher suites available
adjust according to security settings*

z/VM TLS/SSL Server >> FIPS 140-2 Compliance

Requires both database support ...

- In *gskkyman*, the *Create New Database* option will prompt for FIPS mode:

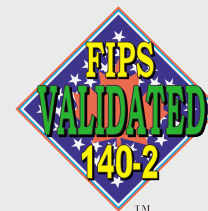
```
Enter 1 for FIPS mode database or 0 to continue:
```

```
1
```

```
Key database /etc/gskadm/ForThisPresentation.kdb created.
```

... and TLS Server Support

- DTCPARMS: **FIPS (or MODE FIPS-140-2)** or
- VMSSL: **FIPS (or MODE FIPS-140-2)**



Configuring TCP/IP Services for Secure Connectivity

- **TCPIP Configuration**

- <http://www.vm.ibm.com/related/tcpip/tcsslcfg.html>
- **SSLIMITS** (determines volume of concurrent connections per server)
- **SSLSERVERID** (identifying the server to TCPIP)
 - If detected, TCPIP will autolog SSLSERV automatically
 - Use * for a pool of SSL machines – association happens in DTCPARMS

- **Implicit (“static”) SSL**

- Establish a permanently secure port for secure connectivity
- Standardized in RFC 2228

- **PROFILE TCPIP:** PORT statement

» PORT

21 TCP FTPSERV **SECURE** *tlslabel*

- *tlslabel* – name of certificate in database (max. of 8 characters)
- Can use port ranges instead of a single port

Configuring TCP/IP Services for Secure Connectivity

- **Configuration File Updates (for “Dynamic” SSL)**
 - ▶ **TN3270:** INTERNALCLIENTPARMS (in PROFILE TCPIP)
 - SECURECONNECTION {**Required** | **Allowed** | **Never**}
 - CLIENTCERTCHECK {**FULL** | **NONE**}
 - TLSLABEL <server_certificate_name>
 - ▶ **FTP:** SRVRFTP CONFIG (server); FTP DATA (client)
 - PASSIVEPORTRANGE
 - SECURECONTROL, SECUREDATA {**Required** | **Allowed** | **Never**}
 - TLSLABEL <server_certificate_name>
 - ▶ **SMTP:** SMTP CONFIG
 - TLS Statement {**Required** | **Allowed** | **Never**}
 - TLSLABEL <server_certificate_name>
- These can be adjusted dynamically (SMSG, NETSTAT OBEY)

Configuring Secure Connectivity Dynamically

- z/VM Applications support SMSG
 - **SMSG** FTPSERV **QUERY** SECURE
 - **SMSG** FTPSERV **SECURE CONTROL** REQUIRED
 - **SMSG** SMTP **TLS** NEVER
 - **SMSG** RSCS **QUERY LINK**
- z/VM Telnet – NETSTAT OBEY / OBEYFILE
 - Adjust INTERNALCLIENTPARMS
- TLS Server
 - Operating parameters (DTCPARMS) **cannot** be dynamically changed
 - Certificate database changes can be seen by issuing **SSLADMIN REFRESH** from GSKADMIN (or another authorized userid).

RSCS: **Best Practices Whitepaper:**

- <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03288USEN&attachment=ZSW03288USEN.PDF>

Running the SSL Server

Starting the Server

When properly configured, SSLSERV or an SSL* pool will start when the TCPIP virtual machine is started

- In a pool, the first pool member (e.g., SSL00001) is autologged first

To bring a specific server online:

- `SSLADMIN START (SSL SSL00004`

or

- `NETSTAT SSL START SSL00004`

Running the SSL Server

SSLADMIN command

- Privileged command (:Admin_ID_list.)
- Reports information on SSL server status and connections
- Can route commands to specific SSL servers or TCPIP stacks

```
                                .-QUERY STATUS SUMMARY-.
>>--SSLADMIN---.-----.--'-command-----'--operands----->
                '-diagnostic_op-'

>--.----->
  '-(--| Options |--.-----'
                '-)-'
Options:

|-----|
|         .-ALL----. | '-TCPserver--userid-' '-MONitor--seconds-'
| '-SSLserver--'-userid--' |
```

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

Running the SSL Server

SSLADMIN command

- **CLEAR** remove userid(s) set by SET
- **CLOSECON / LOG** retrieves console log
- **HELP** displays help information
- **QUERY**
 - Status Summary returns general server data
 - Status Details returns specific server data
 - Settings returns current command defaults
 - Cache returns cache data
 - Sessions returns data on active secure sessions, including protocol level
 - Trace returns trace settings
- **RESTART** quiesces and re-IPL's SSL server
- **REFRESH** reaccess certificate database
- **SET** sets default targets for SSLADMIN commands
- **START / STOP** starts / stops an SSL server
- **SYSTEM** used to issue CP or CMS commands
- **TRACE / NOTRACE** enables / disables tracing

Running the SSL Server

Tracing

- Configured at start-up through DTCPARMS or VMSSL
- Can be turned on/off with SSLADMIN:

```
>>--SSLADMIN--.-TRACE-+-+-----<
|          | -| NORMAL/CONNECTIONS/FLOW Options |--| 
|          |   |-DEBUG-----'                   '| 
|-NOTRACE-----'
```

NORMAL/CONNECTIONS/FLOW Options:

(1)

.-NORMAL-----.	.-ALL or ALL 20-----.
-----+	'-----+
-NORMAL-----	.-20-----.
.-NODATA-.	'.-ALL-----'+-----'
-CONNections--+---+	-ip_address----- (2)
'-DATA----'	:-port----- length---
'-FLOW-----'	-ip_address---:-port- '-ALL-----'
	'-connection_number---

Configuring External Clients to Connect to z/VM

The compatibility and capabilities of external clients will vary

- Consult the TCPIP service webpage for thoughts
- <http://www.vm.ibm.com/related/tcpip/tcsl540.html>

The terminology of external clients may vary (SSL vs TLS)

The certificate management techniques for local clients will also vary (MSCAPI, GSKit, openssl, x3270 ...)

During the handshake, the external client will need to understand both the [server certificate](#) and (if enabled) the [client's certificate](#)

- These may or may not be generated off the same root certificate
- Installation into a local certificate database will be required

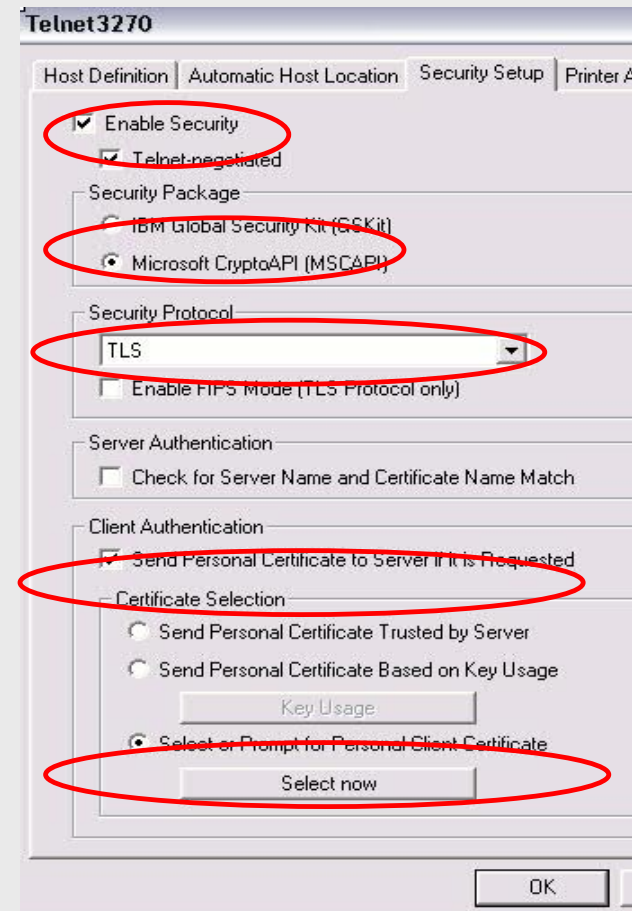
Configuring PComm for Client Certificate Validation

Telnet-negotiated: dynamic SSL

MSCAPI: certificates are stored in Windows, rather than PComm's GSKit library.

