WAVV, Colorado Springs, CO
April 16 – April 19th, 2011

z/VM SSL Server Update

Migrating to Multiple SSL Server Support for z/VM 5.4 and 6.1

Miguel Delapaz
z/VM Development

Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see http://www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

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

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

This presentation covers:

- **About SSL for z/VM**

- **Multiple SSL Server Support**
  - Overview
  - Installation and Migration
  - Configuration (Server, Clients, Certificates)
  - Usage and Status
  - Debugging

About SSL for z/VM

About SSL for z/VM

Overview

- SSL (Secure Sockets Layer) was developed to provide point-to-point encryption of TCP/IP traffic
- Standardized by RFC 2246 as TLS (Transport Layer Security)
- Provides security in a z/VM environment for any server associated with a TCP/IP stack

About SSL for z/VM

z/VM 5.3.0

- Linux-based SSL Server
- Added TLS, support for dynamic SSL, support for certain z/VM clients
- Follow-on APAR for increasing concurrent connections

z/VM 5.4.0

- CMS-based SSL Server (PK65850 and associated service)
- BFS for storing certificate database
- System SSL v1.10 (AES ciphers)

z/VM 6.1.0

- CMS-based SSL Server is part of the base

About SSL for z/VM

What’s Not Supported?

- Some forms of hardware encryption
  - CPACF: yes
  - Crypto accelerators / coprocessors: no

- IPv6

About SSL for z/VM

Performance Concerns for CMS-based server …

- The number of connections supported in 5.4 was limited to 1000 per server
- Processor requirements greater for similar workloads
- Statement released, as a part of an initial SSL Server Performance Report, that this discrepancy would be fixed

Multiple SSL Server Support

- **Overview**
- Installation and Migration
- Configuration
- Usage and Status
- Debugging

For more information, refer to: http://www.vm.ibm.com/related/tcpip/tcsslspe.html

Multiple SSL Server Support

Overview

- Can now deploy multiple SSL servers for a single TCPIP stack
  - Configured as a POOL of virtual machines
  - Use same configuration, respond to same commands
  - Server status is collated and organized

- Increases availability by providing for backup servers

Multiple SSL Server Support

Overview

- Improves server performance by changing internal work-handling model
  - A completely new code implementation
  - Works on select() instead of relying on large numbers of threads
  - Tracing output overhauled

- Increases scalability through additional servers
  - Default: 5 servers, 600 connections = **3000** secure connections

Multiple SSL Server Support

Overview

But should we use a single server, or multiple servers?

- If supporting **a max of 100 concurrent secure connections**, a single SSL server should suffice
- If supporting **100 - 600 concurrent secure connections**, a server pool of five servers, with each defined to support a maximum of 120 sessions, should be considered
  - Reduce CPU on a per-server basis
- To support **more than 600 concurrent connections**, use of the IBM defaults for the size of the server pool and the SSLLIMITS statement should be considered

Multiple SSL Server Support

Overview

- The SSL pool servers must share the same configuration (DTCPARMS)

- The number of active pool servers can be dynamically increased

- Incoming secure connections are routed to the first active server in the pool
  - First active server must be fully utilized before second server is used
  - If all active servers are used, TCPIP will attempt to activate more

Multiple SSL Server Support

- Overview
- **Installation and Migration**
- Configuration
- Usage and Status
- Debugging

For more information, refer to: http://www.vm.ibm.com/related/tcpip/tcspeins.html

Multiple SSL Server Support

Installation and Migration

- PTFs:
  - **UK59535** – Release 540
  - **UK59536** – Release 610

- APARs:
  - **PK97437**: SSLADMIN, TCPRUN and Related Packaging Changes
  - **PK97438**: SSLSERV Module Updates
  - **PK75662**: TCPIP Module Updates

- Enable FIPS 140-2 (PM10616)
  - **UK61574 –** Release 610

Multiple SSL Server Support

Installation and Migration

- If the SSL server is not currently in use on the system, service can be applied without the need for up-front configuration change

- If the SSL server **IS** in use, configuration must be done before issuing PUT2PROD or TCP2PROD
  - Otherwise, the SSL server will not properly initialize and will no longer function

Multiple SSL Server Support

Installation and Migration

- New server virtual machine: SSLDCSSM
  - **Required** whether using single-server support or multiple!
  - Must be defined in user directory

- DTCPARMS definitions in new IBM DTCPARMS file

- New SSL pool: SSL*
  - Needed to run Multiple SSL Server Support
  - Should be defined in user directory
  - DTCPARMS definitions included in new IBM DTCPARMS file

- Standalone Server note:
  - The existing :nick.SSLSERV :type.server entry for the SSLSERV user ID now is listed in this file in comment form only

