Tivoli Directory Server (TDS) for z/OS 1.12: LDAP Update for 2011

Vanguard Security Conference

Jack Jones

johnjone@us.ibm.com

Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
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 trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

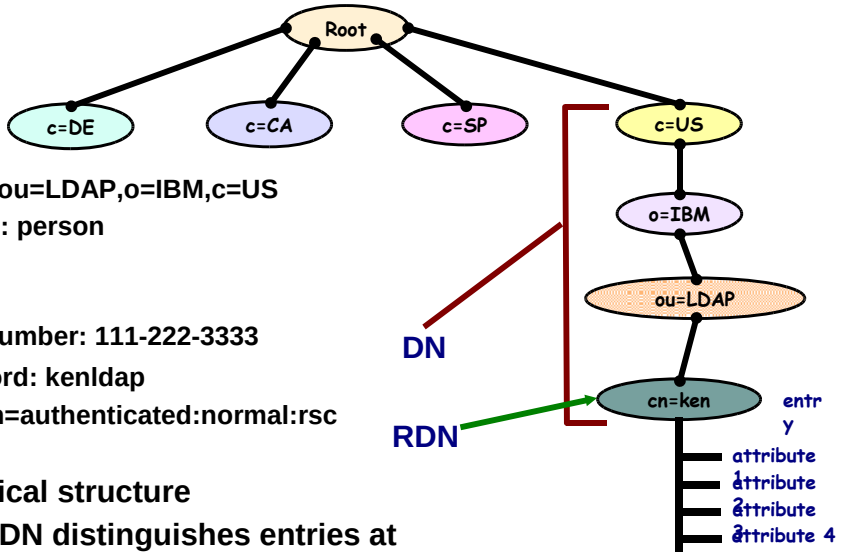
Table of Contents

What is LDAP?

- **Lightweight Directory Access Protocol (LDAP) is a global directory model**
- **Originally developed as front-end of X.500 (DAP)**
- **The LDAP protocol runs over TCP**
- **Global directory model is based on entries**
  - **Each entry identified by its DN (distinguished name)**
    - **Often uses cn (common name), ou (organization unit), o (organization)**
  - **Each entry is a collection of attributes**
    - **Each attribute has a type and values**
    - **Attributes are grouped into object classes**
      - **Determine mandatory and optional attributes for an entry**

DN: cn=ken,ou=LDAP,o=IBM,c=US

LDAP Directory Structure



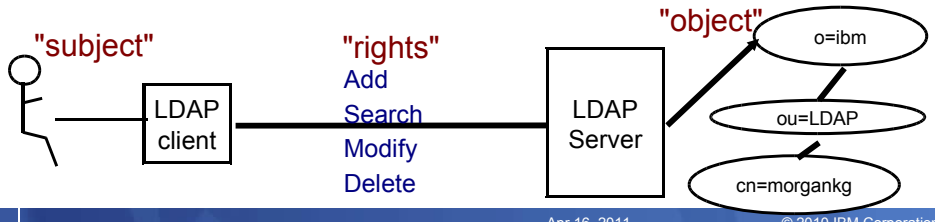
dn: cn=ken,ou=LDAP,o=IBM,c=US
objectclass: person
cn: ken
sn: morgan
telephonenumber: 111-222-3333
userpassword: kenldap
aclentry: cn=authenticated:normal:rsc

- Hierarchical structure
- Relative DN distinguishes entries at same level of hierarchy
- Attributes are protected by Access Control Lists (ACL)

Access Control Checking

☒ **Does subject have the right to perform the requested operation on an object?**

- **"subject" - the "bound" LDAP client identity: DN of requestor + DNs of groups to which requestor belongs**
- **"object" - the entries or the attributes of the entries involved in the operation**
- **"rights" - the access required to perform the requested operation (add/delete entry, read/write/search/compare attribute)**