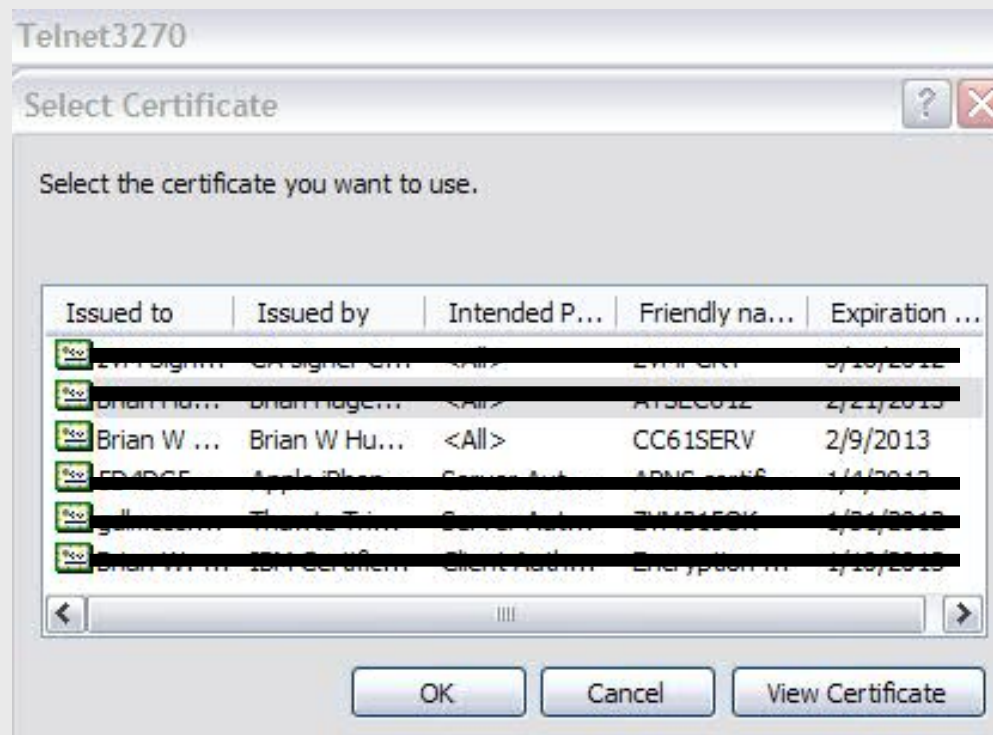
TLS: instead of SSLv3. FIPS mode disabled in this example.
TLS 1.1 and TLS 1.2 available in later versions of the client

“Personal Certificate” represents the client's identifying certificate. This will be sent if z/VM's Telnet server is configured for **CLIENTCERTCHECK FULL**.

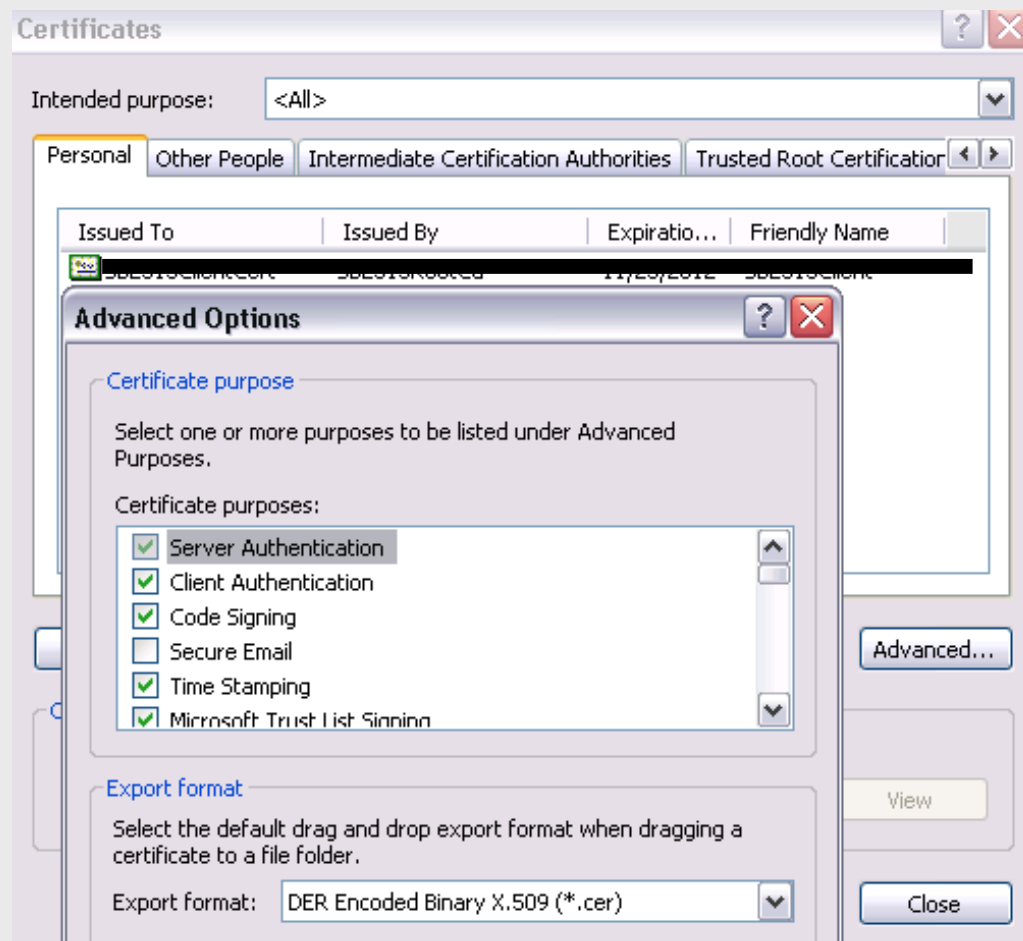


Configuring PComm for Client Certificate Validation

Example of certificates stored in MSCAPI:



Note that certificates stored in MSCAPI will need to be assigned a particular purpose (in the case of our certificate, enabling for client authentication).