Multiple SSL Server Support

Installation and Migration

- SSLPOOL SAMPEXEC
  - generates planning information to assist with defining a "pool" of SSL server machines for a given TCP/IP stack virtual machine
    - Use the “NOPOOL” option for planning the new config of a single server
  - sample CP directory definitions, sample DTCPARMS file entries
  - Can also enroll subject server machines in a designated SFS file pool, and establish files and authorizations to facilitate their use
    - **VMSYS** filepool used by default

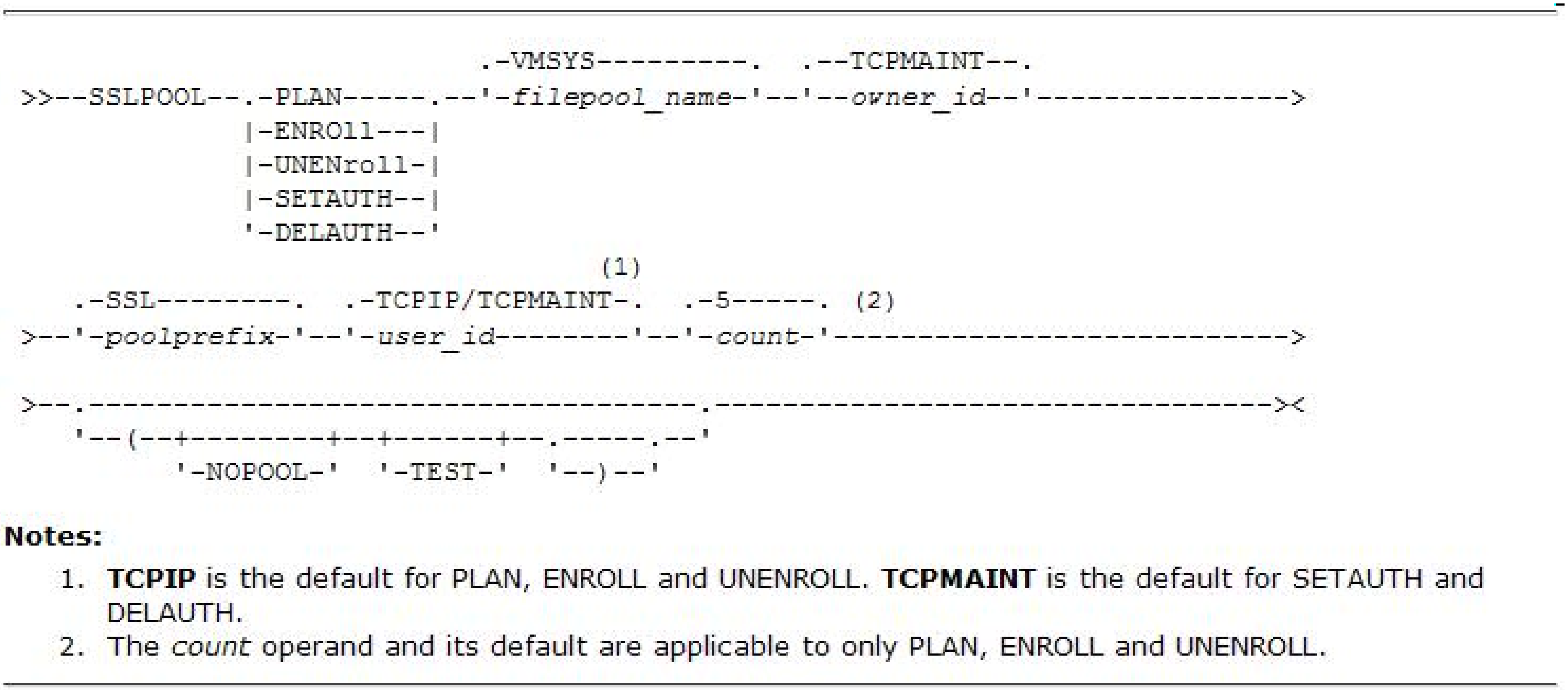
- Shipped as a sample exec

- Rename, move to 191 disk

http://www.vm.ibm.com/related/tcpip/tcspecsp.html

Multiple SSL Server Support

Installation and Migration



```
                           .-VMSYS---------.  .--TCPMAINT--.
>>--SSLPOOL--.-PLAN-----.--'-filepool_name-'--'--owner_id--'---------------->
             |-ENROll---|
             |-UNENroll-|
             |-SETAUTH--|
             '-DELAUTH--'
                                     (1)
   .-SSL--------.  .-TCPIP/TCPMAINT-.  .-5-----. (2)
>--'-poolprefix-'--'-user_id--------'--'-count-'---------------------------->

>--.------------------------------------.----------------------------------><
   '--(--+--------+--+------+--.-----.--'
         '-NOPOOL-'  '-TEST-'  '--)--'
```

Notes:

1. **TCPIP** is the default for PLAN, ENROLL and UNENROLL. **TCPMAINT** is the default for SETAUTH and DELAUTH.
2. The *count* operand and its default are applicable to only PLAN, ENROLL and UNENROLL.