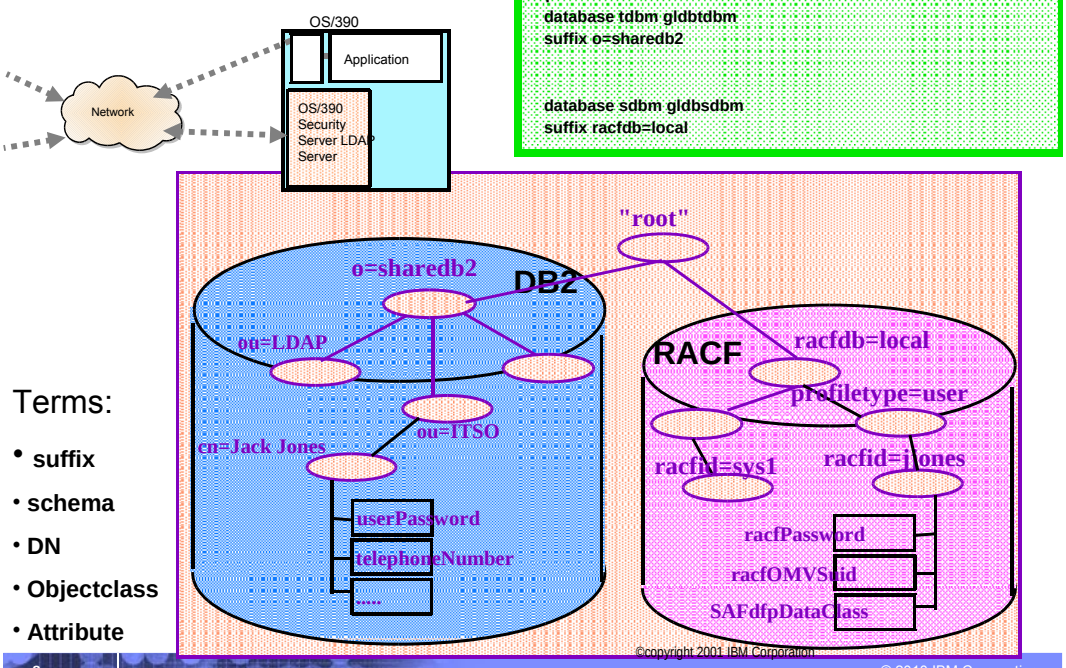


Overview

- **IBM Tivoli Directory Server (IBM TDS) for z/OS V1R11**
  - Integrated Security Services (ISS) Not Supported
  - Must migrate to TDS prior to z/OS R11

- Two LDAP components in z/OS V1R10 base:
  - **IBM Tivoli Directory Server (IBM TDS) for z/OS**
    - LDAP server enhanced in v1R10
    - LDAP client and utilities
  - **Integrated Security Services (ISS)**
    - z/OS V1R6 version of LDAP server
    - Withdrawn in V1R11
  - Both servers installed as part of z/OS V1R10
  - All enhancements to IBM TDS only

SDBM & TDBM Backends



Terms:

- **suffix**
- **schema**
- **DN**
- **Objectclass**
- **Attribute**

Access Control Implementation

- **TDBM/LDBM uses an Access Control List (ACL) to control access to an entry**
  - **Specifies DNs of bound users and groups that can access the entry**
- **Can control access to individual attributes or to classes of attributes (normal, sensitive, critical, restricted and system)**
  - **Attribute's access class defined in the schema**
- **Use LDAP modify operation to set ACL and search operation to display ACL info**
  - **examples:**

aclentry: cn=Jayb,o=Your Company:normal:rwsc:sensitive:rsc
aclentry: racfid=morgankg,profiletype=user,cn=myRacf:object:ad
aclentry: group:cn=mgrs,o=Your Company:at:userpassword:rwsc
aclentry:group:racfid=g1,profiletype=group,cn=myRacf:normal:rwsc

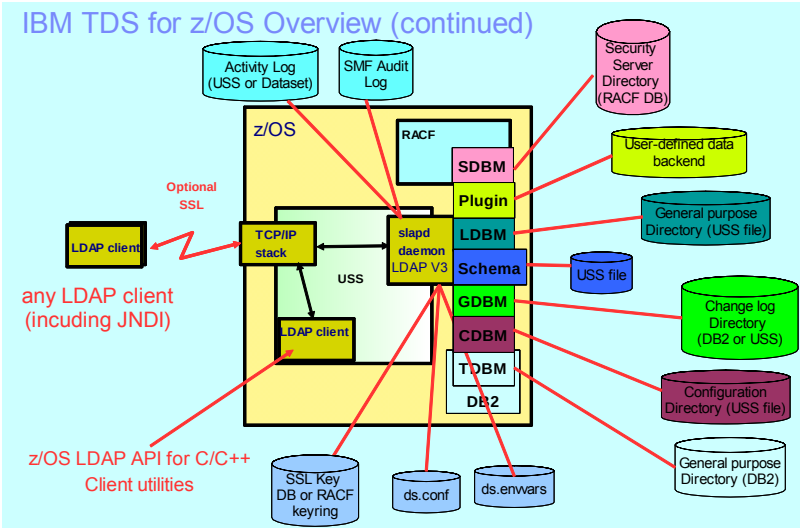
- **Can propagate an entry's ACL to the subtree below it**

Special aclEntry "pseudo-DNs"