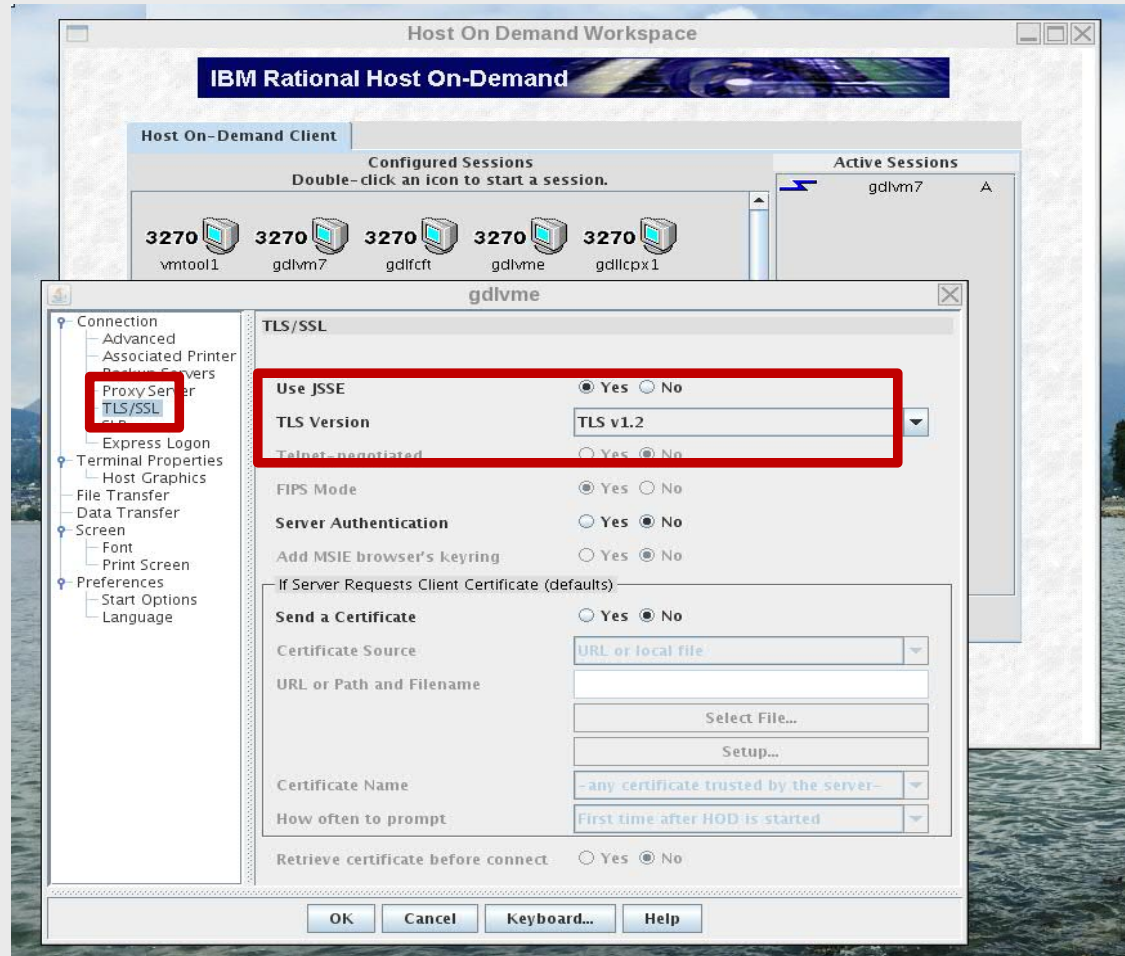
For Linux clients ...

Linux tends to be a little easier – place appropriate certificate files into a local keystore (OpenSSL) and make sure the certificate and/or key files are available when executing OpenSSL or x3270 commands

X3270 seems not to take P12 files; instead, you'll be using commands like:

```
x3270 -certfile mycert.cert -keyfile  
mykey.key -keypasswd string:mypwd -  
cafile MyRootCA.pem 192.168.0.1
```

Host On Demand



Validating Your Security Policy

Bringing it all together

How Do I...

“Turn off algorithm [x]? My security scan is complaining!”

EXEMPT the cipher suite by name.

(EXEMPT by strength is not very flexible, and subject to change when IBM updates its defaults!)

STOP/START all your TLS server machines to pick up changes, then confirm output of

SSLADMIN QUERY STATUS DETAILS >>>

Note:

- Algorithm names are complicated
- They will be similar to the names you see in openssl, but not identical
- When in doubt, check the “cipher codes” in the [TCP/IP Planning & Customization Guide](#).

DTCSSL2430I Cryptographic Mode details:

Server	Status	Modes
--------	--------	-------

S1000001	Enabled	<*None*>
S1000001	Disabled	FIPS-140-2 NIST-800-131A

DTCSSL2430I Protocol details:

Server	Status	Protocols
--------	--------	-----------

S1000001	Enabled	TLSV1_2 TLSV1_1
S1000001	Disabled	TLSV1_0 SSLV3 SSLV2

DTCSSL2430I Cipher details:

Server	State	Ciphers
--------	-------	---------

S1000001	Included	RSA_AES_128_GCM_SHA256 RSA_AES_256_GCM_SHA384
S1000001	Included	DHE_RSA_AES_128_GCM_SHA256
S1000001	Included	DHE_RSA_AES_256_GCM_SHA384
S1000001	Included	DHE_DSS_AES_128_GCM_SHA256
S1000001	Included	DHE_DSS_AES_256_GCM_SHA384 RSA_AES_128_SHA256
S1000001	Included	RSA_AES_256_SHA256 DHE_DSS_AES_128_SHA256
S1000001	Included	DHE_RSA_AES_128_SHA256 DHE_DSS_AES_256_SHA256
S1000001	Included	DHE_RSA_AES_256_SHA256 RSA_AES_256_DHE_DSS_AES_256
S1000001	Included	DHE_RSA_AES_256 RSA_AES_128 DHE_DSS_AES_128
S1000001	Included	DHE_RSA_AES_128 3DES_168_SHA DHE_RSA_3DES
S1000001	Included	DHE_DSS_3DES DES_56_SHA DHE_RSA_DES DHE_DSS_DES
S1000001	Exempt	DH_RSA_AES_128_GCM_SHA256
S1000001	Exempt	DH_RSA_AES_256_GCM_SHA384
S1000001	Exempt	DH_DSS_AES_128_GCM_SHA256
S1000001	Exempt	DH_DSS_AES_256_GCM_SHA384 DH_DSS_AES_128_SHA256
S1000001	Exempt	DH_RSA_AES_128_SHA256 DH_DSS_AES_256_SHA256
S1000001	Exempt	DH_RSA_AES_256_SHA256 RC4_128_SHA RC4_128_MD5
S1000001	Exempt	DH_DSS_AES_256 DH_RSA_AES_256 DH_DSS_AES_128
S1000001	Exempt	DH_RSA_AES_128 RC2_128_MD5 DH_RSA_3DES DH_DSS_3DES
S1000001	Exempt	DH_RSA_DES DH_DSS_DES RC4_40_MD5 RC2_40_MD5
S1000001	Exempt	NULL_SHA256 NULL_SHA NULL_MD5 NULL

TLS Server – Sponsor User Feedback: Protocol Tracking

PTF for APAR PI99184

TLS protocol level now appears on output related to secure connections (**SSLADMIN QUERY SESSIONS** and **NETSTAT IDENTIFY SSL**)

- Easy way to determine who (if anyone) is using an older protocol level

```
ssladmin query sessions (ssl all
```

```
DTCSSL2404I Sending command to server(s): TCPIP01
```

```
DTCSSL2430I Session information:
```

Server	Local Socket	Remote Socket	Type	Label	Cipher Details
SSL00001	9.60.60.3..23	9.60.60.4..1031	I	TESTCERT	TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00002	9.60.60.3..23	9.60.60.7..1036	I	TESTCERT	TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00003	9.60.60.3..23	9.60.60.12..1045	I	TESTCERT	TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00005	<*No Sessions*>				
SSL00004	<*No Sessions*>				

How Do I Force Users to Use a Particular Version of TLS?