Multiple SSL Server Support

- Overview
- Installation and Migration
- **Configuration**
- Usage and Status
- Debugging

Multiple SSL Server Support

Configuration

1. Plan out user directory changes (SSLPOOL); update the user directory and bring changes online.

```
USER SSLDCSSM LBYONLY 32M 64M GE
   INCLUDE TCPCMSU
    LOGONBY TCPMAINT GSKADMIN
   NAMESAVE TCPIP
   OPTION QUICKDSP SVMSTAT
   LINK 6VMTCP10 0491 0491 RR
   LINK 6VMTCP10 0492 0492 RR
   LINK TCPMAINT 0591 0591 RR
   LINK TCPMAINT 0592 0592 RR
   LINK TCPMNT10 0198 0198 RR
   MDISK 0191 3390 2240 5 12345B MR READ WRITE MULTI
```

http://www.vm.ibm.com/related/tcpip/tcspesvm.html

Multiple SSL Server Support

Configuration

- **SSLDCSSM** is required to support connection caching
  - Data stored in a DCSS used by one SSL server pool
  - New virtual machine owns the DCSS
  - Tied through DTCPARMS to a single SSL server pool; cannot be shared among different pools and different TCP/IP stacks!

- At a minimum, define the 191 minidisk for SSLDCSSM as a 1 cylinder minidisk

- Class E privilege is required for SSLDCSSM

- NAMESAVE must match the TCPIP stack virtual machine userid

- The SSL DCSS Management Agent server **must be defined** whether using a single-server or multi-server SSL implementation

Multiple SSL Server Support

Configuration

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

- Defines a pool of userids of format SSLnnnnn (SSL00001 through SSL00005)
- The lower bound of an SSL pool **must be specified as 1**
- Additional SSL servers could be deployed without the need to restart the TCP/IP server:
  - CP directory change to the size of the server pool
    - Update the SSLLIMITS statement, if workload needs to be rebalanced or if new maximum values need to be configured
    - OBEYFILE or NETSTAT OBEY

http://www.vm.ibm.com/related/tcpip/tcspecsp.html

Multiple SSL Server Support

Configuration

```
PROFILE TCPSSLU
* For Multiple SSL Server Support
   IPL CMS PARM FILEPOOL VMSYS
   IUCV ALLOW
   LOGONBY TCPMAINT GSKADMIN
   MACH XA
   NAMESAVE TCPIP
   OPTION ACCT MAXCONN 1024 QUICKDSP SVMSTAT APPLMON
   POSIXINFO UID 7 GNAME security
   SHARE RELATIVE 3000
   CONSOLE 0009 3215 T
   [SPOOL, LINK statements would follow]
```

- One PROFILE required for each SSL* POOL defined; cannot share
- NAMESAVE must match the associated TCPIP stack virtual machine
- GSKADMIN and certificate management are not impacted by these updates

Multiple SSL Server Support

Configuration

2. Configure PROFILE TCPIP

   - ~~**AUTOLOG** <userid>~~
     SSL servers should no longer be included in AUTOLOG statements, nor brought up by AUTOLOG1 or similar mechanisms.
     - Any single-SSL server in the AUTOLOG statement will be removed and not brought online
     - any SSL pool machine in the AUTOLOG statement will be ignored

   - **SSLSERVERID** *userid* **TIMEOUT** *seconds*
     Delays start of other servers until SSL server (or pool) is online. For a pool, *userid* should be in the following format:

     SSLSERVERID *

http://www.vm.ibm.com/related/tcpip/tcspeslc.html

Multiple SSL Server Support

Configuration

- **SSLLIMITS MAXSESSIONS** <number> **MAXPERSSLSERVER** <number> Controls the number of secure connections handled by a member of the SSL pool.
  - Default values: MaxSessions = 3000, MaxPerSSLServer = 600
  - MaxPer.. should divide evenly into MaxSessions
  - MaxPer.. cannot exceed 1000

- Consider how many connections should be managed by an individual server, based upon available resources

- If adding servers dynamically, remember to update SSLLIMITS so that all servers are included in a maximum workload

- If subtracting servers dynamically, remember to update SSLLIMITS so that the smaller number of servers can still support the MaxSession value

Multiple SSL Server Support

Configuration

3. Configure DTCPARMS
   a) SSL Server or SSL Pools

:Admin_ID_list.	User IDs authorized for privileged commands
:Mixedcaseparms.	Parameters in mixed case
:Mount.	Location of the certificate database. Default is /etc/gskadm/
:Parms.	As per the VMSSL command
:Stack.	Associated TCPIP virtual machine *This tag is required; otherwise, the SSL server / pool cannot be identified during stack initialization!*
:Timestamp.	On/Off for timestamps on terminal messages and command responses
:Timezone.	Set timezone of server
:Vmlink.	Sets a Pool member's SFS space

