z/OS V2.5 IBM Education Assistant

Solution Name: NAS NDBM FIPS support

Solution Element(s): Network Authentication Service

July 2021

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

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

Objectives

- Provide continuous support for product compliance
- At the end of this presentation, you would understand the new support from:
  - NAS (Kerberos) NDBM FIPS support

Overview

- Network Authentication Service (NAS) is a Kerberos implementation on z/OS
- Server and client secure communication is through tickets and keys via a Key Distribution Center (KDC)
- KDC in Kerberos can be implemented using SAF (RACF) or NDBM (file system)
- z/OS V2R3 NAS provided FIPS support for the KDC in SAF
- In this release, FIPS support will be available for the KDC in NDBM

Overview (cont'd)

- Who (Audience)
  - Customers run NAS on z/OS
- What (Solution)
  - New NDBM database will be created with the new stronger encryption type aes256-cts-hmac-sha384-192
  - KDC using an existing NDBM database with non-compliant FIPS encryption type will not start if FIPS mode is turned on
  - New support to dump an NDBM database to a file with a new encryption type
  - New support to identify principals that have non FIPS-compliant current or history password keys
  - All the processing using NDBM is also FIPS sensitive when FIPS mode is turned on
- Wow (Benefit / Value, Need Addressed)
  - Have FIPS support for NDBM database to achieve the needed compliant level

Usage & Invocation

- Specify FIPS level for NDBM KDC in the same way for the SAF support

  For admin functions

  – Specify the SKDC_FIPSLEVEL value in the envar file corresponds to the System SSL FIPS level it supports:

    - SKDC_FIPSLEVEL = 0, non FIPS mode (default)
    - SKDC_FIPSLEVEL = 1, FIPS140-2
    - SKDC_FIPSLEVEL = 2, SP800-131A with exception (Key generation, signature creation and encryption need to be performed with the required strength; digital signature verification, decryption can be performed with lower key strength)
    - SKDC_FIPS_LEVEL = 3, SP800-131A without exception (All operations have to be performed with the required strength)

  For client functions

  – Specify the fipslevel value in the krb5.conf file corresponds to the System SSL FIPS level it supports:

    - fipslevel = -1, FIPS mode not to be set (default)
    - fipslevel = 0, non FIPS mode
    - fipslevel = 1, FIPS140-2
    - fipslevel = 2, SP800-131A with exception (Key generation, signature creation and encryption need to be performed with the required strength; digital signature verification, decryption can be performed with lower key strength)
    - fipslevel = 3, SP800-131A without exception (All operations have to be performed with the required strength)

Usage & Invocation (cont'd 1)

- Create a new NDBM
  - kdb5_ndbm create (new default to aes256-cts-hmac-sha384-192) OR
  - kdb5_ndbm create –k <keytype>
- Dump an existing NDBM to a file
  - kdb5_ndbm dump (still default to aes256-cts-hmac-sha1-96) OR
  - kdb5_ndbm dump –k <keytype>
- Create a NDBM using a dump file
  - kdb5_ndbm load …<dump file> - master key encryption type in NDBM is the same as that in dump file
  - kdb5_ndbm load –k <keytype>…<dump file> - if specified key type is not matching that in dump file, command fails with new error message
  - kdb5_ndbm load …-K <keytpe> -mkey_convert <dump file> - master key encryption type in NDBM is the one specified for –K, overriding that in dump file
    - This can prepare for the FIPS compliant NDBM

Usage & Invocation (cont'd 2)

- Check if there are any principals that have non FIPS compliant current or history password keys
  - kdb5_ndbm fips_report
  - If there are, and FIPS is enabled, kadmin change_password will not be able to detect a re-use password encrypted under a non FIPS compliant type
  - If you want to avoid password re-use, don't enable FIPS mode until fips_report returns clean

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - No
- Exploiters
  - NAS customers who wants to enable FIPS in NDBM

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level:
  - Yes
- Toleration/coexistence APAR/ PTFs
  - OA60507 – to keep the password policy operational in a NDBM database shared between a system running with z/OS V2R5 and other lower release systems
  - PTFs UJ04928 (V2R3), UJ04929 (V2R4)
- Things works differently
  - kdb5_ndbm create - new default encryption type is aes256-cts-hmac-sha384-192
  - kdb5_ndbm load –k <keytype>…<dump file> - if specified key type is not matching that in dump file, command fails with error message vs no message before

Installation & Configuration

- List to be aware of for installation:
  - APAR needed: OA60507 – to keep the password policy operational in a NDBM database shared between a system running with z/OS V2R5 and other lower release systems
  - Run kdb5_ndbm fips_report to check if there are any principals that have non FIPS compliant current or history password keys before turning on FIPS mode
  - Default encryption type is changed in this release for a new NDBM created from scratch

Summary

- Now you should understand the support from NAS NDBM FIPS support
  - All the processing using NDBM is also FIPS sensitive when FIPS mode is turned on, just like the SAF based database
  - New NDBM database will be created with the new stronger encryption type
  - KDC using an existing NDBM database with non-compliant FIPS encryption type will not start if FIPS mode is turned on
  - New support to FIPS compliant encryption types
  - New support to check for FIPS readiness for NDBM database

Appendix

- Publication references
  - Integrated Security Services Network Authentication Service Administration
  - Integrated Security Services Network Authentication Service Programming