This is part of your DTCPARMS configuration. Once you've seen no one is using TLS 1.0 anymore, you can update DTCPARMS accordingly. (TLS 1.2 and TLS 1.1 are the current defaults, but it doesn't hurt to disable protocols specifically.)

```
PROTOCOL +TLSV1_2
PROTOCOL -TLSV1_1
PROTOCOL -TLSV1_0
PROTOCOL -SSLV3
PROTOCOL -SSLV2
```

- SSLADMIN QUERY STATUS DETAILS will show the new results once you've RESTARTED your TLS/SSL Server machines

How Do I ...

“Meet my company’s policies on key sizes?”

1. Generate an RSA or DSA certificate of appropriate key length (usually 2048 or greater)
2. Use **MODE NIST-800-131A**
(minimum transport key size of 2048)
3. STOP/START all your TLS server machines, then confirm output of

SSLADMIN QUERY STATUS DETAILS >>>

Note:

MODE settings are “set and forget” for compliance

If you need to be more flexible, you may wish to configure these manually... or use them in conjunction with extra options.

DTCSSL2430I Cryptographic Mode details:

Server Status Modes

```
-----  
S1000001 Enabled <*None*>  
S1000001 Disabled FIPS-140-2 NIST-800-131A
```

DTCSSL2430I Protocol details:

Server Status Protocols

```
-----  
S1000001 Enabled TLSV1_2 TLSV1_1  
S1000001 Disabled TLSV1_0 SSLV3 SSLV2
```

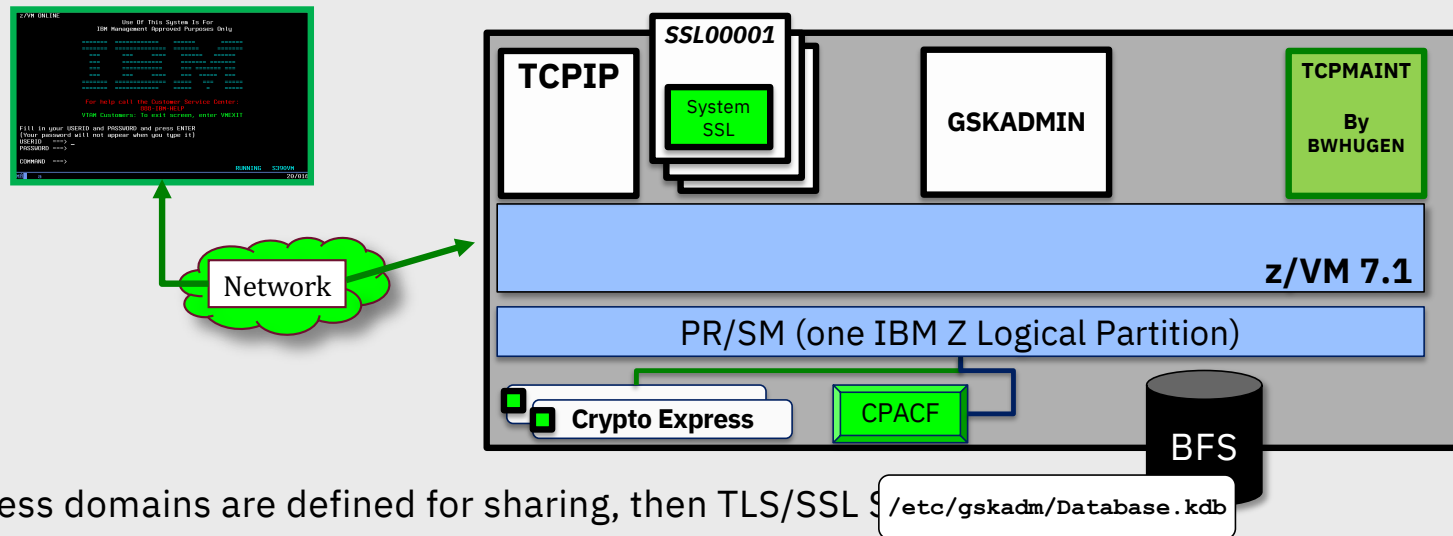
DTCSSL2430I Cipher details:

Server State Ciphers

```
-----  
S1000001 Included RSA_AES_128_GCM_SHA256 RSA_AES_256_GCM_SHA384  
S1000001 Included DHE_RSA_AES_128_GCM_SHA256  
S1000001 Included DHE_RSA_AES_256_GCM_SHA384  
S1000001 Included DHE_DSS_AES_128_GCM_SHA256  
S1000001 Included DHE_DSS_AES_256_GCM_SHA384 RSA_AES_128_SHA256  
S1000001 Included RSA_AES_256_SHA256 DHE_DSS_AES_128_SHA256  
S1000001 Included DHE_RSA_AES_128_SHA256 DHE_DSS_AES_256_SHA256  
S1000001 Included DHE_RSA_AES_256_SHA256 RSA_AES_256_DHE_DSS_AES_256  
S1000001 Included DHE_RSA_AES_256 RSA_AES_128_DHE_DSS_AES_128  
S1000001 Included DHE_RSA_AES_128_3DES_168_SHA DHE_RSA_3DES  
S1000001 Included DHE_DSS_3DES DES_56_SHA DHE_RSA_DES DHE_DSS_DES  
S1000001 Exempt DH_RSA_AES_128_GCM_SHA256  
S1000001 Exempt DH_RSA_AES_256_GCM_SHA384  
S1000001 Exempt DH_DSS_AES_128_GCM_SHA256  
S1000001 Exempt DH_DSS_AES_256_GCM_SHA384 DH_DSS_AES_128_SHA256  
S1000001 Exempt DH_RSA_AES_128_SHA256 DH_DSS_AES_256_SHA256  
S1000001 Exempt DH_RSA_AES_256_SHA256 RC4_128_SHA RC4_128_MD5  
S1000001 Exempt DH_DSS_AES_256 DH_RSA_AES_256 DH_DSS_AES_128  
S1000001 Exempt DH_RSA_AES_128_RC2_128_MD5 DH_RSA_3DES DH_DSS_3DES  
S1000001 Exempt DH_RSA_DES DH_DSS_DES RC4_40_MD5 RC2_40_MD5  
S1000001 Exempt NULL_SHA256 NULL_SHA NULL_MD5 NULL
```

How do I... Use the Crypto Express features with my TLS Server?