Multiple SSL Server Support

Configuration

3. Configure DTCPARMS

   b) SSL DCSS Agent

:For.	User ID or pool ID on which DCSS Agent is acting
:Stack.	Associated TCPIP virtual machine
:DCSS_Parms.	<NONE> -- subject TCPIP is not configured for SSL support <DEFAULT> -- subject TCPIP is configured for SSL, and a DCSS is in use for the shared session cache *dcssname hexpage1-hexpage2* -- subject TCPIP is configured for SSL, and specific parameters are to be used for definition of an SSL shared session cache DCSS

http://www.vm.ibm.com/related/tcpip/tcspedtp.html

Multiple SSL Server Support

Configuration

3. Configure DTCPARMS

   b) TCPIP

:Attach.	
:Authlog.	
:VCTC.	
:VNIC.	
:DCSS_Parms.	<NONE> -- subject TCPIP is not configured for SSL support <DEFAULT> -- subject TCPIP is configured for SSL, and a DCSS is in use for the shared session cache *dcssname hexpage1-hexpage2* -- subject TCPIP is configured for SSL, and specific parameters are to be used for definition of an SSL shared session cache DCSS

http://www.vm.ibm.com/related/tcpip/tcspestc.html

Multiple SSL Server Support

Configuration

4. Setup Certificate Database

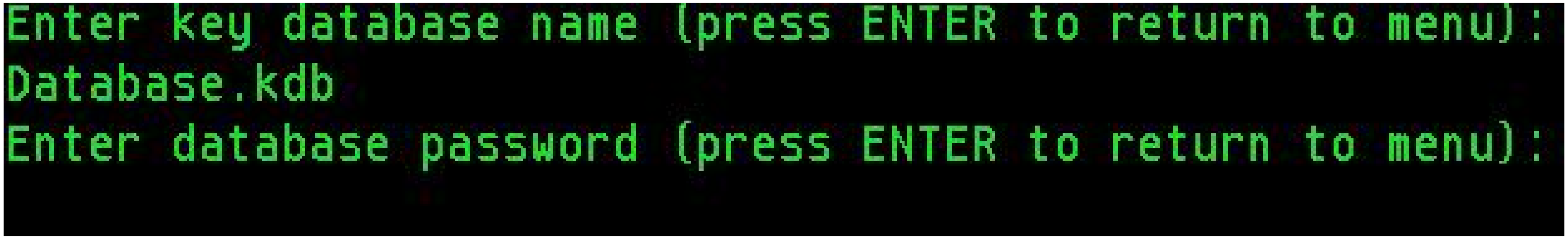
About gskkyman

- First available in z/VM 5.3.0. – LDAP server
- Came to z/VM by way of z/OS
- Manages databases stored in a Byte-File System
- SSL Servers and LDAP Servers can share databases and certificates
- GSKADMIN user ID created to manage gskkyman

