z/VM SSL parameters - Things that changed

TCPMAINT

Profile TCPIP

```
 SSLSERVERID * TIMEOUT 60   ; (Identify a SSL server )

 SSLLIMITS MAXSESSIONS 1000 MAXPERSSLSERVER 100

PORT
 992   TCP INTCLIEN NOAUTOLOG SECURE ZVM01

  81   TCP PERFSVM NOAUTOLOG SECURE ZVM01

INTERNALCLIENTPARMS
  PORT        992
  TLSLABEL     ZVM01


SYSTEM DTCPARMS

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

PERFSVM

```
FC MONCOLL WEBSERV ON SSL TCPIP TCPIP 81
```

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

PC3270

```
      Link Parameters  change to PORT 992
      Security Setup   enable Security
```

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


z/VM Security Certificate steps - Things that need to be done

Log on to GSKADMIN

GSKADMIN

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:

select option 1 - Create new database

database name - ex: zVMCerts.kdb
database password - ex: adminpw
reenter password        adminpw
press enter for no password experation
press enter for default record length
enter 1 for fips

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

enter

select option 10 - Store database password

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

enter
```

```
enter 0

openvm list (own
Directory = '/etc/gskadm'
User ID    Group Name  Permissions Type  Path name component
gskadmin   security    rw- --- ---  F    'zVMCerts.kdb'
gskadmin   security    rw- --- ---  F    'zVMCerts.rdb'
gskadmin   security    rw- --- ---  F    'zVMCerts.sth'

openvm permit /etc/gskadm/zVMCerts.kdb rw- r-- ---
openvm permit /etc/gskadm/zVMCerts.rdb rw- r-- ---
openvm permit /etc/gskadm/zVMCerts.sth rw- r-- ---

openvm listf (own
Directory = '/etc/gskadm'
User ID    Group Name  Permissions Type  Path name component
gskadmin   security    rw- r-- ---  F    'zVMCerts.kdb'
gskadmin   security    rw- r-- ---  F    'zVMCerts.rdb'
gskadmin   security    rw- r-- ---  F    'zVMCerts.sth'

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:
2

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

       Key Management Menu

       Database: /etc/gskadm/zVMCerts.kdb
       Expiration: None
       Type: FIPS

   1 - Manage keys and certificates
   2 - Manage certificates
   3 - Manage certificate requests
   4 - Create new certificate request
```

```
   5 - Receive requested certificate or a renewal certificate
   6 - Create a self-signed certificate
   7 - Import a certificate
   8 - Import a certificate and a private key
   9 - Show the default key
  10 - Store database password
  11 - Show database record length

   0 - Exit program

Enter option number (press ENTER to return to previous menu):
4

       Certificate Key Algorithm

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

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

       RSA Key Size

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

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

       Signature Digest Type

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

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

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

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

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

```
  Organizational unit (optional):
systems

  Organization (required):
ZVM

  City/Locality (optional):


  State/Province (optional):


  Country/Region (2 characters - required):
US

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

       Subject Alternate Name Type

   1 - Directory name (DN)
   2 - Domain name (DNS)
   3 - E-mail address (SMTP)
   4 - Network address (IP)
   5 - Uniform resource identifier (URI)

Select subject alternate name type (press ENTER if name is
complete):
2

Enter DNS name (press ENTER to return to menu):
vmlpar.testlpar.com

       Subject Alternate Name Type

   1 - Directory name (DN)
   2 - Domain name (DNS)
   3 - E-mail address (SMTP)
   4 - Network address (IP)
   5 - Uniform resource identifier (URI)

Select subject alternate name type (press ENTER if name is
complete):

enter

Please wait .....

Certificate request created.
Press ENTER to continue.
```

```
       Key Management Menu


   0 - Exit program

Enter option number (press ENTER to return to previous menu):
0
Ready(00001); T=4.17/4.33 16:05:11

openvm list
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links          Bytes Path name
component
06/03/2019 16:05:05   F        1           1098 'zvm01.crq'
03/14/2019 14:09:38   F        1          65088 'zVMCerts.kdb'
06/03/2019 16:04:46   F        1           5088 'zVMCerts.rdb'
11/27/2018 12:50:05   F        1            129 'zVMCerts.sth'
Ready; T=0.01/0.01 16:05:38

openvm get zvm01.crq zvm01 crq a (bfsline NL

filel
      ZVM01    CRQ      W1 V         64         18          1
6/03/19 16:07:33
      PROFILE  EXEC     W2 V         74        198          3
8/24/16 10:47:10

openvm listf (own
Directory = '/etc/gskadm'
User ID    Group Name  Permissions Type  Path name component
gskadmin   security    rw- r-- r--  F    'zvm01.crq'
gskadmin   security    rw- r-- ---  F    'zVMCerts.kdb'
gskadmin   security    rw- r-- ---  F    'zVMCerts.rdb'
gskadmin   security    rw- r-- ---  F    'zVMCerts.sth'
Ready; T=0.01/0.01 09:50:37

send this off to Info Defense group

do the following if needed other wise SF the 3 certs from another
LPAR

** VIP **

GO TO COMMAND PROMPT on PC - enter  certmgr
(see DOC)