PTFs for APAR PI72106 (z/VM 6.4)



If Crypto Express domains are defined for sharing, then TLS/SSL \$ /etc/gskadm/Database.kdb

– **Clear-key RSA operations** are the primary beneficiary

- Handshaking, rather than data transfer – **benefit will come from a lot of connections**
- Will still use CPACF when pertinent

– Meant as a performance enabler, not to replace key storage (still need .kdb or .p12 in BFS)

~30% savings in CPU time per transaction -- <http://www.vm.ibm.com/perf/reports/zvm/html/640cip.html>

Crypto APVIRT for the z/VM TLS/SSL Server

PTFs for APAR PI72106 – or by default in z/VM V7.1

Add **CRYPTO APVIRT** to your SSL server's **PROFILE** entry

- **TCPSSLU** (the default PROFILE entry for the TLS/SSL Server)
- APDED not allowed for a POOL of userids

Insert directly into VM definition for:

- **LDAPSRV** (uses its own System SSL build)
- **GSKADMIN** (certificate creation / management)
- A **stand-alone TLS/SSL server** (non-POOL), if you have an old VM from z/VM 5.4 defined (not recommended)

```
PROFILE TCPSSLU
  CRYPTO APVIRTUAL
  IPL CMS PARM FILEPOOL
  IUCV ALLOW
  LOGONBY IBMVM1
  NAMESAVE TCPIP
  OPTION ACCT MAXCONN 1024 QUICKDSP
  POSIXINFO UID 7 GNAME security
  CONSOLE 0009 3215 T
  [...]
```

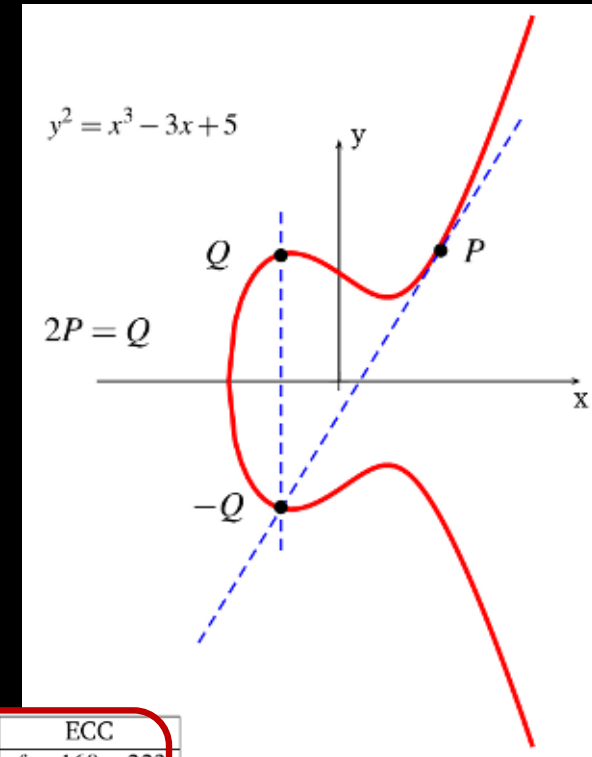
How do I... use Elliptic Curve with the TLS Server

PTF for APAR PI99184 -

http://www.vm.ibm.com/newfunction/#elliptic_support

- Elliptic Curve variants of many major ciphers now available for the TLS Server
 - Not enabled by default
 - Currently lacks hardware acceleration
 - Still faster/stronger than asymmetric algorithms based on prime factorization
- Elliptic Curve operations available for certain asymmetric operations as well as key exchange algorithms
- Important update for future growth (TLS 1.3 will be made exclusively of Elliptic Curve ciphers)

Bits of Security	Symmetric Algorithm	RSA	ECC
80	2TDEA	$k = 1024$	$f = 160 - 223$
112	3TDEA	$k = 2048$	$f = 224 - 255$
128	AES-128	$k = 3072$	$f = 256 - 383$
192	AES-192	$k = 7680$	$f = 384 - 511$
256	AES-256	$k = 15360$	$f = 512+$



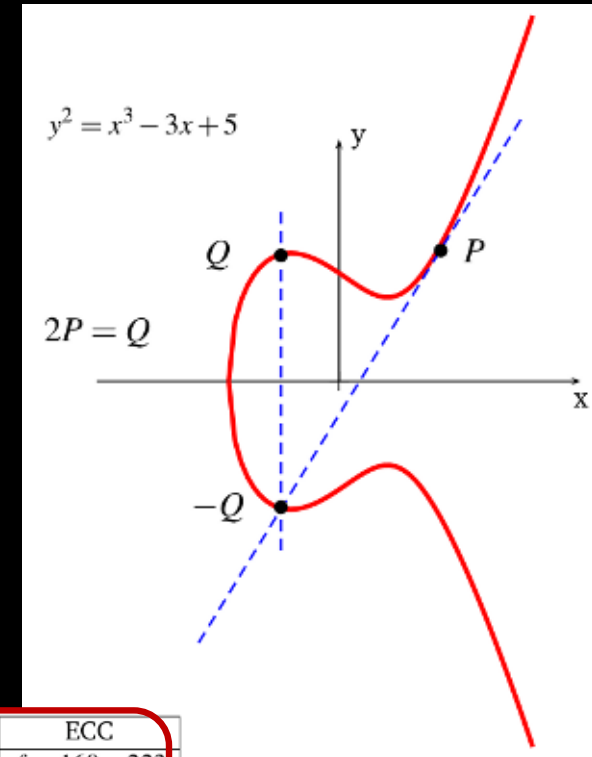
Notes on Elliptic Curve Crypto

PTF for APAR PI99184 –

http://www.vm.ibm.com/newfunction/#elliptic_support

- You don't necessarily need new certificates
 - EC primarily appears as part of the key exchange protocols
 - RSA and DSA certificates will still work with Elliptic Curve ciphers
 - EC options are available in **gskkyman**
- Performance report available:
<http://www.vm.ibm.com/perf/reports/zvm/html/4q8qk.html>

Bits of Security	Symmetric Algorithm	RSA	ECC
80	2TDEA	$k = 1024$	$f = 160 - 223$
112	3TDEA	$k = 2048$	$f = 224 - 255$
128	AES-128	$k = 3072$	$f = 256 - 383$
192	AES-192	$k = 7680$	$f = 384 - 511$
256	AES-256	$k = 15360$	$f = 512+$



Conclusion

Summary

Protecting connectivity to the hypervisor is a key part of a security policy. **z/VM offers you the controls** to restrict ports, enable timeouts, and manage access

The TLS/SSL service virtual machines scale to handle encrypted traffic to (and inside) the hypervisor

z/VM 7.1 delivers enhanced function:

Updated support for CPACF, Elliptic Curve, and TRNG (on the z14)

Support for the latest Crypto Express features

Updated strong defaults and protocol selection (with z/VM 6.4)

Stronger cryptographic modes, more resilient hashing (with z/VM 6.4)

Select the security policy that is right for you and your company


Thank you!