Multiple SSL Server Support

Opening a Certificate Database

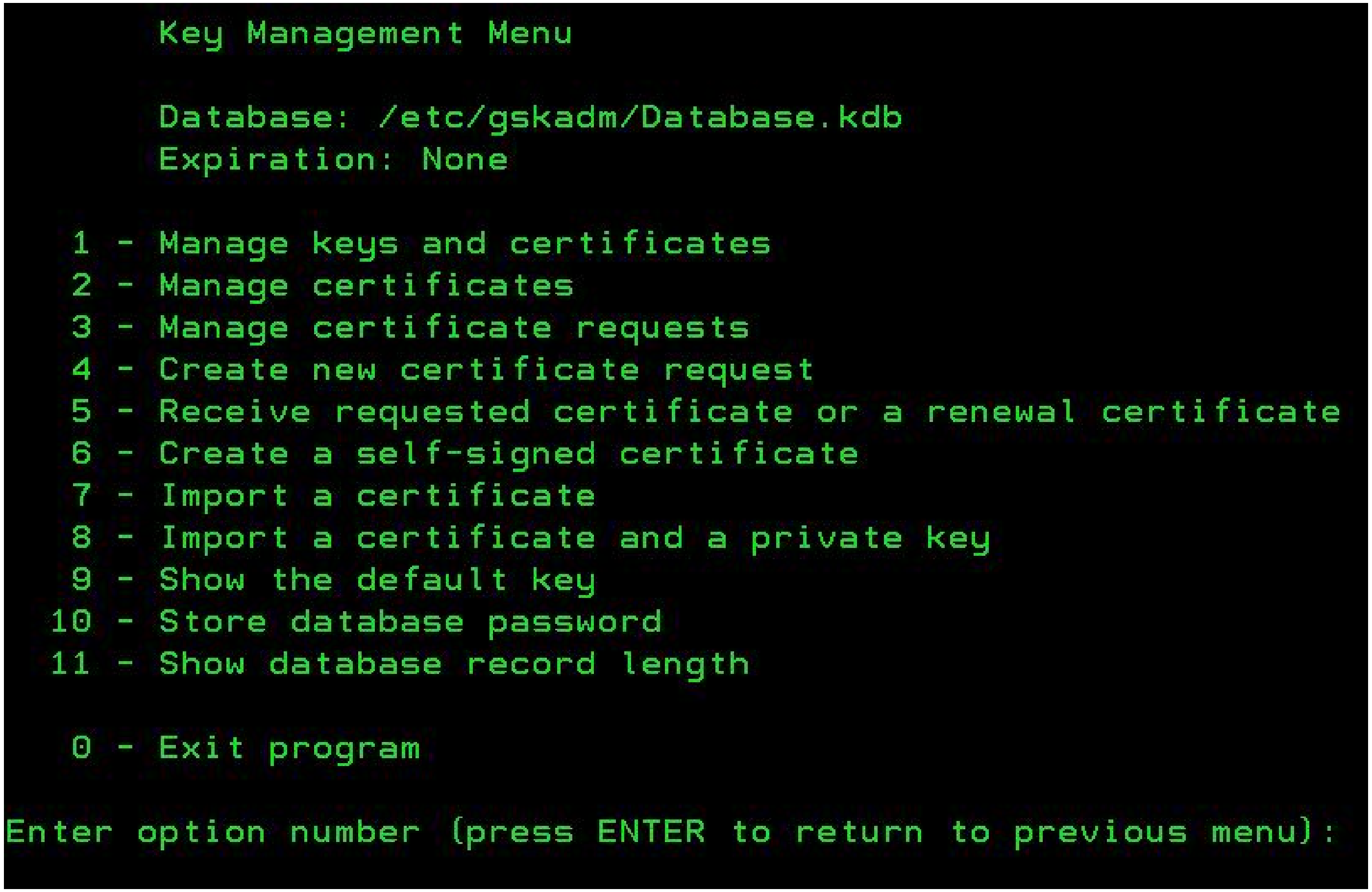
- gskkyman option 2. Open Database



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

- **GSKADMIN automatically mounts and accesses the database’s directory**
  - Default database location: **/etc/gskadm**
  - Database should be located at mount point
  - May require manual configuration if not using the defaults

Multiple SSL Server Support



```
       Key Management Menu

       Database: /etc/gskadm/Database.kdb
       Expiration: None

   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):
```

