z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: TLS 1.3 Support

Element(s)/Component(s): TDS-LDAP

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
  - Exploitation of TLS V1.3 Support
- 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, exploiting the recent enhancements provide with TLS V1.3 Support.
- Solution
  - The z/OS IBM Tivoli Directory Server, its client C-API, and its command line utilities (which utilize the client C-API) support current z/OS System SSL capabilities, including TLS V1.3 Support.
- Benefit / Value
  - Increased security is available for the SSL connections used to communicate between z/OS IBM Tivoli Directory Server and client.

Overview

- ITDS LDAP server allows LDAP clients and applications to secure connections using both the SSL (V2/V3) and TLS (V1.0, V1.1 and V1.2) protocol versions. In this release, ITDS plan to support new protocol version TLS1.3.

- This EPIC depends on System SSL TLS1.3. LDAP doesn't need code enhancement, no LDAP code change on V2R4.

- The following items will be supported:
  - Full handshake with and without client authentication – support for AES-GCM (TLS_AES_128_GCM_SHA256 and TLS_AES_256_GCM_SHA384) and CHACHA (TLS_CHACHA20_POLY1305_SHA256) based ciphers and (EC)DHE key exchanges

Usage & Invocation…Server

- TLS V1.3 protocol requires 4 byte cipher specifications, 2 byte ciphers aren't supported any more.
- The **sslCipherSpecs** server configuration option should be specified with GSK_V3_CIPHER_SPECS_EXPANDED

2-character cipher number	4-character cipher number	Short name	Description	FIPS 140-2	Base security level FMID HCPT440	Security level 3 FMID JCPT441
	1301	TLS_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and HKDF (HMAC-based Extract-and-Expand Key Derivation Function) with SHA256	X		X
	1302	TLS_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 256-bit AEAD authentication and HKDF (HMAC-based Extract-and-Expand Key Derivation Function) with SHA384	X		X
	1303	TLS_CHACHA20_POLY1305_SHA256	ChaCha20 encryption with 256-bit AEAD authentication and HKDF (HMAC-based Extract-and-Expand Key Derivation Function) with SHA256			X

Usage & Invocation…Server

- RSA, ECC certificates are supported with TLS1.3. DSA and fixed DH certificates are not supported with TLS 1.3.

- For TLS 1.3, the GSK_CLIENT_TLS_KEY_SHARES (on your LDAP client side) and the GSK_SERVER_TLS_KEY_SHARES (on your LDAP server side) must be specified if a TLS 1.3 connection gets negotiated.

- GSK_TLS_SIG_ALG_PAIRS

  Specifies the list of TLS V1.2 and TLS V1.3 hash and signature algorithm pair specifications that are supported by the client or server for use in digital signatures of X.509 certificates and TLS handshake messages.

  export GSK_TLS_SIG_ALG_PAIRS=0804080508060601060305010503040104030402030103030302020102030202

Usage & Invocation…Server

Example:

- Server configuration file, in the general section:

  sslCipherSpecs GSK_V3_CIPHER_SPECS_EXPANDED

- Server environment variable file:

  GSK_PROTOCOL_TLS_V1_3=ON

  LDAP_SSL_CIPHER_FORMAT=CHAR4

  GSK_SERVER_TLS_KEY_SHARES=002300240025

  GSK_V3_CIPHER_SPECS_EXPANDED=130113021303

  GSK_TLS_SIG_ALG_PAIRS=0804080508060601060305010503040104030402030103030302020102030202

Usage & Invocation…client C-API

- The LDAP client using C-API to enable TLS V1.3 protocol connection.

- The **ldap_set_option**() API could be used to explicitly set the cipher specs with the **LDAP_OPT_SSL_CIPHER_EXPANDED** option.

  The cipher specifications could be specified using the list of z/OS System SSL 4 character values in string form.

```
ldap_set_option(ld, LDAP_OPT_SSL_CIPHER_EXPANDED, "1301");
ldap_set_option(ld, LDAP_OPT_SSL_CIPHER_FORMAT,
        LDAP_SSL_CIPHER_FORMAT_CHAR4);
```

- When not executing in FIPS mode, the following default values are set:

  TLS V1.0 is enabled (SSL V2, SSL V3, TLS V1.1, TLS V1.2, and TLS V1.3 are disabled by default).

- When executing in FIPS mode, the following default values are set:

  TLS V1.0 is enabled (SSL V2, SSL V3, TLS V1.1, TLS V1.2, and TLS V1.3 are disabled by default).

Usage & Invocation…command line utilities

- The following LDAP command line utilities which use the C-API will behave according to the environment variables:

- ldapchangepwd
- ldapcompare
- ldapdelete
- ldapmodify/ldapadd
- ldapmodrdn
- ldapsearch

- db2pwden
- ds2ldif -r (remote option, using extended operation)
- ldapexop

Usage & Invocation …command line utilities

Example:

export LDAP_SSL_CIPHER_FORMAT=CHAR4

export GSK_PROTOCOL_TLSV1_3=ON

export GSK_V3_CIPHER_SPECS_EXPANDED=1301

export GSK_CLIENT_TLS_KEY_SHARES=0023

ldapsearch -p 636 -Z -K *my.kdb* -P my*kdbpw* -N *mykeylabel*
-D *bindDN* -w *mybindpw* -b *basedn* “objectclass=*”

Migration & Coexistence Considerations

- None

Installation

- None

Validation During ESP

- ESP Validation Requested: No

Session Summary

- You should have an understanding of …
  - The IBM Tivoli Directory Server enhancements for exploitation of TLS V1.3 Support
  - 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