Brian Hugenbruch



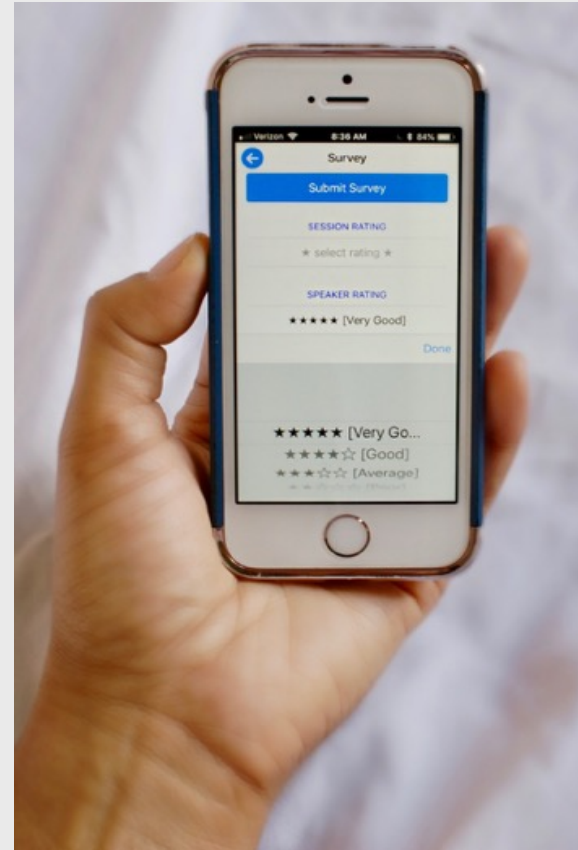
IBM Z Security for Virtualization & Cloud

bwhugen@us.ibm.com

 @Bwhugen

www.vm.ibm.com/devpages/hugenbru

Please complete the Session Evaluation!

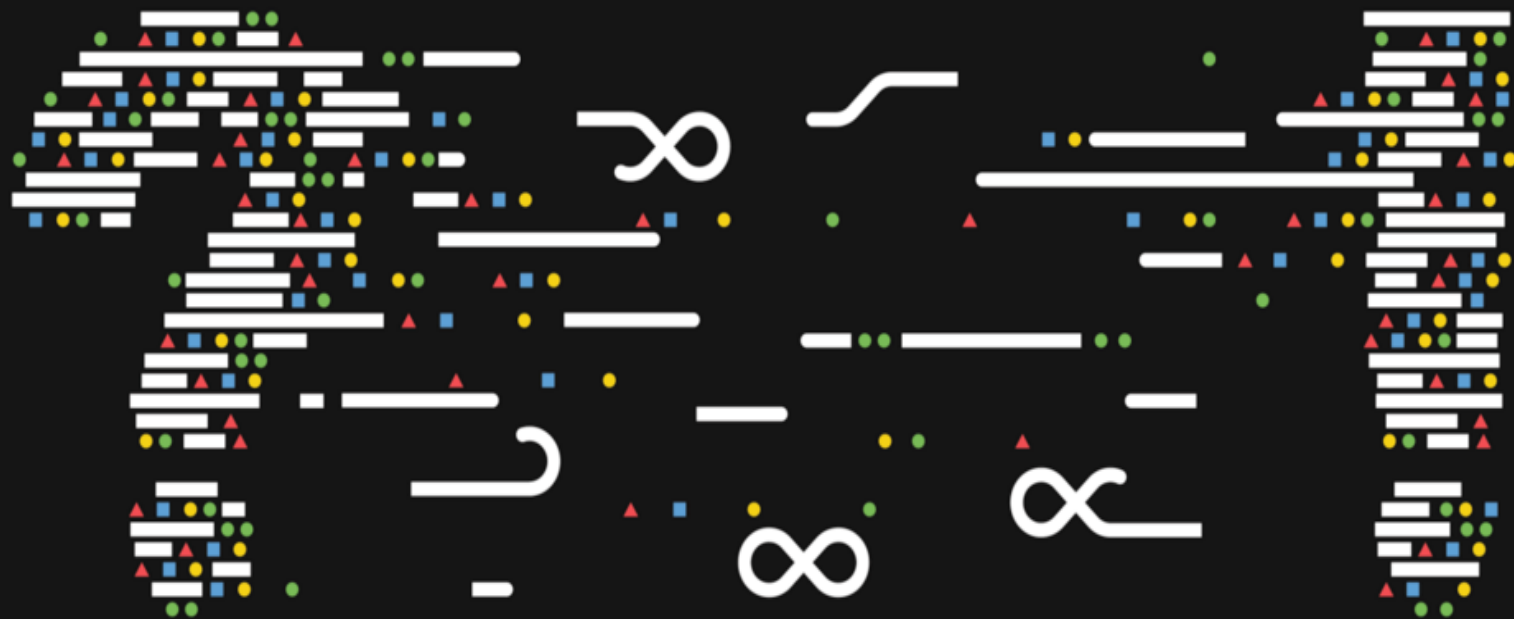


Notices and disclaimers

- © 2019 International Business Machines Corporation.
No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.**
IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- 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 about this publication 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. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.
- .



Break glass in case of
emergency:
Backup Slides

Frequently Asked Questions

Frequently Asked Questions

Does z/VM SSL use the Crypto Express Cards?

Answer: Yes – as of z/VM 6.4 APAR PI72106. Add CRYPTO APVIRT to your PROFILE TCPSSLU or userid of choice (LDAPSRV, GSKADMIN).

Why isn't RACFVM the keystore or certificate store for [insert function here]?

Answer: RACFVM does not support **RACDCERT** or the **DIGTCERT** class, so it cannot provide that functionality.

Can TLS servers for different TCP/IP stacks share the same certificate database?

Answer: Yes, as long as your security policy permits this. Bear in mind that this may require “wildcard” certificates which cover multiple subdomains on your network.

Frequently Asked Questions

Is FIPS Mode for SSLSERV the same as the Common Criteria certified configuration?

Answer: No. FIPS 140-2 and Common Criteria, while analogous in their cipher requirements, are **not** the same – they have slightly different requirements for key length and cipher suite usage. Additionally, FIPS mode may require changes to your certificate database.

Check your security policy; your environment configuration may require either, or both, or something even more stringent.

Can RACF and SSL be combined? What implications does this have for configuration?

Answer: Yes! Just be certain that the SSL Server virtual machines have the authorities it needs in order to do its job. For example:

RACF: Reader access for SSL

Authorize all users to send files to the SSL machine's reader.