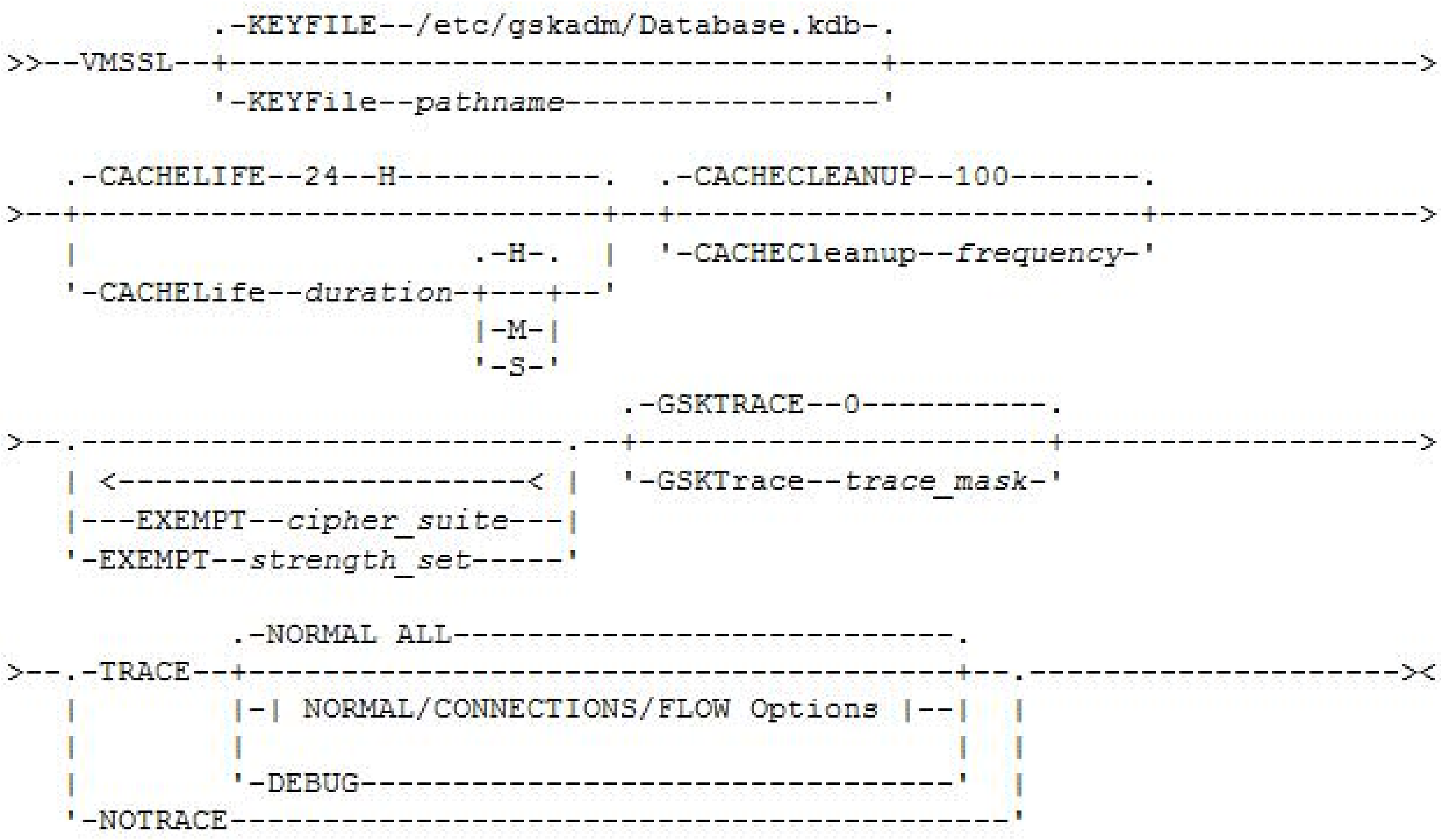
Multiple SSL Server Support

Configuration

5. Configure the SSL server
   - From a command-line invocation of VMSSL
   - In DTCPARMS, on the :Parms. Tag, using the VMSSL operands