- **cn=anybody**
  - **Applies when no other specific ACL value applies**
- **cn=authenticated**
  - **Applies when the requestor has authenticated to the directory but no other specific ACL value applies**
  - **Meant to allow more access than cn=anybody ACL value**
- **cn=this**
  - **Applies when the requestor has authenticated with the same DN as the entry being accessed**
  - **Used to grant individuals access to their own entry**
- **Example:**

aclentry: cn=anybody:normal:rsc
aclentry: cn=authenticated:normal:rsc:sensitive:rs
aclentry: cn=this:normal:rscw:sensitive:rscw:critical:rsc

LDAP Component Overview



Unique z/OS Features

- **Sysplex Support**
  - DB2 data sharing
  - XCF message support
  - Failover in multi-servermode
- **WLM workload classification and Vipa health**
- **SMF 83 Security Audit Records**
- **LDAP access to RACF**

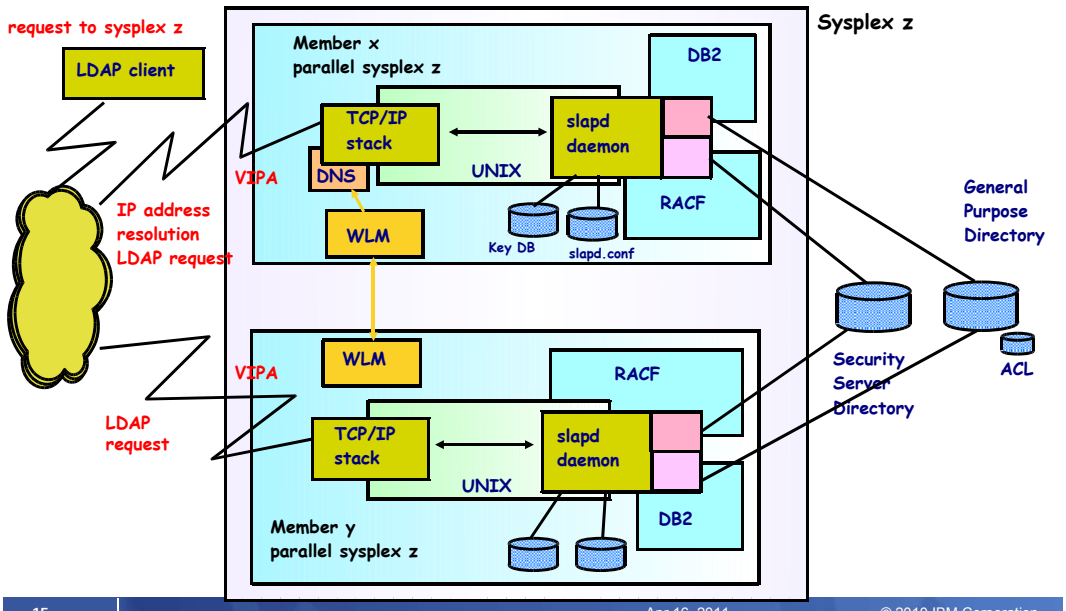
z/OS R11 TDS Features (Current)

- **Advanced Replication Support**
  - Replication of subtrees of the Directory Information Tree (DIT) to a specific server
  - multi-tier topology referred to as cascading replication
  - assignment of server role (master or replica) by a subtree
  - filtered replication
  - support of gateway replication
  - enhanced conflict resolution
- **WLM and VIPA Health support**
  - Supports classification of LDAP work by client IP or binddn
- **Accessing RACF Resource Profiles via TDS**
  - Define ldap schema for RACF resource profile and access via SDBM

z/OS R12 TDS (GA 9/2010)

- Password Policy
  - Password policy is a set of rules that controls how passwords are used and administered in the IBM Tivoli Directory Server for z/OS.
- ACL by IP
  - An extension to ACLs which clarifies a BIND DN by IP address or subnet
- Salted SHA
  - This is a salted version of the SHA-1 Secure Hash Algorithm.
- Schema Updates
  - Support for 21 new schema syntaxes matching rules which will make z/OS TDS compatible with those supported by TDS .
- Activity Log Management
  - Additional support for auto roll of activity log including operator commands to roll it by size/count.

