z/OS LDAP: Overview and New Function Update

Valid thru z/OS 1.6
Session W16

Jack Jones in coordination with the IBM z/OS LDAP Development
Poughkeepsie NY
johnjone@us.ibm.com

Disclaimer

Trademarks

T r a d e m a r k s

The following are trademarks of the IBM Corporation. An asterisk following the name denotes a registered trademark.

ACF/VTAM*
ADSTAR*
Advanced Function Printing
Advanced Peer-to-Peer Networking
AIX*
AIX/6000
APL2*
APPN
Approach
AS/400*
C/VM
C/370
Callup
CICS
CICS/VSE*
Common User Access
Current
CUA
DataJoiner
DataPropagator
DB2*
DB2 Connect
DB2/2
DB2/6000
DFS
DFSMS
DFSMS/VM
DirMaint
DisplayWrite*
Distributed Relational Database Architecture
Domino
DRDA*
Enterprise Systems Connection Architecture
Enterprise Systems Architecture/390
ES/9000*
ESCON*
GDDM*
Hardware Configuration Definition
IBM*
IBM Business Partner
IBMLink
IMS
Language Environment*
Lotus Notes
Lotus SmartSuite
MQ
MQ Series
Multiprise
MVS*
MVS/ESA
MVS/SP
MVS/XA
Net.Data
NetView*
Notes
NotesPump
OfficeVision*
OfficeVision/VM
Open Blueprint
OSA
OS/2*
OS/390
Parallel Sysplex
PowerPC
PR/SM
PROFS*
QMF
RACF
RAMAC
RISC System/6000*
RS/6000
SQL/DS
SQL Master
System/390*
S/370
S/390*
S/390 Multiprise
S/390 Parallel Enterprise Server
TalkLink
Time and Place
Ultrastar
VisualAge
VisualGen
VisualLift
Visual Warehouse
VM/ESA*
VM/XA
VSE/ESA
VTAM*
Wordpro

The names listed below are trademarks or registered trademarks and are the properties of their respective companies.

ANSI
Apple
Beyond Software
C++
CATIA
CSS
DEC
DirectPC
EnterpriseWeb/VM
EnterpriseWeb Calendar
Enterprise View
Ethernet
Eudora
Gateway
Hewlett-Packard
HP
IEEE
ITAA
Java
KERBEROS
LAN Manager
Macintosh
Mortice Kern Systems InterOpen
NCR
NCE
NetWare
Network File System
Novell
NFS
Open Software Foundation
OSF, Motif
Outlook
POSIX
SAS
SnapShot
Sterling Software
Sun Microsystems
SunOS
ULTRIX
UNIX
VAX
VM:Webserver
Windows
Windows NT
XPG4
X-Windows

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

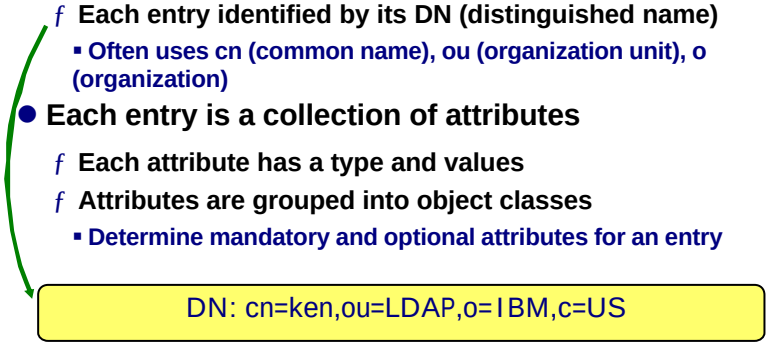
Agenda

- **LDAP Overview**
- **LDAP Authentication**
  - **Using RACF**
  - **Using TDBM**
  - **Native Authentication**
- **LDAP Authorization/Access Control**
  - **Under RACF**
  - **TDBM ACLs**
- **LDAP Change Log SPE**
- **z/OS V1R6 LDAP New Function**

