CS z/OS Application Enhancements: TN3270

TN3270 and System SSL cipher suites

- **TN3270 Server**
  - Option to control use of SSL V2 or not
  - AES encryption support
- **System SSL uses a 2-digit number to identify the various cipher suites it supports.**
  - Sendmail configuration is based on those 2-digit numbers
  - TN3270 supports a text string-based configuration that is then translated by TN3270 to the 2-digit numbers system SSL uses
- **TN3270 supports the following cipher suites:**
  - SSL_RC4_SHA
  - SSL_RC4_MD5
  - SSL_AES_256_SHA
  - SSL_AES_128_SHA
  - SSL_3DES_SHA
  - SSL_DES_SHA
  - SSL_RC4_MD5_EX
  - SSL_RC2_MD5_EX
  - SSL_NULL_SHA
  - SSL_NULL_MD5
  - SSL_NULL_Null

TN3270 server SSL/TLS support - 128/256 bit AES encryption

- **TN3270 supports more levels of SSL/TLS protocols:**
  - SSLv2 - generally considered to be a weak security protocol
    - The TN3270 server in z/OS V1R7 adds configuration control to disallow/allow a client to negotiate use of SSL V2 protocol levels:
      - SSLV2 or NOSSLV2 - default is NOSSLV2
    - This option can be specified on TelnetGlobals, TelnetParms, or in a ParmsGroup
  - SSLv3
  - TLSv1

TN3270 server support of cipher suites

This is the default TN3270 server cipher suite list in the order of preference.

If you need to change that order or to exclude certain choices, code the ENCRYPTION / ENDENCRYPTION block in TelnetGlobals, TelnetParms or in a ParmsGroup.

The two-digit telnet display abbreviation codes are not the same as the system SSL 2-digit cipher suite codes.

Cipher suite	Telnet display abbreviation
SSL_RC4_SHA	4S
SSL_RC4_MD5	4M
SSL_AES_256_SHA	**A2 <== New in z/OS V1R7**
SSL_AES_128_SHA	**A1 <== New in z/OS V1R7**
SSL_3DES_SHA	3S
SSL_DES_SHA	DS
SSL_RC4_MD5_EX	4E
SSL_RC2_MD5_EX	2E
SSL_NULL_SHA	NS
SSL_NULL_MD5	NM
SSL_NULL_Null	NN

Display command example

NOTES

- **Display TCPIP,,Telnet,PROF to see if SSLv2 is supported**

```
EZZ6060I TELNET PROFILE DISPLAY
  PERSIS   FUNCTION     DIA  SECURITY  TIMERS  MISC
 (LMTGQAK)(OATSKTQSWHT)(DRF)(PCKLECXL2)(IKPSTS)(SMLT)
  -------  -----------  ---  --------  ------  ----
  LMSM***  **TSBTQ*WHT  DJ*  BB******2  ***STS  SMD*
----- PORT:    23  ACTIVE              PROF: CURR CONNS:      0
-------------------------------------------------------------
   FORMAT           LONG
   TNSACONFIG       DISABLED
5 OF 5 RECORDS DISPLAYED
```

Display command example

NOTES

- **Display TCPIP,,Telnet,PROF,DETail to see which cipher suites are supported**

```
EZZ6080I TELNET PROFILE DISPLAY
  PERSIS    FUNCTION      DIA  SECURITY  TIMERS  MISC
 (LMTGQAK) (OATSKTQSWHT) (DRF) (PCKLECXN2) (IKPSTS) (SMLT)
  -------  -----------   ---  ---------  ------  ----
  *******  **TSBTQ***T   EC*  BB**D****  ***STS  *DD* *DEFAULT
  -------  -----------   DC-  ---------  ------  ---- *TGLOBAL
  -------  ---------H-   ---  SSS-DF---  ------  ---- *TPARMS
  *******  **TSBTQ**HT   DC*  SSS*DF***  ***STS  *DD* CURR
 PERSISTENCE
   NOLUSESSIONPEND
 ...
 SECURITY
   SECUREPORT          327
   CONNTYPE            SECURE
   KEYRING             SAF TNsafkeyring
   CRLLDAPSERVER       NONE
   ENCRYPTION          4S,4M,A2,A1,3S,DS,4E,2E,NS,NM,NN (DEF)
   CLIENTAUTH          SAFCERT
   NOEXPRESSLOGON
   NONACUSERID
   SSLV2
 TIMERS
```

Things to think about

- **A TN3270 client that only works with SSLV2 will no longer be able to work with the TN3270 server in z/OS V1R7, unless the TN3270 server configuration is changed to specify the SSLV2 option.**
  - The default is NOSSLV2

Trademarks, Copyrights and Disclaimers

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

IBM	CICS	IMS	MQSeries	Tivoli
IBM(logo)	Cloudscape	Informix	OS/390	WebSphere
e(logo)business	DB2	iSeries	OS/400	xSeries
AIX	DB2 Universal Database	Lotus	pSeries	zSeries

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 registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. 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. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. 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 in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance 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 or performance improvements equivalent to the ratios stated here.