#SHAREorg

SHARE
Technology · Connections · Results

z/OS LDAP Plug-ins: Endless Opportunities

Saheem Granados, CISSP®
IBM
sgranado@us.ibm.com
Wednesday, August 8, 2012
11628

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

SHARE in Anaheim 2012

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- CICS*
- DB2*
- IBM*
- IBM (logo)*
- OS/390*
- RACF*
- Websphere*
- z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Identrus is a trademark of Identrus, Inc

VeriSign is a trademark of VeriSign, Inc

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput 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 improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- LDAP Primer
- Intro to TDS for z/OS
- Standard LDAP Operations available with TDS
- Customizing TDS Behavior via Plug-ins
  - What are Plug-ins?
  - How are Plug-ins configured?
  - When are Plug-ins called?
  - Words of Caution
- Why Customize TDS?
- Summary
- Additional References

What is LDAP?

- Directory – data repository
  - Data stored in Entries managed in a hierarchical fashion, e.g., entries have parent entries
  - Commonly used to store user repository data
    - Also used to store application specific configuration data
  - Each entry contains 1 or more attributes
    - Every entry has a Distinguished Name attribute – unique identifier of the entry
    - Other attributes include password, native ID, etc..
- Lightweight Directory Access Protocol
  - A standard protocol for accessing/managing Directory data over TCP/IP
    - Add, delete, modify entries…
    - Search entries
- Can be key to an enterprises IT security infrastructure
  - Authentication of user
  - Authorization

Directory Server for z/OS

- Tivoli Directory Server is a LDAP server implementation fully optimized for z/OS
  - **Not** a port of distributed TDS server to z/OS
- Supports standard LDAP V3 protocol
- z/OS specific optimizations include
  - Full sysplex support
  - System SSL, ICSF, CTRACE, WLM, ARM, DB2, etc… support
  - LDAP based access to RACF data
    - RACF still responsible for authorization
- LDAP-RACF relationship allows
  - LDAP based remote authentication to be done by RACF
  - Limited LDAP based access to RACF user, resource, and custom profiles
  - LDAP plugin allows for remote RACF audit and authorization services.

Standard LDAP Operations

- TDS for z/OS supports the following standard directory related operations
  - Bind
  - Add
  - Modify
  - Delete
  - Rename
  - Search
  - Compare
  - Unbind/Close
  - Extended Operations
- Operations can be configured to result in Type 83 Subtype 3 SMF Record output

Standard LDAP Operations: Bind

- TDS authenticates the LDAP user
- Usually done before client attempts any other LDAP operation
  - Not required – ACL entries setup would need to authorize Anonymous operations
- Various types of Binds
  - Certificate based authentication
  - Password based authentication: two types
    - Native Authentication: RACF performs authentication
    - Password stored in Directory managed by TDS
  - Kerberos based authentication

Standard LDAP Operations: Add/Modify

- Add: Adds new entries into the directory
  - Recall directory is hierarchical
    - LDAP client must be authorized to ADD objects under an existing directory entry
- Modify: Modifies attribute values of entries in the directory
  - LDAP client must be given WRITE authority on the attribute being modified

Standard LDAP Operations: Delete/Rename

- Delete: Deletes entries from the directory
  - LDAP client must be authorized to DELETE target object
- Rename (Modify DN, move): Modifies the DN of the entry, essentially moving the entry within the directory
  - LDAP client must be given WRITE authority on the attributes being modified in the DN
  - If setting new superior, client must be ADD authority on new parent

Standard LDAP Operations: Search/Compare

- Search: Query and retrieve entries from the directory
  - LDAP client must be authorized to READ attribute values being sought and compared within the search filter
- Compare: Query and compare entry attribute values from the directory
  - LDAP client must be given COMPARE authority on the attributes being compared
  - Occasionally used as a means of authentication
    - LDAP compare against userPassword attribute

Standard LDAP Operations: Unbind/Close

- Unbind: Closes LDAP client's connection to server
  - To reconnect: LDAP client must initialize a new connection AND issue a new bind (or work anonymously with LDAP server)

What are TDS Plug-ins?

- TDS allows for administrators to extend/alter how it services the standard LDAP operations
  - Plug-ins provide code to be executed when an event occurs during TDS operation processing
- Plug-in is a DLL usually written in the C language
  - IBM provides a few, e.g., ICTX Plug-in
- TDS provides the SLAPI interface for Plug-ins
  - SLAPI interface is an open interface implemented/supported by many LDAP Server implementations (e.g., openLDAP, TDS for Distributed platform)
    - Facilitates code reuse across server implementations

What are TDS Plug-ins? Cont…

- TDS allows for three different Plug-in types
  - Pre Operation – Handle events before standard TDS processing
  - Post Operation – Handle events after standard TDS processing
  - Client Operation – Replaces standard TDS processing
- Plug-in registration consists of two steps
  - Definition of Plug-In details/parameters within LDAP configuration file: plugin postOperation PLUGSAMP plugin_init "auditFile"
    - Type of Plug-in
    - Plug-in DLL Name
    - Initialization Function Name
    - Any custom configuration parameters needed by Plug-in
  - Plug-in initialization function uses SLAPI interface to register for different events
- More than one plug-in can be registered

When are TDS Plug-ins Invoked?