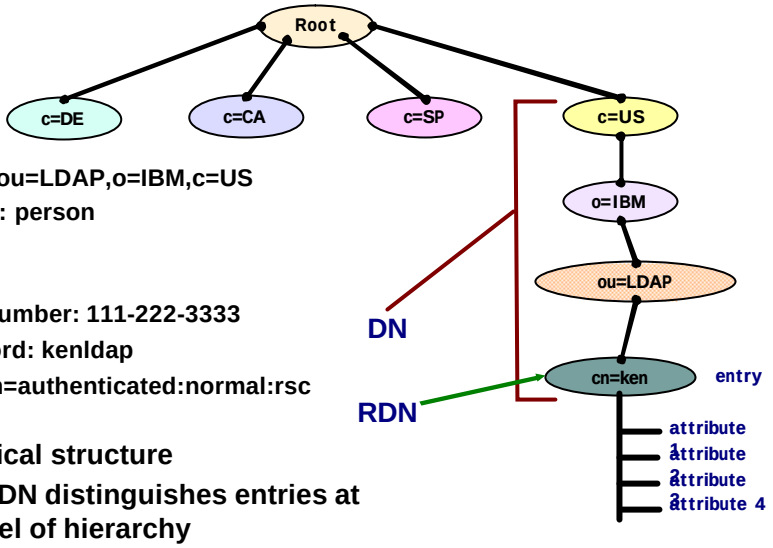
Overview of LDAP

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



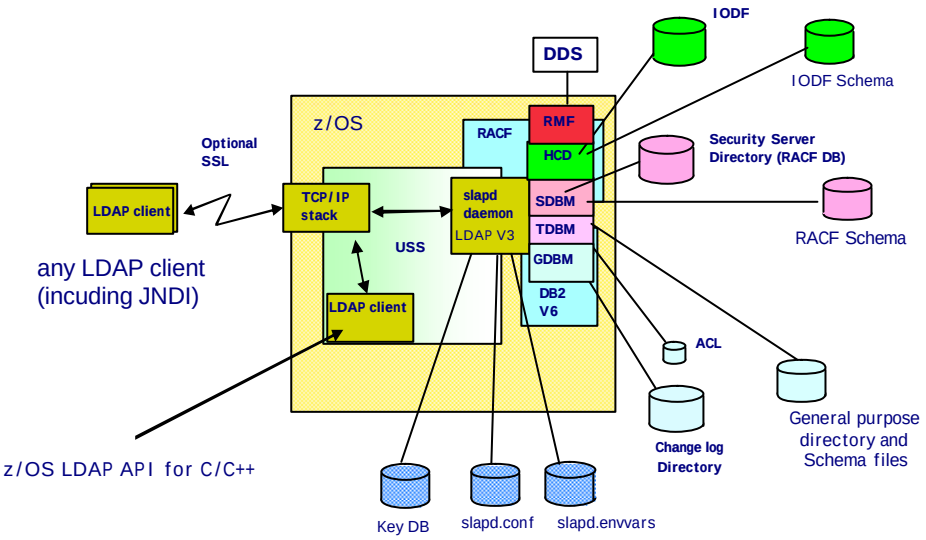
LDAP Directory Structure



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)**

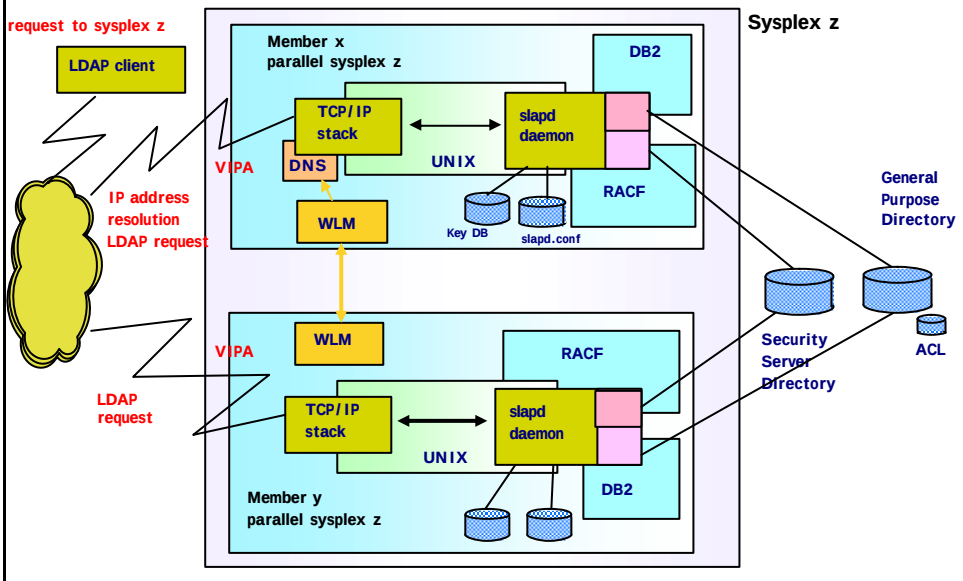
LDAP Server on z/OS

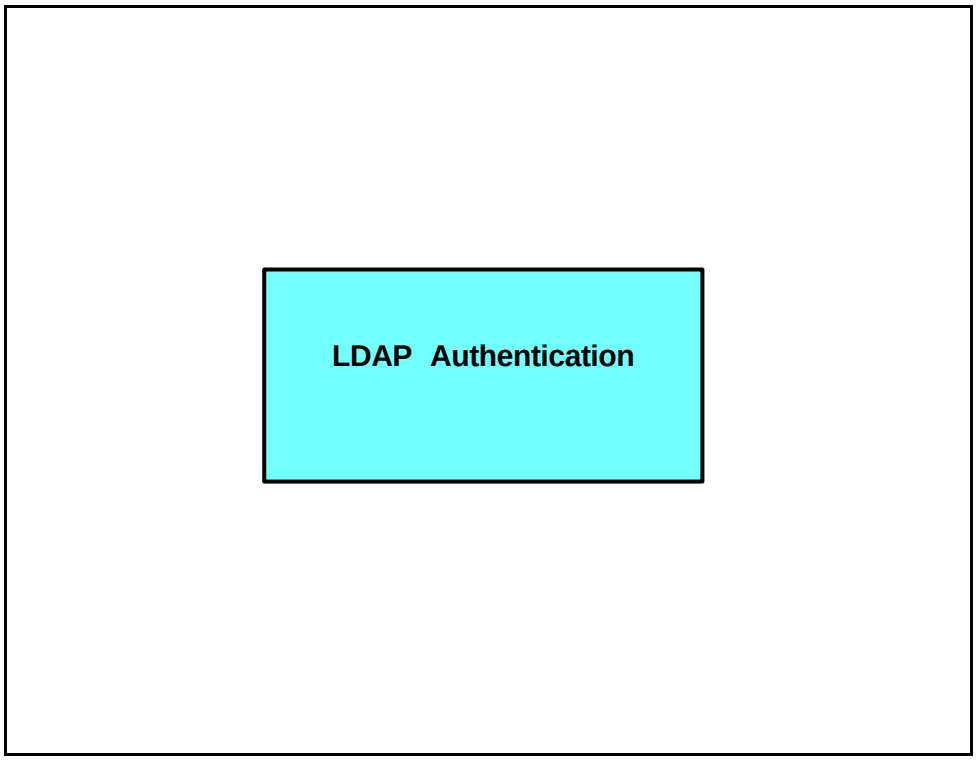


LDAP Server on z/OS...

- **LDAP Server has multiple backends (data stores)**
  - **TDBM: General purpose directory**
    - **Full LDAP V3 support, including modifiable schema**
    - **Data stored in DB2 database**
    - **Full scalability**
  - **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 TDBM (DB2 based) but restricted operations**
  - **Limited function special backends**
    - **HCD: IODF definitions, data in IODF - shipped with HCD**
    - **RMF: RMF data, stored in RMF DDS server - shipped with RMF**