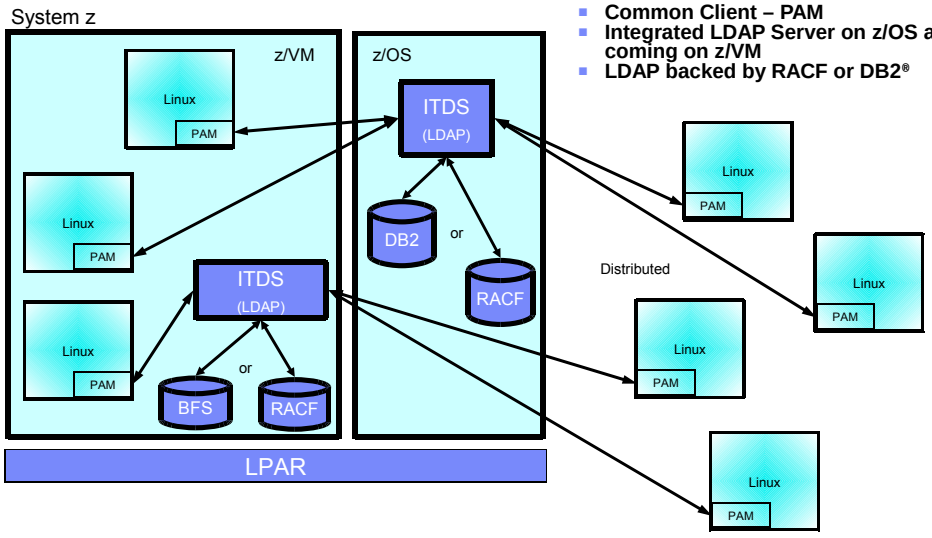
LDAP for z/OS Parallel Sysplex Support



IBM TDS has Multiple Backends

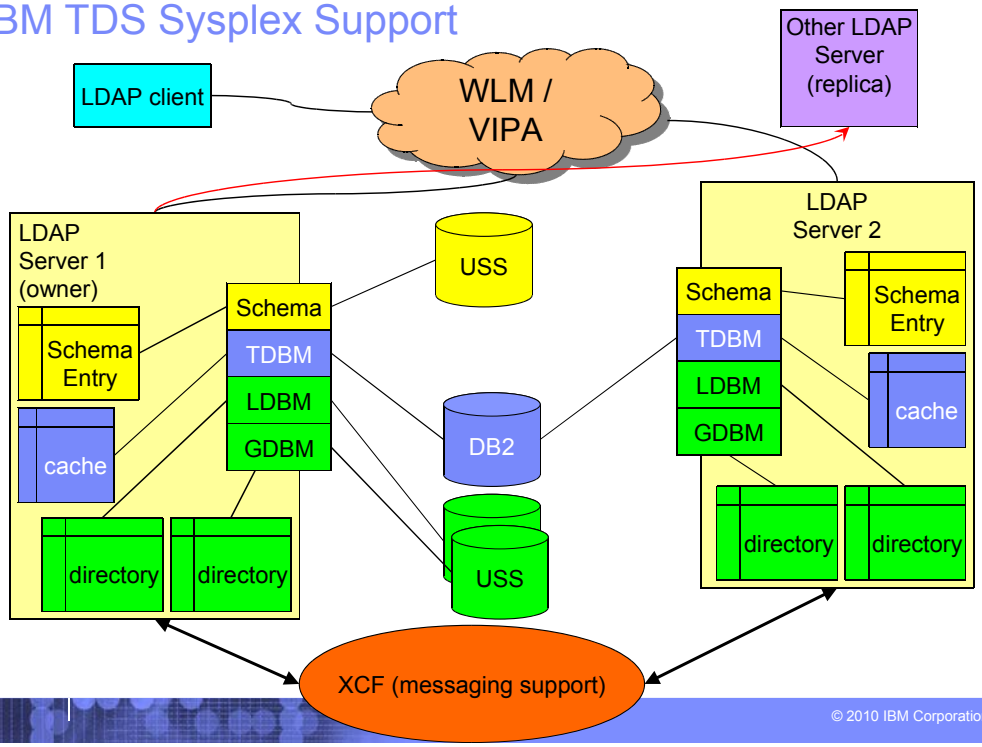
- **LDBM, TDBM**: General purpose directories
  - Full LDAP V3 support
  - Data stored in USS files (LDBM) or DB2 database (TDBM)
  - More Speed (LDBM) or More Room (TDBM)
- **SDBM**: RACF users, groups, and user-group connections
  - Provides remote RACF administration and authentication
  - Fixed schema
  - Data stored in RACF database
  - Limited search capability
- **GDBM**: Change log directory
  - Similar to LDBM or TDBM but restricted operations
  - Contains records of changes to other backends and RACF
  - User configurable to be stored in USS files or DB2