- For each Plug-in type (pre, post, client), Plug-ins can register for different events
  - Abandon
  - Add
  - Bind
  - Compare
  - Delete
  - Extended operation
  - Modify
  - Modify DN(rename)
  - Search
  - Unbind
  - **Callback**

When are TDS Plug-ins Invoked? Cont…

- Callback – special event
  - Only available to client operation plug-ins
  - Allows plug-in to alter security related information used by TDS during normal process:
    - Get Password (for DN or UID)
    - Get Groups
    - Get Alternate DNs
- When LDAP event occurs via a client request, the plug-in is invoked by TDS.
- Example Processing Flow
  - Plug-in defined in configuration file as Post operation
  - TDS start up: Plug-in initialization function registers for Add event
  - TDS receives an Add request
    - TDS performs standard processing and commits update to the directory
    - TDS invokes Plug-in's registered function for the Add event
    - Plug-in code gets control

Words of Caution

- Plug-in DLL must reside in APF authorized data set
- Plug-in code executes within TDS address space
  - Coding error could result in TDS ABEND
- Plug-ins can alter TDS's security semantics
  - CALLBACK event – can alter LDAP client's security credentials
- Plug-ins can alter directory data and alter operation results
  - Pre and Client operation plug-ins can bypass TDS entirely
  - SLAPI interface provides API for plug-in initiated LDAP operations
    - E.g: Delete Post op Plug-in issues via SLAPI, LDAP add operation

Why Plug-ins?

- Leveraging mature protocol to manage proprietary data
  - Example: Data may reside in other databases with different structure, e.g., DB2 Table
    - Pre or client type operations can be deployed to “translate” data to/from LDAP directory data
      - *LDAP is a mature/open protocol*
      - *Applications can be designed to standardized LDAP*
- Alter Security Semantics
  - Example: Proprietary identity mapping or group membership rules
  - Example: Different password repository
    - Client operation plug-ins can implement Callback event to alter Client’s security credentials

Why Plug-ins? Cont…

- Enhance auditing
  - Example: TDS Auditing does not meet organizational requirements
    - Post operation plug-in can be deployed to perform additional auditing tasks
- Interact with different user repositories
  - Example: Data layout and business requirements necessitate data aggregation from different ActiveDirectory, DB2, and openLDAP repositories
    - Pre/client can be deployed to service LDAP operations by communicating with other repositories and aggregating the necessary data to return standard LDAP results to the client

How do I get started?

- Sample plug-in shipped with TDS for z/OS
  - */usr/lpp/ldap/examples/plugin_sample.c*
- IBM Tivoli Directory Server Plug-in Reference for z/OS
  - Reference for Plug-in writers
  - Contains instructions for building, testing, and deploying sample plug-in
- Remember: Plug-ins allow great flexibility, but care must be taken given their relationship with TDS and their APF Authorized state.

Summary

- TDS supports Plug-ins
- Plug-ins must be compiled into a DLL and reside in an APF authorized data set
- Plug-ins must be registered via the configuration file AND calls from within the plugin to the SLAPI interface

- Plug-ins allow for administrators to extend/alter how TDS services standard LDAP operations
  - This flexibility facilitates standards based data access/management by applications without requiring significant restructuring of proprietary data or business processes

References

- z/OS Hot Topics Newsletter http://www-03.ibm.com/systems/z/os/zos/bkserv/hot_topics.html
  - #22, March 2010: “We’ve got your back(bone)”
  - #25, August 2011: “Don’t judge an LDAP server by its name!”
  - #26, August 2012: “z/OS LDAP Plug-ins: Endless Opportunities”
- z/OS Publications http://www-03.ibm.com/systems/z/os/zos/bkserv/
  - IBM Tivoli Directory Server Client Programming for z/OS
  - IBM Tivoli Directory Server Messages and Codes for z/OS
  - **IBM Tivoli Directory Server Plug-in Reference for z/OS**
  - IBM Tivoli Directory Server Administration and Use for z/OS
- IBM Education Assistant http://publib.boulder.ibm.com/infocenter/ieduasst/stgv1r0/index.jsp?topic=/com.ibm.iea.zos/plugin_coverpage.html
  - V1R11 – Security
    - Accessing RACF Resource Profiles through the IBM Tivoli Directory Server for z/OS
    - • Introduction to configuring advanced replication in the IBM Tivoli Directory Server for z/OS
  - V1R12 – Security
    - Password policy in the IBM Tivoli Directory Server for z/OS