LDAP for z/OS Parallel Sysplex Support

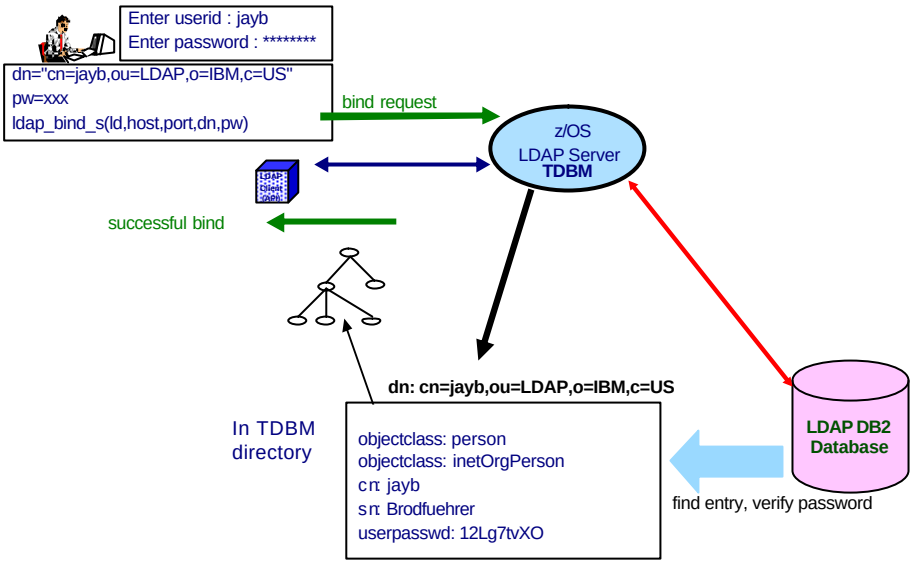




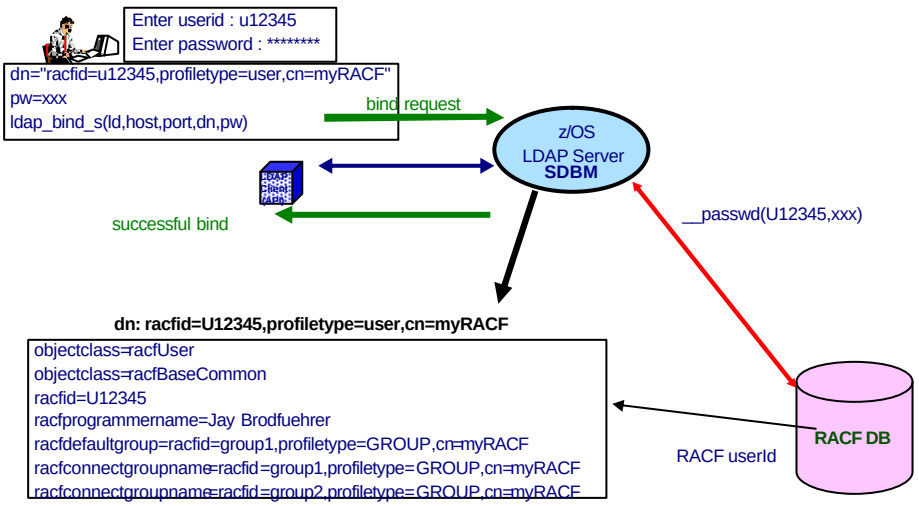
Authentication with an LDAP Server

- **LDAP is a stateful protocol**
  - **Session starts when client "binds" to server**
  - **Session can be unauthenticated (anonymous bind)**
  - **Authentication is performed during bind**
    - **Check password or certificate**
    - **Determine groups to which user belongs (for authorization checking)**
- **LDAP supports different authentication protocols**
  - **Simple bind: Distinguished Name and password**
    - **Session can optionally be protected with SSL**
    - **Passwords can be stored in LDAP directory, optionally one-way (MD5, SHA-1, crypt) or two-way (TDES) encrypted, or stored in RACF**
  - **Certificate bind: X.509 digital certificate over SSL**
    - **Distinguished name in certificate must conform with distinguished name of person authenticating**
  - **Kerberos bind: Kerberos principal sends ticket for LDAP server**
    - **Attribute: ibm-kn = principal @ realm**
  - **CRAM-MD5, DIGEST-MD5 binds: DN/userid and password**
    - **Client hashes password using MD5 encryption**

LDAP TDBM Authentication



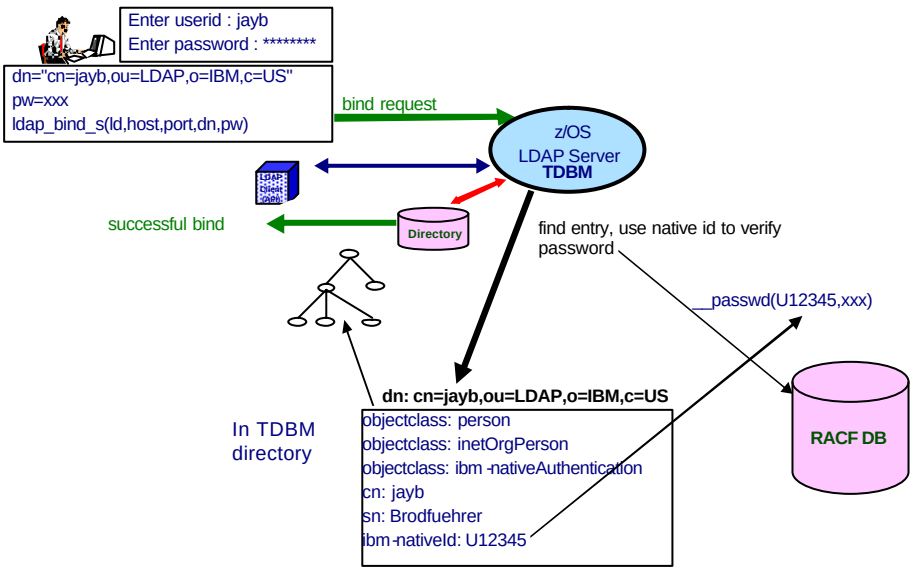
LDAP Authentication with SDBM (RACF)