Centralized Authentication & User Management

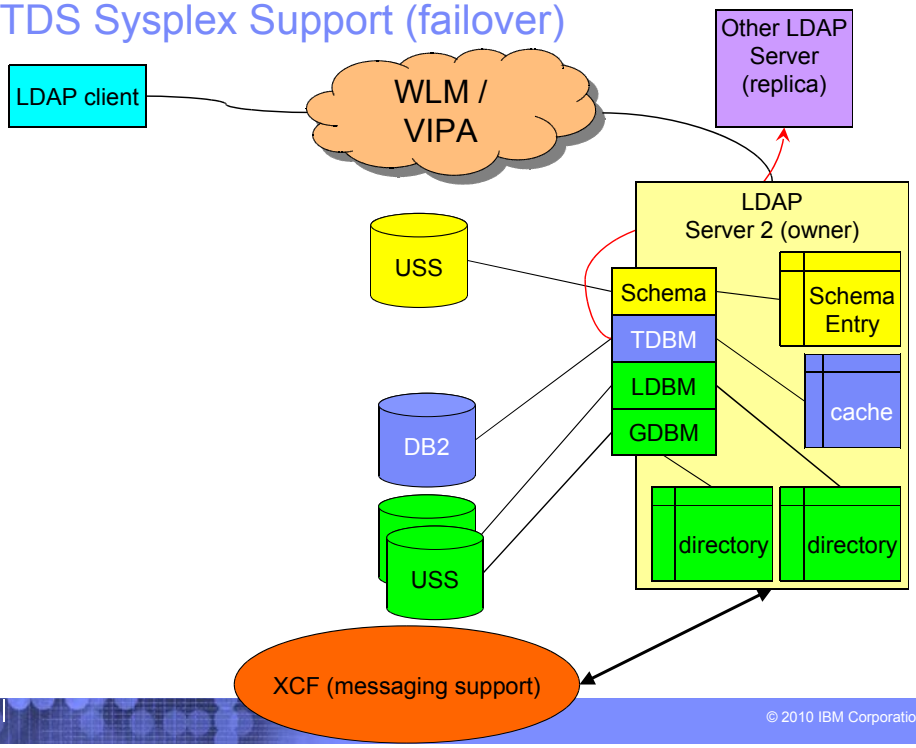


- **Common Client – PAM**
- **Integrated LDAP Server on z/OS and coming on z/VM**
- **LDAP backed by RACF or DB2®**

IBM TDS Sysplex Support



IBM TDS Sysplex Support (failover)



IBM TDS Sysplex Support - Continued

- First server in sysplex is the owner - Owns the resources
  - USS files (Schema, LDBM, and file-based GDBM)
    - Performs update and sends change to sysplex replicas
    - USS files must be in either zFS or shared HFS and available to all servers in the sysplex
  - Owns LDAP replication out of the sysplex

- Other servers are sysplex replicas
  - USS file based backends request directory from owner at startup
  - Applies changes from owner
  - Passes modification requests to owner

IBM TDS Sysplex Support - Continued

- TDBM and GDBM (DB2-based) backends are shared between all sysplex replicas
  - Uses DB2 data sharing
  - Notifies other LDAP servers of changes
  - Invalidates internal caches when notified of changes
- When owning server terminates
  - Oldest sysplex replica becomes owner
  - Owns resources
  - Replicates

IBM TDS Overview - Continued

- Runs in 31 or 64 bit mode (if using DB2-based backends only 31 bit)
- RAS enhancements
  - Enhanced error messages when processing configuration file
  - Create SMF 83 audit records for server events
    - **audit** *audit_option*
  - Automatic restart management (ARM) support
    - **armName** *name*
  - Server startup error monitoring
    - **srvStartUpError** [IGNORE | TERMINATE]
  - TCPIP error monitoring
    - **tcpTerminate** [TERMINATE | RECOVER]
  - File system error monitoring
    - **fileTerminate** [TERMINATE | RECOVER]
  - DB2 error monitoring
    - **db2Terminate** [TERMINATE | RECOVER | RESTORE]
      - Available previously
  - Creation of CTRACE records for server errors

New server utilities

- **ds2ldif** – Used to unload TDBM, LDBM, and schema backends
- **ldif2ds** – Used to load TDBM backend
- **dsconfig** – Used to configure IBM TDS

IBM TDS Schema

- Single server-wide schema used by all backends
  - Simplified name: **cn=schema**
- Stored as a file in USS file system - does not use DB2
  - Can change path with **schemaPath** configuration option
- Initial schema sufficient for SDBM and GDBM backends
  - Probably need to add schema for LDBM or TDBM
- Supports non-numeric OIDs for attribute and objectclass
  - Cannot use if sharing TDBM with ISS LDAP server
- Cannot change schema definition for existing data