If there is already a SSL VMRDR profile defined, alter it, by entering:

- RAC RALTER **VMRDR** SSL00001 UACC(UPDATE)
- RAC RALTER **VMRDR** SSL00002 UACC(UPDATE)
- RAC RALTER **VMRDR** SSL00003 UACC(UPDATE)
- RAC RALTER **VMRDR** SSL00004 UACC(UPDATE)
- RAC RALTER **VMRDR** SSL00005 UACC(UPDATE)
- RAC RALTER **VMRDR** SSLDCSSM UACC(UPDATE)

RACF, SSL and VMSEGMT

If RACF is being used to control restricted segments with the VMSEGMT class, give UPDATE authority for SSL to so SSL has shared write access to the DCSS.TCPIP segment.

```
- RAC RDEFINE VMSEGMT DCSS.TCPIP UACC(NONE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSL00001) ACCESS(UPDATE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSL00002) ACCESS(UPDATE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSL00003) ACCESS(UPDATE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSL00004) ACCESS(UPDATE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSL00005) ACCESS(UPDATE)
- RAC PERMIT DCSS.TCPIP CLASS (VMSEGMT) ID(SSLDCSSM) ACCESS(UPDATE)
```

RACF, SSL, and RACROUTE

To record activity in the RACF system audit trail, they must each be authorized. Enter:

- **RAC SETROPTS CLASSACT(FACILITY)**
- **RAC RDEFINE FACILITY ICHCONN UACC(NONE)**
- RAC PERMIT ICHCONN **CLASS(FACILITY)** ID(SSL00001) ACCESS(UPDATE)
- RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00002) ACCESS(UPDATE)
- RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00003) ACCESS(UPDATE)
- RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00004) ACCESS(UPDATE)
- RAC PERMIT ICHCONN CLASS(FACILITY) ID(SSL00005) ACCESS(UPDATE)

RACF, SSL, and Minidisk Access

If RACF is being used to control minidisk access with VMMDISK class, enable minidisk access for any TCPIP userids that SSL uses.

- RAC PERMIT 6VMTCP40.491 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
- RAC PERMIT 6VMTCP40.492 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
- RAC PERMIT TCPMAINT.591 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
- RAC PERMIT TCPMAINT.198 CLASS (VMMDISK) ID (SSLDCSSM) ACCESS (READ)
- RAC PERMIT 6VMTCP40.491 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
- RAC PERMIT 6VMTCP40.492 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
- RAC PERMIT TCPMAINT.591 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
- RAC PERMIT TCPMAINT.198 CLASS (VMMDISK) ID (SSL00001) ACCESS (READ)
- (repeat for SSL00002, SSL00003 ...)

RPIDIRECT should cover these already ...

Back-Up Slides:

HOW TO BE YOUR OWN CERTIFICATE AUTHORITY IN Z/VM TLS/SSL

How To Be Your Own Certificate Authority

Problem: Obtaining certificates from a trusted Certificate Authority is good for external-facing zones ... but paying money for the privilege of an officially recognized certificate may be beyond the needs of your environment.

Solution: Be your own Certificate Authority

- Can answer certificate requests using *gskkyman*
- Useful for test-oriented or internal-only environments

References:

- *z/VM TCP/IP Planning and Customization*, Chapter 18
- *z/VM TCP/IP LDAP Administrator's Guide*, Chapter 15

How To Be Your Own Certificate Authority

Certificate Authority (System A)	Server or Client (System B)
Step 1 - Create a key database	
Create a key database using the gskkyman command: <ul style="list-style-type: none">From the Database Menu, select option 1 - Create new database See "Creating, Opening and Deleting a Key Database File" on page 203 for details.	Create a key database using the gskkyman command: <ul style="list-style-type: none">From the Database Menu, select option 1 - Create new database See "Creating, Opening and Deleting a Key Database File" on page 203 for details.
Step 2 - Create a Root Certificate Authority certificate	
Create a Certificate Authority certificate: <ul style="list-style-type: none">From the Key Management Menu, select option 6 - Create a self-signed certificateFrom the Certificate Type menu, select one of the CA values for your certificate type See "Creating a Self-Signed Server or Client Certificate" on page 208 for details.	No action required.
Step 3 - Create a certificate request	
No action required.	Create a certificate request: <ul style="list-style-type: none">From the Key Management Menu, select option 4 - Create new certificate requestFrom the Certificate Type menu, select one of the certificate types See "Creating a Certificate Request" on page 211 for details.

How To Be Your Own Certificate Authority

Step 4 - Send the certificate request to the CA

No action required.

Send the certificate request to the CA:. See [“Sending the Certificate Request”](#) on page 217.

Step 5 - Sign the certificate request

To sign the certificate request, the **gskkyman** command must be issued using command-line options (see [“GSKKYMANTM Command Line Mode Syntax”](#) on page 237 for a description of the options). The **gskkyman** command must be issued with the following parameters:

```
gskkyman -g -x num-of-valid-days  
-cr certificate-request-file-name  
-ct signed-certificate-file-name  
-k CA-key-database-file-name  
-l label
```


How To Be Your Own Certificate Authority

Step 6 - Send the signed CA certificate and the newly signed certificate to the requestor	
Export the signed CA certificate (created in Step 2) to a Base64 file (DER or PKCS #7) See "Copying a Certificate Without its Private Key" on page 222. Send (for example, without its private key ftp) the Base64 file and the newly signed certificate (created in Step 4) to the requestor.	No action required.
Step 7 - Import the CA certificate	
No action required.	Import the CA certificate. See "Importing a Certificate from a File as a Trusted CA Certificate" on page 231.
Step 8 - Receive the signed certificate	
No action required.	Receive the signed certificate. See "Receiving the Signed Certificate or Renewal Certificate" on page 217. Note: Depending upon the SSL application, you may need to either send the CA certificate to the client, or the server application may actually present the certificate to the client for them during SSL session setup.

Back-Up Slides:

DEBUGGING THE TLS/SSL SERVER

TLS/SSL Server: Debugging

Common data you may need to debug SSL server problems:

- TCPIP DATA (connection to the TCP/IP stack)
- DTCPARMS (server configuration, SSLDCSS configuration)
 - *Most common problems tend to be either a misconfiguration of DTCPARMS or a DTCPARMS / TCPIP mismatch*
- PROFILE TCPIP (stack configuration)
- SSL, TCP/IP and SSL DCSS Management Agent server console messages
- SSLADMIN or NETSTAT command responses
- GSKADMIN console information
- Trace output from SSL or TCP/IP

TLS/SSL Server: Debugging

Problem: The SSL server does not initialize and run SSLSERV MODULE

Symptoms:

- TCPIP starts, but SSL server and protected services do not
- Console messages for the SSL server which resemble:

```
DTCRUN1028E :Stack.TCPIP11 specified in GDLRCT2 DTCPARMS D1 does not match  
            "TcpipUserid TCPIP10" in the TCPIP DATA file  
DTCRUN1099E Server not started - correct problem and retry
```

TLS/SSL Server: Debugging

Problem: The SSL server does not initialize and run SSLSERV MODULE

Analysis:

- Check the SSL server console for messages
- Verify that the TCPIPUSERID statement in TCPIP DATA lists the correct TCPIP virtual machine for your SSL server
- Confirm DTCPARMS settings for **:stack.** tags and **:vmlink.** tag
- For an SSL pool server, confirm that the server has been enrolled in the appropriate SFS file pool, and that an alias to the (common-use) PROFILE EXEC is in place
- For an SSL pool server (and, the case of having attempted a restart of the subject server) confirm that DTCPARMS configuration has not been changed, while one or more other pool servers remain in operation

TLS/SSL Server: Debugging

Problem: the server cannot use the key database

Symptoms:

- SSL server does not start
- Console messages for the SSL server which resemble:

```
DMSOVZ2113E Object does not exist: '/../VMSYSU:GSKADMIN/etc/gskadl'  
DTCRUN1001E "OPENVM MOUNT '/../VMSYSU:GSKADMIN/etc/gskadl /" failed with  
            return code 28  
DTCRUN1099E Server not started - correct problem and retry
```