z/OS LDAP Server Native Authentication

- **Disadvantage of Authentication in RACF:**
  - **SDBM backend required**
  - **Nonstandard Distinguished Name (racfid, profiletype)**
  - **Fixed schema: only RACF information is available, cannot add attributes to contain additional information**
- **Native Authentication uses TDBM backend**
  - **Standard Distinguished Name (e.g. cn, ou, o)**
  - **Any schema supported by LDAP V3 for person entry can be used**
    - **Any information supported by the schema can be retrieved**
    - **Use TDBM groups and group membership in ACLs**
  - **Authentication (password verification) performed by RACF**
    - **Password for entry is in security server (not in TDBM)**
    - **No need for administration or synchronization of multiple password registries**
    - **RACF authentication triggered by attribute ibm-nativeId in TDBM entry**
  - **Can limit native authentication to specific TDBM subtrees or entries - some entries use RACF, others have passwords in entry**

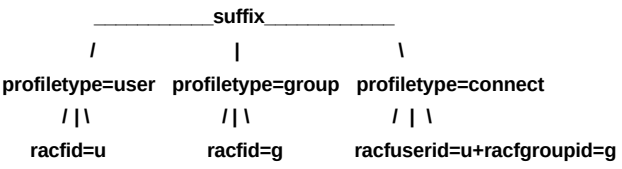
LDAP Native Authentication



Accessing RACF via LDAP

SDBM Support of RACF

- **Use LDAP to add, modify, delete, display RACF users, groups, and user-group connection - remote admin**
  - **Equivalent to RACF commands: ADDUSER, ALTUSER, DELUSER, LISTUSER, ADDGROUP, ALTGROUP, DELGROUP, LISTGRP, CONNECT, REMOVE**
- **SDBM directory structure**



example DN: racfid=kmorgan,profiletype=user,cn=myRacf

- **Hard coded schema definitions**
- **Limited search capabilities - predefined by SDBM**
- **All data accessed via RACF**
  - **No RACF Data in LDAP**
  - **Authorization controled by RACF, based on bound userid**

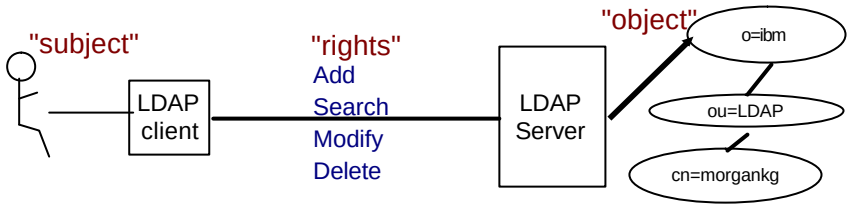
Changing the RACF Password

- **ldapmodify can be used to change RACF password**
  - **Via SDBM:**
    - **dn: racfid=G12345,profiletype=user,cn=myRACF**
      changetype: modify
      replace: racfPassword
      racfPassword: *new_password*
  - **Via TDBM with native authentication**
    - **dn: cn=jayb,ou=LDAP,o=ibm,c=us**
      changetype: modify
      delete: userPassword
      userPassword: *old_password*
      -
      add: userPassword
      userPassword: *new_password*
      -
    - **Note:** replace: userPassword **cannot be used - not supported**
- **LDAP SDBM or native authentication bind can be used to change a password (even if expired)**
  - **Specify *old_password*| *new_password***

Access Control in TDBM

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)**



Access Control Implementation

- **TDBM 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**

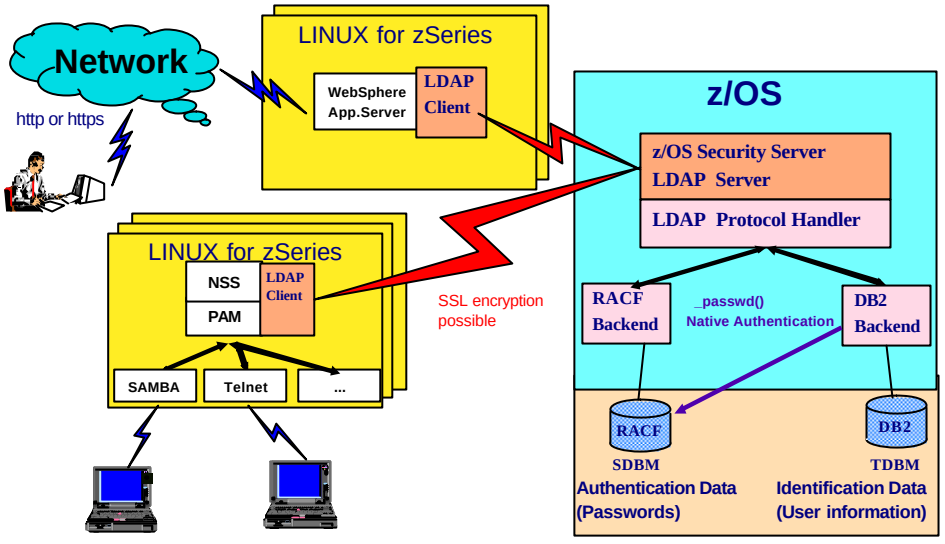
Special aclEntry "pseudo-DNs"