IBM TDS LDBM Backend

- General purpose backend – stores any data
- Entries stored in USS files (DB2 not used)
  - Can change directory where LDBM files are stored with **databaseDirectory** configuration option
- Runs in 31 and 64 bit mode
- LDBM backend can be shared in a sysplex
- Can configure multiple LDBM backends
- Entries stored in memory while server is running
  - Advantage: fast access
  - Trade off: large directory requires a lot of memory and server start-up and shutdown is slow (reads in all those entries)
- Intended for small to medium size directory
  - About 250K entries in 31 bit, or 500K entries in 64 bit
- LDBM supports TDBM level of functionality
  - Aliasing, Native Authentication, Replication, change logging…

IBM TDS TDBM Backend

- Similar to TDBM in ISS LDAP server
- Uses a new set of replication tables
  - **DIR_REPLICA**, **DIR_REPENTRY**, **DIR_LONGREPENTRY**
  - Old replication tables are ignored if present
  - Replication on a backend level
- **DB_VERSION** set to ‘4.0’ for full function
  - Leave at ‘3.0’ if sharing TDBM with ISS LDAP server
    - Enhanced sysplex support and replication disabled
    - Schema updates that contain Non-numeric OID rejected
- Schema entry no longer stored in TDBM – now using LDAP server global schema

IBM TDS GDBM Backend

- GDBM can now be DB2-based or file-based:
  - GDBM is file-based unless the **dbuserid** configuration option is specified
  - File-based can run in 31 or 64 bit mode
    - Change path with **databaseDirectory** configuration option
  - DB2-based can run in 31 bit mode only
- logs changes to LDBM,TDBM,SDBM and schema entries
  - unless **changeLoggingParticipant** configuration option is set to **no**
  - RACF changelogging require RACF configuration

IBM TDS SDBM Backend

- Uses R_admin profile extract interface for obtaining user, group, connection entry
  - No limitations on amount of data returned
    - Complete list of groups to which user belongs and of members in a group
- RACF still limits output on search when using the RACF SEARCH command
- All data stored in RACF

New R10 Function

- **z/OS LDAP Password phrase**
- **RACF Custom User Field Support**
- **Certificate validation (map to RACF user ID)**
- **LDAP wait for DB2 during startup**
- **TDS Compatibility – SHA/MD5 encrypted passwords**
- **TDS Compatibility - Plug-in Support**
- **Operations monitor for gathering search statistics**
  - Will also be available on z/OS R8 and R9 via SPE

Note: NO functional enhancements to 'old' ISS LDAP server

z/OS LDAP Password Phrase

- **Used by SDBM or Native Authentication in LDBM or TDBM backends to bind**
  - Specified the same as a password
  - Anything longer than 8 characters is a Password Phrase

```
ldapsearch -D racfid=x,profiletype=user,cn=racf1 -w
  this1PhraseIsOk4Me …
```

- **RACF determines min and max length allowed**
- **Changed just like an SDBM/Native Auth password**
  - *<oldpwd>/<newpwd> during bind*
  - Via LDAP modify
- **Use SDBM to retrieve via Password Phrase PKCS 7 envelope**
  - racfPassPhraseEnvelope attribute
- **RACF can log Password Phrase changes in changelog**

RACF Custom User Fields

- Attributes can be added to Schema that map to a RACF custom field.
  - Specify RACF custom field info in new RACFFIELD keyword in ibmAttributeTypes definition
    RACFFIELD ('*racfFieldName*') or RACFFIELD ('*racfFieldName*' '*racfFieldType*')

attributeTypes: (SSN-oid NAME ('SSN') DESC 'Social Security Number' EQUALITY caseIgnoreIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 SINGLE-VALUE USAGE userApplications)

ibmAttributeTypes: (SSN-oid RACFFIELD ('USER-CSDATA-SSN' 'char') ACCESS-CLASS sensitive)

- Use field via normal SDBM operations (add/modify/compare/search)
  - ldapsearch …. –b racfid=x,profiletype=user,cn=racf1 "objectclass=*"

    racfid=x,profiletype=user,cn=racf1
    …
    ssn=000-11-2222

Certificate Validation

- Can fail certificate bind if not associated with a RACF user
  - New config option
    - sslMapCertificate {off | check | add | replace} {fail | ignore}
      - Default: **off fail**
- Now able to perform SDBM operations after Certificate, Kerberos or Native Authentication bind
  - RACF ID associated with bind identity is stored in bind info
  - SDBM operations after binding use RACF ID from bind info