** VIP **

GO TO TRUSTED ROOT CERTIFICATION AUTHORITIES
pull down " Primary Certificate Authority "
IND$FILE PUT PRIMARY CER A ( ASCII CRLF RECFM V LRECL 133
GO TO TRUSTED INTERMEDIATE CERTIFICATION AUTHORITIES
```

```
pull down " Intermediate Certificate Authority "
IND$FILE PUT INTERMED CER A ( ASCII CRLF RECFM V LRECL 133

get the Primary and Intermediate cert loaded to the system
and if you have the signed CERT you can load it now as well

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

openvm list
Directory = '/etc/gskadm'
Update-Dt  Update-Tm Type  Links          Bytes Path name
component
07/17/2019 11:53:00   F        1           2000 'primary.cer'
07/22/2019 15:55:41   F        1           1984 'intermed.cer'
06/03/2019 16:05:05   F        1           1098 'zvm01.crq'
06/10/2019 16:14:57   F        1           2427 'zvm01.cer'
06/19/2019 15:00:37   F        1          65088 'zVMCerts.kdb'
06/03/2019 16:04:46   F        1           5088 'zVMCerts.rdb'
11/27/2018 12:50:05   F        1            129 'zVMCerts.sth'
Ready; T=0.01/0.01 11:53:10

gskkyman

       Database Menu


Enter option number:
2

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


       Key Management Menu


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

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

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

Certificate imported.

Press ENTER to continue.
```

```
       Key Management Menu


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

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

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

Certificate imported.

Press ENTER to continue.

 0 - Exit program

enter 0


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

IND$FILE PUT ZVM01 CER A ( ASCII CRLF RECFM V LRECL 133

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

open data base


       Key Management Menu


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

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

Certificate received.

Press ENTER to continue.

       Key Management Menu

   2 - Manage certificates

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

       Certificate List
```

```
        Database: /etc/gskadm/zVMCerts.kdb

   1 - Equifax Secure Certificate Authority
   2 - Equifax Secure eBusiness CA-2
   3 - VeriSign Class 1 Public Primary CA - G2
   4 - VeriSign Class 2 Public Primary CA - G2
   5 - VeriSign Class 3 Public Primary CA - G2
   6 - VeriSign Class 4 Public Primary CA - G2
   7 - VeriSign Class 1 Public Primary CA - G3
   8 - VeriSign Class 2 Public Primary CA - G3
   9 - VeriSign Class 3 Public Primary CA - G3

   0 - Return to selection menu

Enter label number (ENTER for more labels, p for previous list):


        Certificate List

        Database: /etc/gskadm/TstCerts.kdb

   1 - VeriSign Class 4 Public Primary CA - G3
   2 - VeriSign Class 3 Public Primary CA - G5
   3 - PRIMARY

   0 - Return to selection menu

Enter label number (ENTER to return to selection menu, p for
previous list)
0


gskkyman

        Database Menu

        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:
2
```

```
       Key Management Menu

   2 - Manage certificates

Enter option number:
2

       Certificate List

       Database: /etc/gskadm/zVMCerts.kdb

   1 - Equifax Secure Certificate Authority
   2 - Equifax Secure eBusiness CA-2
   3 - VeriSign Class 1 Public Primary CA - G2
   4 - VeriSign Class 2 Public Primary CA - G2
   5 - VeriSign Class 3 Public Primary CA - G2
   6 - VeriSign Class 4 Public Primary CA - G2
   7 - VeriSign Class 1 Public Primary CA - G3
   8 - VeriSign Class 2 Public Primary CA - G3
   9 - VeriSign Class 3 Public Primary CA - G3

   0 - Return to selection menu

Enter label number (ENTER for more labels, p for previous list):
       Certificate List

       Database: /etc/gskadm/TstCerts.kdb

   1 - VeriSign Class 4 Public Primary CA - G3
   2 - VeriSign Class 3 Public Primary CA - G5
   3 - PRIMARY
   4 - INTERMED

   0 - Return to selection menu

Enter label number (ENTER to return to selection menu, p for
previous list):


       Key Management Menu

   1 - Manage keys and certificates


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

       Key and Certificate List

       Database: /etc/gskadm/TstCerts.kdb

   1 - ZVM01
```

```
Enter label number (ENTER to return to selection menu, p for
previous list):
1

       Key and Certificate Menu

       Label: ZVM01

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

   0 - Exit program

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

                 Label: ZVM01
             Record ID: 16
      Issuer Record ID: 15
               Trusted: Yes
               Version: 3
         Serial number: 42b24e5c00000001b138
           Issuer name: Company Name Issuing
                        xxxdom01
                        xxx
                        com
          Subject name: vmlpar.testlpar.com
                        systems
                        XXX
                        Xxx Xxx
                        Xxxxxxx
                        US
                        US
        Effective date: 20xx/06/07
       Expiration date: 20xx/06/06
   Signature algorithm: sha512WithRsaEncryption
      Issuer unique ID: None
     Subject unique ID: None
  Public key algorithm: rsaEncryption
       Public key size: 2048
```

```
            Public key: 30 82 01 0A 02 82 01 01 00 93 99 05 97 24
C8 DE
                        B1 02 32 D3 F0 84 15 23 A3 02 03 01 00 01
  Number of extensions: 8

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