- **cn=anybody**
  - **Applies when no other specific ACL value applies**
- **cn=authenticated**
  - **Applies when the requestor has authenticated to the directory bu t 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

The Big Picture

User Information and Authentication in LDAP



Change Log SPE

LDAP-RACF Change Log SPE

- **Provides way to propagate RACF user changes (including password changes) to other systems**
- **RACF part:**
  - **Notifies LDAP when a change to a user occurs**
  - **Creates PKCS7 envelope containing clear password**
- **LDAP part:**
  - **Creates an entry containing the RACF info in the changelog directory (in new change log backend - GDBM)**
    - **Can be accessed using normal LDAP operations from any LDAP client**
  - **Supports retrieval of RACF password envelope via LDAP search**
- **Used by IBM Tivoli Directory Integrator to synchronize passwords:**
  - **Periodically does LDAP search of change log for new entries**
  - **If password changed, performs LDAP search of RACF user to retrieve enveloped password**
  - **Decrypts envelope and sets password on other systems**

Change Log SPE - continued

- **Searching the change log**

> ldapsearch … -b cn=changelog changenumber>=1023
CHANGENUMBER=1023,CN=CHANGELOG

```
objectclass: CHANGELOGENTRY
objectclass: IBM-CHANGELOG
changenumber: 1023
targetdn: racfid=U12345,profiletype=user,CN=MYRACF
changetime: 20030611161820.374472Z
changetype: MODIFY
changes: replace: racfpassword
racfpassword: *ComeAndGetIt*
-
ibm-changeinitiatorsname: racfid=RADM,profiletype=user,CN=MYRACF
```

- **Retrieving RACF envelope containing new password**

> ldapsearch –D racfid=cladmin,profiletype=user,cn=myRacf –w passwd –L -b racfid=U12345,profiletype=user,cn=myRacf "objectclass=*" racfpasswordenvelope

```
racfid=U12345,profiletype=USER,cn=myRacf
racfpasswordenvelope:: base-64_encoded_password_envelope
```

New Function in z/OS V1R6
LDAP

V1R6 Function Availability on Previous z/OS Releases

- **Late-breaking news: "IBM z/OS V1.6: Integrating new applications" announcement (#204-180, Aug 10, 2004)**
- **z/OS V1R6 LDAP fuctions will be made available on z/OS V1R4 and z/OS V1R5**
  - **In "LDAP Enhancements for z/OS V1R4/R5 and z/OS.e V1R4/R5" Web deliverable**
- **Will not support WebSphere Application Server for z/OS and OS/390, V4.0.1**
- **Planned availability: Nov 19, 2004**

Change Logging Enhancements

- **Problem: Have change log entries for RACF user changes but no indication of changes to TDBM entries**
- **Solution:**
  - **Create change log entry for each change to any TDBM entry**
    - **Including schema entry**
- **Same change log as for RACF changes**
  - **Change log entries from RACF and TDBM intermixed**
- **Complete changes attribute**
  - **userpassword value replaced with *ComeAndGetIt***
- **No suppport for enveloping TDBM password**
  - **Can already retrieve password (depending on encryption in use)**
- **Configuration options to turn on/off TDBM change logging**
  - **Default is ON**

Change Logging Enhancements - continued

- **Example of change log entry for add of a TDBM entry:**

CHANGENUMBER=1024,CN=CHANGELOG
objectclass: CHANGELOGENTRY
objectclass: IBM -CHANGELOG
changenumber: 1024
targetdn: cn=ken,o=Your Company
changetime: 20030611161820.374472Z
changetype: ADD
changes: objectclass: inetorgperson
cn: ken34
userpassword: *ComeAndGetIt*
sn: Morgan
telephonenumber: 123-456-7890
ibm-entryuuid: 59290000-73D7-1F7B-94ED-40206404095
-

ibm-changeinitiatorsname: racfid=dept68mgr,o=Your Company

Persistent Search (Event Notification)