TLS/SSL Server: Debugging

Problem: the server cannot use the key database

Analysis:

- Verify that the Byte File System (BFS) parameters for the DTCPARMS **:mount.** tag
- Confirm that the necessary file permissions have been established
 - Database.kdb, Database.rdb, Database.sth
- Confirm that the file pool server for the BFS user space (**VMSYSU**, by default) is operational
- Use the GSKKMAN utility to confirm that the key database has been properly created, and that the correct database has been identified via the VMSSL command KEYFILE operand

TLS/SSL Server: Debugging

Problem: a server cannot use the session cache

Symptoms:

- TCPIP and SSL pool initialize properly
- Connections suddenly cannot be **re**-established
- SSLADMIN messages which resemble the following:

```
DTCSSL2421E SSL00001: Communication error: Connection timed out
```


TLS/SSL Server: Debugging

Problem: a server cannot use the session cache

Analysis:

- Verify that the SSL DCSS Management Agent is operational
 - QUERY <userid> should indicate that the machine is running disconnected:

```
query sslcsm
SSLDCSSM - DSC
Ready;
```
- Verify that SSLDCSSM has been configured properly
 - Check DTCPARMS and configuration files
 - Issue CP QUERY NSS commands
 - **Class E privilege** required for the issuing userid
 - User count should match pool size plus one (SSL* and DCSSM) if servers are running

Output should look similar to the following:

```
--> CP QUERY NSS NAME TCPIP MAP
FILE FILENAME FILETYPE MINSIZE BEGPAG ENDPAG TYPE CL #USERS PARMREGS VMGROUP
9539 TCPIP DCSS N/A 10000 100FF SN R 00006 N/A N/A

--> CP QUERY NSS USERS TCPIP
FILE FILENAME FILETYPE CLASS
9539 TCPIP DCSS R

SSL00005 SSL00004 SSL00002 SSL00003 SSL00001 SSLDCSSM
```

(continued ...)

TLS/SSL Server: Debugging

Problem: a server cannot use the session cache

Analysis:

- Verify that SSLDCSSM has been initialized prior to the SSL server
 - `DTCRUN1043I Initiating XAUTOLOG of server SSLDCSSM`
This message should appear in the TCPIP stack's console log prior to any SSL configuration / initialization messages
- Confirm that the necessary NAMESAVE statements are present in the CP directories for the SSL server and its DCSS Management Agent

TLS/SSL Server: Debugging

Problem: The server cannot connect to the TCP/IP virtual machine

Analysis:

- Verify the TCPIPUSERID statement in TCPIP DATA file
 - should cite the correct TCP/IP server virtual machine
- Confirm that the correct TCP/IP server is identified by a DTCPARMS **:stack.** tag defined for the subject SSL server
- Verify that the TCP/IP server is started
- Check the TCP/IP server console for messages that indicate a problem. (*z/VM: TCP/IP Messages and Codes*)
- Use the FLOW or DEBUG traces to gather additional information. Update the DTCPARMS **:parms.** tag for the SSL server to include the TRACE FLOW or TRACE DEBUG operand, then start the server. This will provide debug information during the server start up.

TLS/SSL Server: Debugging

Problem: Incorrect parameters are passed to SSL server

Symptom: SSL server is running, but not behaving as expected

Analysis:

- Use SSLADMIN QUERY STATUS to determine which options are in effect
- Check that all parameters are correctly specified in the DTCPARMS :parms. Tag
- Compare parameters against message DTCRUN1011I in the server console

TLS/SSL Server: Debugging

Problem: Protected application server (e.g., FTP) shuts down at start-up

Symptoms:

- Console files received from application userids on autolog of TCPIP virtual machine
- Application server cannot be autologged, will not respond to commands

TLS/SSL Server: Debugging

Problem: Protected application server (e.g., FTP) shuts down at start-up

Analysis:

- Confirm SSL server is running (NETSTAT CONFIG SSL)
- Confirm SSL server is listening (NETSTAT CONN or NETSTAT ALLCONN)
- Verify the SSLSERVERID statement in PROFILE TCPIP reflects the correct SSL server configuration
- Check the application server console for indications of problems. (z/VM: *TCP/IP Messages and Codes*) For example:

```
12:30:46 DTCFTS8467E Error verifying TLS label NOTTHERE: Label is not recognized
```

TLS/SSL Server: Debugging

Problem: Protected application server (e.g., FTP) shuts down at start-up

Analysis:

- Using the GSKKYMAN utility, verify that the TLSLABEL specified is present in the certificate database, and conforms to naming requirements
 - On GSKADMIN or other authorized userid, invoke *gskkyman*
 - Open the appropriate certificate database `<filename>.kdb`
 - Choose option 1, “Manage keys and certificates”
 - The certificate with key with the correct TLSLABEL should appear on this list
- Verify the TLSLABEL statement and the correct value have been specified in the application server configuration file:
 - PROFILE TCPIP (or its equivalent) for TELNET
 - SMTP CONFIG (or its equivalent) for SMTP
 - SRVRFTP CONFIG (or its equivalent) for FTP
- An incorrect or misspelled TLSLABEL value in an application server configuration file can prevent such a server from initializing

TLS/SSL Server: Debugging

Problem: Connection to protected application cannot be established

Symptom, z/VM FTP:

220 Connection will close if idle for more than 5 minutes.

>>>AUTH TLS

421 Temporarily unable to process security

Command:

Symptom, z/VM Telnet:

VM TCP/IP Telnet Level 610

SSL Server is not available on local system.

Quitting...bye

TLS/SSL Server: Debugging

Problem: Connection to protected application cannot be established

Analysis:

- Confirm SSL server is running (NETSTAT CONFIG SSL)
- Confirm SSL server is listening (NETSTAT CONN or NETSTAT ALLCONN)
- Use SSLADMIN QUERY STATUS or NETSTAT CONFIG SSL to determine the current number and maximum number of active sessions
- Check SSL server console log for messages
- Issue SSLADMIN TRACE CONN
- Activate TCPIP tracing (SSL, TCPUP, TCPDOWN) to gather more data

TLS/SSL Server: Debugging

Problem: Connection closes due to errors

Analysis:

- Verify the certificate label is correct:
 - *gskkyman* certificate label, in the appropriate database
 - TLSLABEL on PORT statement or in application server configuration
- Verify that the certificate has not expired
 - View certificate information in *gskkyman*
- Verify that the SSL server is accessing the most recent certificate updates (SSLADMIN REFRESH)
- Check SSL Server console for messages
- Issue SSLADMIN TRACE CONNECTIONS to gather more data

TLS/SSL Server: Debugging

Problem: Incorrect input or output inside a secure connection

Analysis:

- Verify that the subject connection has been established
 - SSLADMIN QUERY SESSIONS
- Check messages from the SSL server for any problems
 - SSLADMIN CLOSECON
- Verify that data is flowing correctly through the server
 - SSLADMIN TRACE CONNECTIONS DATA
 - Try connection again after Trace has been configured
 - Consider limiting the trace to a specific IP address / port