IBM Education Assistance (IEA) for z/OS V2R3

TDS-LDAP FIPS Compliant

Material prepared for IBM Education Assistance

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Validation During ESP
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None.

Session Objectives

- At the end of this presentation, you should have an understanding of …
  - The IBM Tivoli Directory Server enhancements for
    - FIPS compliant of SSL/TLS-protected connection
  - How to use the enhancements

Overview

- Problem Statement / Need Addressed
  - Customers want to use secure connections for applications communicating to the z/OS IBM Tivoli Directory Server over SSL, making it be FIPS compliant which means that it would meet security related criteria defined both in 'FIPS 140-2 LEVEL1' and NISTSP800-131A.
- Solution
  - The z/OS IBM Tivoli Directory Server, its client C-API, and its command line utilities (which utilize the client C-API) are enhanced to support current z/OS System SSL capabilities to be FIPS compliant.
  -
- Benefit / Value
  - Increased security is available for the SSL connections used to communicate between z/OS IBM Tivoli Directory Server and client. When executing in FIPS mode, it is more restrictive with respect to cryptographic algorithms,protocols and key sizes that can be supported.
  -

Usage & Invocation … Server

- In server configuration file general section a new configuration option is introduced in this line-item: **sslFipsState.**
- For sslFipsState configuration option, supported values are OFF, LEVEL1, LEVEL2, LEVEL3.
  - OFF means non-FIPS state.
  - LEVEL1 means it has been set to FIPS state and should meet 80-bit security strength.
  - LEVEL2 means it has been set to FIPS state and should meet 112-bit security strength when creating new keys or performing digital signature generation and encryption type operations. And should meet 80-bit security strength when do digital signature verification, decryption using TDES and RSA decryption to process already protected information.
  - LEVEL3 means it has been set to FIPS state and should meet 112 bit or higher security strength as defined in NIST SP800-131A.
- **Example: sslFipsState Level1**

Usage & Invocation … Server

- When executing in FIPS mode, only TLS1.0, TLS1.1 and TLS1.2 protocols are allowed. SSL V2 and SSL V3 protocols are not supported and will be ignored, if specified.
- When FIPS mode set to on, all certificates in a certificate chain must meet the security criteria as specified by sslFipsState configuration option.
- When FIPS mode set to on, if you set a key database file to the configuration file sslKeyRingFile, it must be created as a FIPS mode database.
- When FIPS mode set to on, the cipher specs set to configuration option sslCipherSpecs must meet the FIPS level as specified by sslFipsState configuration option.
  - If you set GSK_V3_CIPHER_SPECS_EXPANDED to sslCipherSpecs, the 4 bytes cipher specs specified externally in the environment variable of the same name also must meet the FIPS level defined in sslFipsState configuration option.

Usage & Invocation … Server

- In advanced replication and basic replication, the replicating server acts as an SSL/TLS client to the replica, in the mean time, the replicating server also acts as an SSL/TLS server that listening for common clients.
-
- So the new configuration option **sslFipsState** will control the FIPS mode for both inbound client connections to the replicating server and for outbound connections from the replicating server to the replica.

Usage & Invocation … Server dsconfig utility

- The dsconfig utility enhanced to support configuring new option **sslFipsState**.

Usage & Invocation … client C-API

- An new client API ldap_ssl_set_fips_state() introduced in this line-item. As an application developer, the user needs to invoke this new API if the user wants to enable FIPS enforcement in SSL/TLS connection.
- The format of this new API is as following:
  - ***ldap_ssl_set_fips_state(int state, int *ssl_rsncode)***
  - You can specify following four types of numeric values to the first parameter:1101 , 1110,1120,1130 to set FIPS mode. They represents OFF, LEVEL1,LEVEL2,LEVEL3 respectively.
  - The second parameter is an output parameter. It returns the LDAP reason code as defined in the ldapssl.h include file.
- ldap_ssl_set_fips_state must be run before starting ldap_ssl_client_init() to set the FIPS mode of System SSL client.

Usage & Invocation … command line utilities

The following LDAP command line utilities which use the C-API would rely on -x option to set the FIPS mode as OFF/LEVEL1/LEVEL2/LEVEL3:

ldapchangepwd
ldapcompare
ldapdelete
ldapmodify/ldapadd
ldapmodrdn
ldapsearch

db2pwden
ldapexop

For ds2ldif utility, when -Z parameter specified, by default, the ds2ldif utility attempts to use SSL to communicate with the LDAP server assuming that the LDAP server configuration file has the necessary SSL options, including sslFipsState option.

Example:

```
ldapsearch -h 127.0.0.1 -p 3022 -Z -x level3 -K keydatabasefile -P passwd -D
cn=admin -w secret -s sub -b "o=IBM" "objectclass=*
```

Interactions & Dependencies

- Software Dependencies
  - As an application of System SSL, if you want SSL/TLS-protected LDAP connection to run in FIPS mode, System SSL that can be run in FIPS mode should be available.
  -
- Hardware Dependencies
  - When executing in FIPS mode, System SSL continues to take advantage of the CP Assist for Cryptographic Function (CPACF) when available.
  - Cryptographic functions performed by ICSF-supported hardware when running in non-FIPS mode continue to be used when executing in FIPS mode apart from RSA and ECC signature generation which must be performed in software.
  - Hardware cryptographic functions allowed in FIPS mode support clear keys only.
  -
- Exploiters
  - Any customer applications that communicate with LDAP protocol either with the z/OS IBM TDS directory server or using its client C-API with secure socket communications are potential exploiters of the enhanced System SSL features provided by this support.

Migration & Coexistence Considerations

- Because not all cryptographic algorithms and key sizes and SSL protocols used in non-FIPS mode secure communication are supported in FIPS mode, certificates/key database files with key sizes and algorithms that are valid in FIPS mode will be needed to add or replace if the LDAP server runs in FIPS mode.

- In multiple server environments, the expectation and recommendation is that all such servers should communicate using the same SSL/TLS options. This is essentially unchanged by the introduction of the new FIPS support in this line-item.

Installation

- None

Session Summary

- You should have an understanding of …
  - The IBM Tivoli Directory Server enhancements for FIPS compliant of SSL/TLS-protected connection
  - How to use the enhancements

Appendix

Publications

- IBM Tivoli Directory Server Plug-in Reference for z/OS
- IBM Tivoli Directory Server Administration and Use for z/OS
- IBM Tivoli Directory Server Messages and Codes for z/OS
- IBM Tivoli Directory Server Client Programming for z/OS
- IBM z/OS Cryptographic Services Secure Systems Socket Layer Programming