- **Problem: Integrator products not notified when change to RACF user or TDBM entry occurs**
  - **Needed to continually poll change log**
- **Solution: Allow a search to persist**
  - **Optionally first return existing entries matching search criteria**
  - **Continue to return an entry each time it is changed and matches search criteria (base, scope, and filter)**
- **New control on search request to indicate persistent**
  - **LDAP Server config option to allow/reject persistent searches**
  - **Control can specify types of change to monitor (add, modify, delete, rename)**
- **Persistent search continues until client issues abandon or unbind**
- **Example: typical Integrator product persistent search**

base: cn=changelog scope: subtree filter: objectclass=*

types of change: add

Alias Support

- **Problem: need a simple, well-known name for an entry**
  - **Application shouldn't fail if entry containing information is moved**
- **Solution: allow creation of an alias entry that points to the 'real' entry**
  - **Alias DN can be much simpler than DN of real entry**
  - **Application uses alias entry**
  - **If real entry moves, just change pointer in alias entry**
- **Alias support involves**
  - **Creating an alias entry which points to another DN**
  - **Supporting dereferencing during search**
    - **When find alias entry, continue search using DN pointed to**
      - Must be within same backend
      - Can contain an alias (dereference it!)
  - **Alias support in TDBM only (not SDBM)**
- **Dereferencing is only done during search operation**
  - **Client specifies level of dereferencing on search request**

Alias Support - continued

- **Example:**
  - **If create alias entry**

    ou=LDAPZOS,o=IBM

    to point to 'real' entry

    ou=DEPTC8NG,o=Pok,o=IBM_US,o=IBM

  - **And do a dereferenced search with base DN**

    cn=morgankg,ou=LDAPZOS,o=IBM

  - **Search dereferences alias within base DN and processes entry**

    cn=morgankg,ou=DEPTC8NG,o=Pok,o=IBM_US,o=IBM

  - **Normal (non-dereferenced) search would return LDAP_NO_SUCH_OBJECT**

- **Warning:**
  - **Alias dereferencing degrades search performance**
  - **Some clients (e.g. JNDI client) set dereferencing on by default**

Enhanced Access Groups

- **Problem: limited ways to create large access groups**
  - **Used in determining group membership for ACL checking**
- **Solution: provide more ways to create TDBM groups**
- **Static groups: added ways to specify members**
- **Additional types of groups**
  - **Dynamic groups**
    - **Membership defined by a search expression: base, scope, and filter**
    - **Membership re-evaluated each time dynamic group is used**
  - **Nested groups**
    - **Group of groups - create hierarchy of groups**
    - **Contains names of other static, dynamic, and nested groups**
- **New attributes to determine group membership**
  - **ibm-allMembers - returns all members of a group**
  - **ibm-allGroups - returns all groups to which a user belongs**
  - **Supported on search and compare operations**
  - **Resolves nested group hierarchy and dynamic membership**

Peer to Peer Replication

- **Problem: if master (read-write) server fails, difficult to reset a read-only replica to become a master**
- **Solution: support multiple read-write master servers**
  - **If one fails, direct updates to another one**
- **Peer replicas**
  - **All read/write**
  - **Replicate update operations to one another**
- **Replica network can contain peer replicas and read-only replicas**
  - **Each peer must replicate updates to all other replica servers**
  - **Each read-only replica must refer update requests to a peer server**
    - **Can set up list of peer servers to contact until get response**

DB2 Restart and Recovery

- **Problem: LDAP server doesn't react if DB2 terminates**
  - **Client requests fail, LDAP administrator unaware of problem**
- **Solution: monitor DB2 and react accordingly**
- **If DB2 fails, LDAP server can optionally**
  - **Terminate**
    - **Useful in SYSPLEX - requests get routed to other LDAP servers**
  - **Or sever DB2 connections and reconnnect to DB2 when DB2 restarts**
    - **Client requests to DB2- based backends refused while DB2 is down**
    - **Other backends (e.g. SDBM) can continue to be used**
- **Configuraton option to set reaction mode**