Multiple SSL Server Support

Configuration



```
           .-KEYFILE--/etc/gskadm/Database.kdb-.
>>--VMSSL--+-----------------------------------+---------------------------->
           '-KEYFile--pathname-----------------'

   .-CACHELIFE--24--H-----------.  .-CACHECLEANUP--100-------.
>--+----------------------------+--+-------------------------+------------->
   |                     .-H-.  |  '-CACHECleanup--frequency-'
   '-CACHELife--duration-+---+--'
                         |-M-|
                         '-S-'
                                 .-GSKTRACE--0----------.
>--.--------------------------.--+----------------------+------------------>
   | <----------------------< |  '-GSKTrace--trace_mask-'
   |---EXEMPT--cipher_suite---|
   '-EXEMPT--strength_set-----'

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

Multiple SSL Server Support

Configuration

- **VMSSL Changes:**
  - CACHESIZE
    - obsolete (uses DCSS instead)
  - MAXSESSIONS
    - obsolete (SSLLIMITS)
  - MAXUSERS
    - obsolete (SSLLIMITS)
  - CACHELIFE
    - accepts duration of H, M, S
  - CACHECLEANUP
    - new: how often expired entries are removed from the cache
  - TRACE CONN
    - a new length parameter has been added

Multiple SSL Server Support

Configuration

High	Medium	Low	None
3DES_168_SHA	RC4_128_SHA	RC2_40_MD5	NULL
DH_DSS_3DES	RC4_128_MD5	RC4_40_MD5	NULL_SHA
DH_RSA_3DES	RSA_AES_128	DES_56_SHA	NULL_MD5
DHE_DSS_3DES	DH_DSS_AES_128	DH_DSS_DES	
DHE_RSA_3DES	DH_RSA_AES_128	DH_RSA_DES	
RSA_AES_256	DHE_DSS_AES_128	DHE_DSS_DES	
DH_DSS_AES_256	DHE_RSA_AES_128	DHE_RSA_DES	
DH_RSA_AES_256			
DHE_DSS_AES_256			
DHE_RSA_AES_256			

Note 1: Cipher suites can be exempted from processing based on either cipher name or by strength set, per the above – but not both.

Note 2: Exempting by strength automatically exempts a lower strength!

Multiple SSL Server Support

- Overview
- Installation and Migration
- Configuration
- **Usage and Status**
- Debugging

Multiple SSL Server Support

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
  - NETSTAT SSL START SSL00004

Multiple SSL Server Support

Server States

- **Active**
  - This server is logged on, talking to TCPIP and may be able to accept new connections.

- **Eligible**
  - This server has been defined for use, but is not active. (Not logged on, initialized or talking to TCPIP). May become ACTIVE if prompted by TCPIP. Cannot respond to SSLADMIN commands.

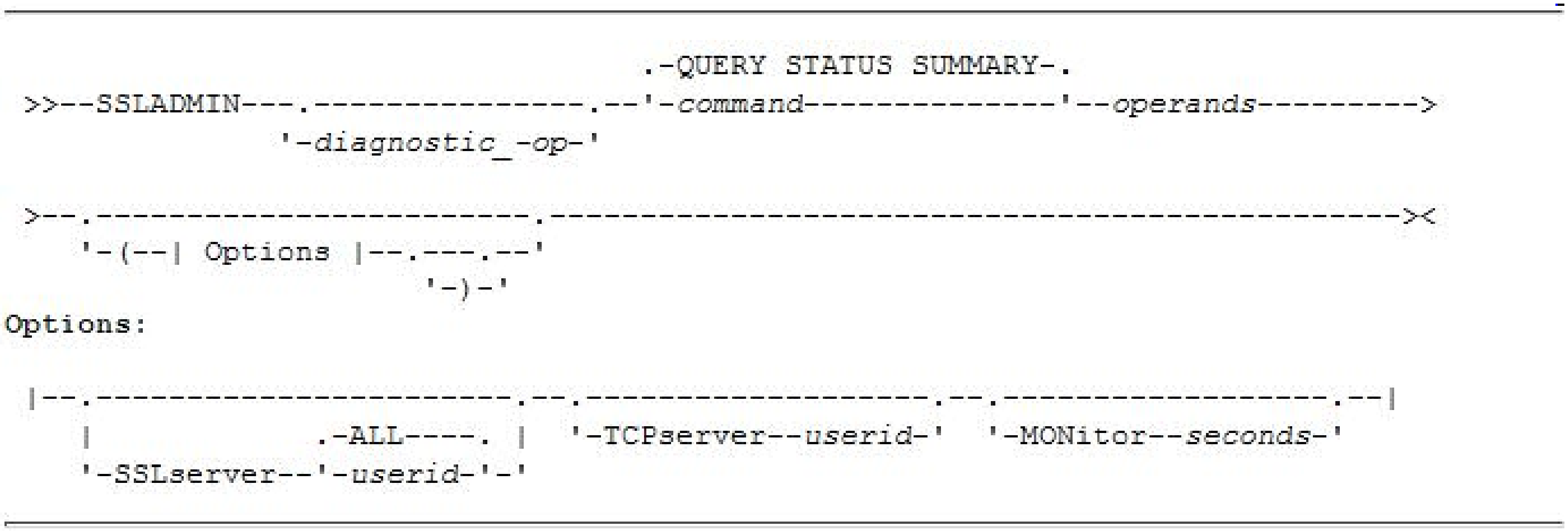
- **Starting**
  - This server is initializing.

- **Stopped**
  - This server was overtly stopped, and will not respond to commands or to TCPIP.

Multiple SSL Server Support

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/tcspecsa.html

Multiple SSL Server Support

SSLADMIN command

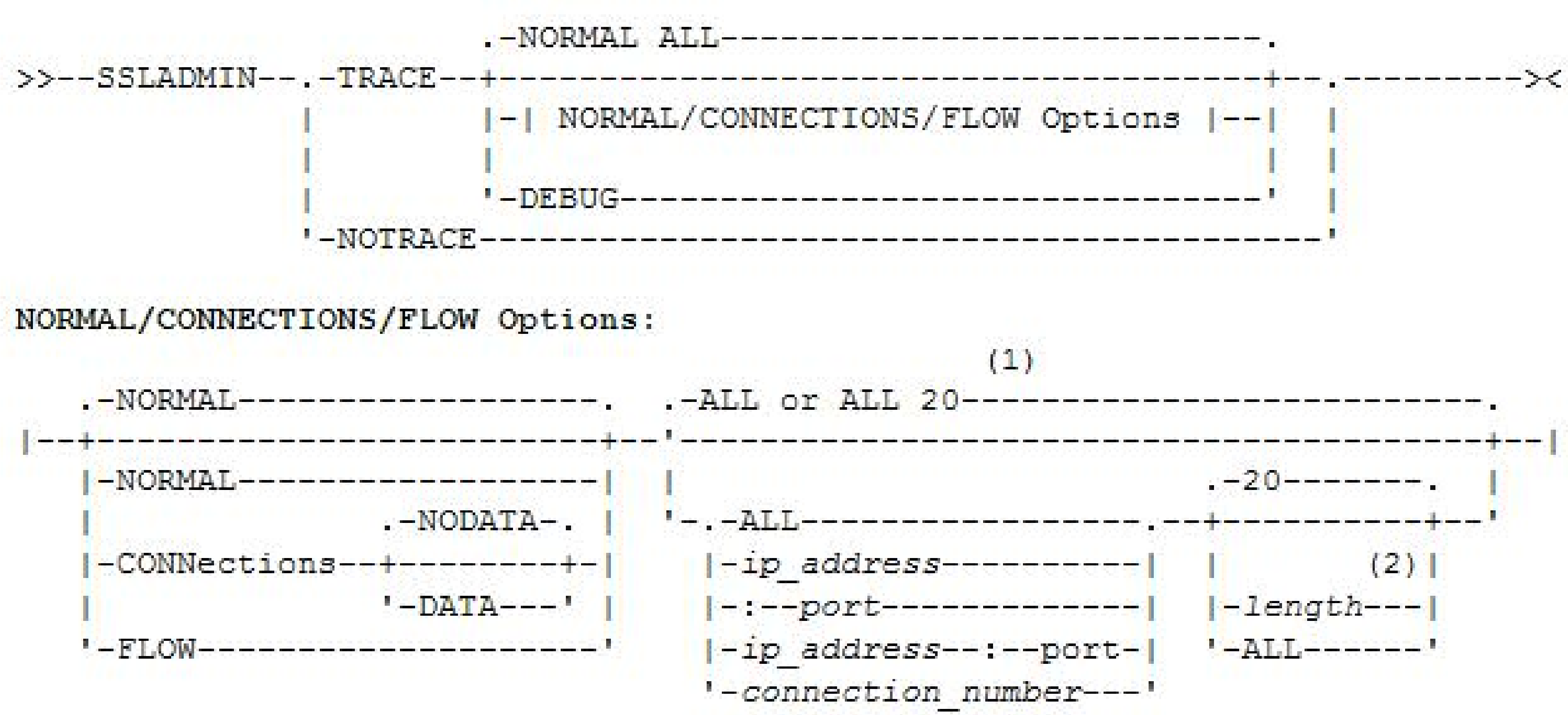
- **CLEAR -** remove userid(s) set by SET
- **CLOSECON** / **LOG** - retrieves console log
- **HELP -** displays help information
- **QUERY**
  - **Status Summary -** returns general server data
  - **Status Details -** returns specific server data
  - **Settings -** returns current command defaults
  - **Cache -** returns cache data
  - **Sessions -** returns data on active secure sessions
  - **Trace -** returns trace settings
- **RESTART -** quiesces and re-IPL's SSL server
- **REFRESH -** re-access 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

http://www.vm.ibm.com/related/tcpip/tcspecsa.html

Multiple SSL Server Support

Tracing

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