LDAP Wait for DB2 During Startup

- LDAP server can now be started before DB2.
  - LDAP will wait for DB2.
  - No requests will be processed while waiting.
- Two new configuration options
  - **db2StartUpRetryLimit** ***num-retries***
    - Maximum number of times to retry connecting to DB2
      - Default is 0 (no retries)
  - **db2StartUpRetryInterval** ***num-seconds***
    - Number of seconds to wait between each retry attempt
      - Default is 45
- **srvStartUpError** config option determines LDAP behavior if no DB2 connection after retries
  - **ignore** – LDAP server initialization continues but DB2-based backends not available
  - **terminate** – LDAP server ends
- **db2Terminate** specifies LDAP behavior if DB2 goes down after DB2-based backends successfully start

TDS Compatibility – SHA/MD5 encrypted passwords

- Encryption tag can be either within the encrypted data or in the clear before the encrypted data.
- z/OS LDAP previously only allowed the tag within the encrypted data.
  - userPassword:: *base64encodedValue*
    where *base64encodedValue* is a base64 encoding of {*tag*}encryptedValue and *tag* is SHA or MD5
- Other LDAP server`s tag is before the encrypted data.
  - userPassword: {*tag*}*base64encoded_and_encryptedValue*
    where *tag* is SHA or MD5
- z/OS LDAP now supports both formats
  - Search optionally returns the new format.
    - New config option **pwSearchOutput** [binary | base64]

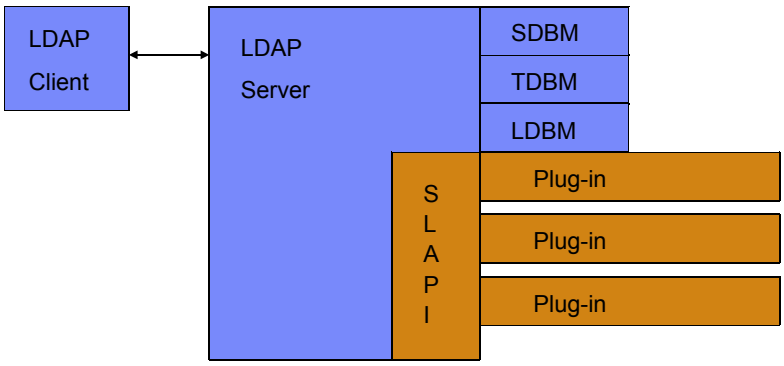
AES Encryption with ICSF

- Can use an AES key stored in the ICSF CKDS on **pwEncryption** and **secretEncryption** configuration options
  - Examples:
    pwEncryption AES:ICSFKEY
    secretEncryption AES:ICSFKEY
- AES encryption and decryption now occurs in ICSF if the AES key resides in the CKDS

TDS Compatibility - Plug-in Support

- **Customers and applications can add function to LDAP**
- **Plug-in is insulated against changes to LDAP internals**
- **Plug-in may be compatible with multiple LDAP platforms**
- **ICTX and HCD now exploit the Plug-in interface**

Plug-in Picture



Plug-in Overview

- New configuration option (plugin) to define a Plug-in
- 3 Plug-in types supported
  - **Pre-operation** – Plug–in called before each client request is processed (regardless of suffix)
  - **Client-operation** – Plug-in called to process a client request if
    - Target DN of operation is under a Plug-in suffix
    - Extended operation OID is registered for the Plug-in
  - **Post-operation** – Plug-in called after each client request is processed (regardless of suffix)
- Plug-in DLL is loaded by the LDAP server during startup
- Plug-in registers function pointers for LDAP server front-end calls
  - Only called for registered functions
- Also registers any suffixes it controls and extended operations it supports (client-operation only)
- LDAP server calls Plug-in when appropriate during client request processing

Building Plug-ins

- **slapi-plugin.h** – defines the data structures and service routine prototypes
- GLDSLP31.x and GLDSLP64.x provide LDAP server DLL entry points for 31-bit and 64-bit load modules
- New book to describe APIs and how to create a Plug-in
  - IBM Tivoli Directory Server Plug-in Reference for z/OS (SA76-0418)

Operations Monitor

- **Allows monitoring of search performance**
  - Detect SPAM and slow search performance
  - New subentry **cn=operations,cn=monitor** to hold search statistics
    - Use ldap_search to view statistics
  - Results show Client IP address, search request, and performance.
  - New global configuration options:
    - operationsMonitor
      - Specifies the granularity of the search operations monitored by the LDAP server
    - operationsMonitorSize
      - Maximum number of different search patterns to store in operations monitor (least recently used pattern is trimmed)