Schema Migration

- **Problem: large number of complaints about schema migration**
  - **Updating schema between releases or for service is not a trivial task for customers**
  - **Cannot just modify using latest schema file**
    - **modify 'add' fails due to duplicate values**
    - **modify 'replace' removes all extra values added by customer**
- **Solution: enhance schema modification to support replacing specific schema values for modify 'replace'**
  - **If 'replace' value**
    - **is in schema - replace existing value with new value**
    - **is not in schema - add new value to schema**
  - **All other attribute values remain unchanged**
- **Config option and modify operation control to use new or old schema replace behavior**
  - **New behavior is the default**

Additional Schema Enhancements

- **Problem: no easy way to fix a schema attribute with an incorrect OID**
  - **All entries using this attribute lose access to the attribute**
- **Solution: allow special OID change schema modify**
  - **Entries using the attribute do not have to be changed**
- **Problem: Over 20 small schema files shipped by LDAP**
  - **Made service harder to apply**
  - **Too difficult to keep up to date**
- **Solution: only ship 2 combined schema files**
  - **schema.user.ldif and schema.IBM.ldif contain all contents of the small files**
  - **Schema philosphy:**
    - **z/OS LDAP ships general base schema**
    - **Applications need to ship their specific schema**

Cache Monitoring

- **Problem:**
  - **No way to determine if caches are effective or to change cache sizes**
  - **Improve search performance in TDBM (continual goal)**
- **Solution**
  - **Improve cache usage monitoring**
    - **Detailed performance info now kept in cn=monitor entry**
    - **Can view by ldapsearch or by operator MODIFY command**
  - **Configuration options to set size of each cache**
  - **Add TDBM search filter and entry caches**
    - **Contains search results**
    - **Another search for same base, scope, filter, dereference can retrieve results from cache**
    - **Search filter cache cleared whenever any entry is changed**

Cache Monitoring - continued

- **Example of monitor output:**

```
>ldapsearch  ...  -b cn=monitor   "objectclass=*"

...
cn=backendtdbm1,cn=monitor
...
entry_cache_size=5000
entry_cache_current=11
entry_cache_hit=11
entry_cache_miss=0
entry_cache_percent_hit=100.00%
entry_cache_refresh=0
entry_cache_refresh_avgsize=0
filter_cache_size=5000
filter_cache_current=2
filter_cache_hit=1
filter_cache_miss=2
filter_cache_percent_hit=33.33%
filter_cache_refresh=0
filter_cache_refresh_avgsize=0
filter_cache_bypass_limit=100
```

Miscellaneous Enhancements

- **ldapcnf (LDAP configuration tool) enhancements**
  - **Can now use ldapcnf to configure GDBM (change log backend)**
  - **Can now configure any combination of backends**
    - **TDBM, GDBM, SDBM, and PC interface**
- **LDAP executable code now installed in SYS1.SIEALNKE (was *GLD*.SGLDLNK)**
  - **Easier to use since already APF authorized and in LINKLST**
    - **STEPLIB removed from JCL and shell scripts shipped by LDAP**
  - **Other LDAP datasets not moved**
    - ***GLD*.SGLDEXEC, *GLD*.SGLDEXPC, *GLD*.SGLDHDRC, *GLD*.SGLDSAMP**

Miscellaneous Enhancements - continued

- **Enhanced z/OS LDAP client**
  - **SOCKS Version 5 support**
  - **64-bit support**
- **Added support for IPv6 addressing (in client and server)**
- **Capabilities attributes added to rootDSE entry**
  - **Indicate capabilities of the z/OS LDAP server**
    - **Allows an application to determine what functions it can use**
  - **ibm-supportedCapabilities - functions supported by z/OS LDAP**
  - **ibm-enabledCapabilities - supported functions that can be currently used**
  - **Example:**

```
> ldapsearch ...  -s base   -b ""   "objectclass=*“
...
ibm-supportedcapabilities=1.3.18.0.2.32.3
ibm-enabledcapabilities=1.3.18.0.2.32.3
```

References:

- **z/OS LDAP Documentation**
  - **SC24-5923 z/OS Integrated Security Services LDAP Server Administration and Usage Guide**
    - **http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHZBK42**
  - **SC24-5924 z/OS Integrated Security Services LDAP Client Programming**
    - **http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHZBK42**
- **Redpaper: Linux on IBM zSeries and S/390: Securing Linux for zSeries with a Central z/OS LDAP Server (RACF)**
  - **http://www.redbooks.ibm.com/redpapers/abstracts/redp0221.html**
- **PAM Documentation:**
  - **http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/pam-4.html**
- **NIS Schema for z/OS LDAP Server:**
  - **ftp://www.redbooks.ibm.com/redbooks/REDP0221**
- **Contacting me**
  - **e-mail: johnjone@us.ibm.com**