```
                       .-NORMAL ALL----------------------------.
>>--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---'
```

Multiple SSL Server Support

Tracing – SSLADMIN options

- **Normal**: records successful connections
- **All**: indicates tracing for all incoming connections
  - This can be delineated by an IP address, port number or connection number
- **Connections**: records state changes and handshake results.
- **Data**: displays the first ***length*** bytes of send/receive entries
- **NoData**
- **Flow**: traces the flow of control and system activity
- **Debug**: extensive tracing for all control and system activities as well as data on ALL connections
  - Usage note: both Trace Flow and Trace Debug generate a lot of data; this not only causes major performance impact but will fill up spool space more quickly.
- **NoTrace**: turns off **all** tracing.

Multiple SSL Server Support

- Overview
- Installation and Migration
- Configuration
- Usage and Status
- **Debugging**

For more information, refer to: http://www.vm.ibm.com/related/tcpip/tcspedgd.html

Multiple SSL Server Support

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

Multiple SSL Server Support

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
```

Multiple SSL Server Support

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

Multiple SSL Server Support

Problem: The SSL 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
```

Multiple SSL Server Support

Problem: The SSL 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 GSKKYMAN 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

Multiple SSL Server Support

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
```

Multiple SSL Server Support

Problem: A server cannot use the session cache

Analysis:

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

```
query ssldcssm
SSLDCSSM - DSC
Ready;
```

(continued ...)

Multiple SSL Server Support

Problem: A server cannot use the session cache

Analysis:

- 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 ...)

Multiple SSL Server Support

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

Multiple SSL Server Support

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.

Multiple SSL Server Support

Problem: Incorrect parameters are passed to the 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

Multiple SSL Server Support

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

Symptoms:

- Console files received from application user IDs on autologof TCP/IP virtual machine
- Application server cannot be autologged, will not respond to commands

Multiple SSL Server Support

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

(continued ...)

Multiple SSL Server Support

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
  - Open the appropriate certificate database <filename>.kdb
  - Choose option 1, “Manage keys and certificates”
  - The certificate with key matching the TLSLABEL should appear in 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

Multiple SSL Server Support

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
```

Multiple SSL Server Support

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

Multiple SSL Server Support

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

Multiple SSL Server Support

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

Questions?

References

Speaker: Miguel Delapaz

- E-mail: migueld@us.ibm.com

z/VM SSL web pages:

- http://www.vm.ibm.com/related/tcpip/vmsslinf.html -- SSL Information
  - All the links in this presentation will be available through this URL
- http://www.vm.ibm.com/related/tcpip/tcsl540.html -- 540 Config and Install
- http://www.vm.ibm.com/related/tcpip/tcsslsvc.html -- SSL Service Notes
- http://www.vm.ibm.com/related/tcpip/ -- z/VM TCPIP

Special Thanks to:

- Brian Hugenbruch (z/VM Security Champion)
- Mark Cibula (z/VM Development)
- Alan Altmark (Lab Services and Training)