Sysplex Considerations

- All servers must be TDS servers at V1R10 level to get consistent results when using new functions in TDS V1R10
  - ISS LDAP server and older levels of TDS servers do not support the various new functions
  - V1R8 does not support Custom Fields
    - If RACF field added to v1R10 server, v1R8 servers in the sysplex group will not provide access
- Problem with older levels of TDS server in sysplex – cannot share schema due to extra fields (for RACFFIELD info)
  - APAR OA22022 - PTFs UA38112 and UA38113
    - RACFFIELD data could be lost
  - Not a problem in ISS LDAP servers - already ignore extra info

ISS to TDS Migration Considerations

- Utilities to migrate are available now
  - ISS is withdrawn in v1R11
- Configuration file changed
  - Example: DLL names and sysplex configuration options
  - Can use **dsconfig** to create new files and server proc
- TDBM schema migration
  - Done automatically by IBM TDS during initialization
  - Problem if multiple TDBM backends in ISS server with conflicting schema definitions

New R11 Function

- **LDAP Support for RACF Resource Profile**
  - New subtrees added to SDBM for for classes and for setropts
- **Advanced Replication Support**
  - New server plugin to support advanced replication configurations
  - Migration steps required to convert old replication to new support
  - Can continue to use old replication support
- **WLM Support**
  - LDAP worker threads assigned to WLM enclaves
  - Multiple enclaves supported

LDAP/SDBM Support for RACF Resources

- Extend SDBM hierarchy with new entries:
  - A class entry to represent each RACF class
  - A resource entry for each RACF resource profile
  - A setropts entry to represent RACF system values
- Use LDAP search to display RACF resource profiles and setropts settings
- Use LDAP add, modify, delete to manage RACF resource profile
  - RACF RDEFINE, RALTER, RDELETE, PERMIT, SETROPTS commands
- Log changes to RACF resource profiles in LDAP changelog
- Does not support DATASET resource profiles
- Limited RACF SETROPTS support

Advanced Replication Support

- **Supports the following replication configurations**
  - Peer-to-Peer, Master-to-Replica
  - Subtree replication
  - Cascade
  - Forwarding
  - Gateway
- **Additional Capabilities**
  - Replication filtering
  - Conflict Resolution
  - Additional Logging, Replication Error Log, Conflict Resolution Log
  - Queue Management
  - New Extended Operations (LDAPEXOP utility)
  - Interoperability with TDS Distributive platforms
  - Compare subtrees on different servers (LDAPDIFF utility)

WLM Support

- Directs ldap operations to run under WLM enclaves
- Work can be classified by client IP address and/or Bind DN
- Support dynamic reclassification of work via LDAP WLMEXCEPT operator modify command
- WLM health service used to update TCP/IP sysplex distributor load balancing

z/OS Security R12 – ITDS for z/OS

- Password Policy Support
  - Provided LDAP password quality, expiry, account lockout, warning of pending LDAP password expiry
- Dynamic LDAP ACLs using LDAP filters
  - Authority can be define based on:
    - IP address, Time of day and Day of week, clear or encrypted connection
      - SSL or non-SSL protected connections, Filters used wth aclEntry and entryOwner attributes
      - New LDAP operators to control ACLS: UNION, INTERSECT, REPLACE
  - Intended to provide capabilities similar to other LDAP implementations to help directory consolidation on z/OS
- Activity Log Manangement
  - Controls size of ITDS activity Log – new log file creaded when limits are readched:
    - Time of day, size in bytes or Console command
    - New single record format
    - Filter records by Clinet IP addres
- Salted SHA – Compatible with distributed ITDS, OpenLDAP
  - userPassword LDAP attribute in CDBM, LDBM and TDBM backends
- Schema Updates
  - Supports syntax and matching rules – supported by distributed ITDS, openLDAP and sunOne LDAP directory Severs
  - Improves migration and LDAP replication between ITDS distributed and ITDS for z/OS
    - 22 new Syntaxes, 14 new Matching rules

Improves the interoperability of z/OS ITDS and ITDS Distributed

Session Summary

- Overview of the IBM TDS for z/OS server
- Defined the functional content and benefits of IBM TDS
- Identified migration considerations
- ISS will NOT be shipped in v1R11

Publications References

- IBM TDS for z/OS server
  - SC23-5191 IBM Tivoli Directory Server Server Administration and Use for z/OS
  - SA76-0418 IBM Tivoli Directory Server Plug-in Reference for z/OS
- IBM TDS LDAP for z/OS client
  - SA23-2214 IBM Tivoli Directory Server Client Programming for z/OS
- Integrated Security Services LDAP server
  - SC24-5923 z/OS Integrated Security Services LDAP Server Administration and Use