z/OS LDAP Overview and Announcements (SHARE Session 1721)

Tim Hahn
IBM z/OS LDAP Development
hahnt@us.ibm.com

Directory Services on OS/390 and z/OS

- OS/390 provides services for serving Directory information
  - TCP/IP provides DNS
  - Security Server provides 3 Directories
    - Security Server - OS/390 users, groups, other classes
    - LDAP Server - general repository for locating and configuration information
    - DCE Security Server - users, groups, organizations for DCE

Why is a Directory Service Important?

- Example - Domain Name Service (DNS). We use it everyday - without it we wouldn't find services on the Internet.
- Within an Intranet or across the Internet there is a need to provide "locating information". Example - BigYellow.com.
- In addition, remote, distributed, single point of control is necessary for Enterprise Management. Example - DEN (Directory Enabled Network).
- Some view this as the key to PKI (Public Key Infrastructure) and Single Sign-On.

What is LDAP?

- LDAP - Lightweight Directory Access Protocol
- de-facto Internet (TCP/IP-based) wire protocol for accessing and updating directory information
- "V2" defined in Internet Drafts
- "V3" defined in IETF RFCs 2251-2256, 2829, 2830
- New RFCs all the time (e.g. RFC 2849 - LDIF format)
- Protocol defines interfaces between a client and a server for requesting and returning information

z/OS LDAP Components

- ➤LDAP C/C++ APIs (client)
  - ➤DLL provides interfaces that can be called from C or C++ programs to contact any server supporting the LDAP protocol
  - ➤APIs are callable from COBOL via C; but not callable from CICS applications
- ➤LDAP Java APIs (client)
  - ➤JNDI interface, available as of V2R7
  - ➤Compatible with AIX JNDI (OW41326)

Features of the z/OS LDAP Clients

- ➤ Secure communications using SSL
- ➤ LDAP V3 protocol support
    - ➤ Certificate Bind (SASL bind)
    - ➤ Controls
    - ➤ V3 referrals
    - ➤ SOCKS support
- ➤ Client ships as ALWAYS ENABLED in z/OS Security Server

z/OS LDAP Components

- LDAP Server
  - Accepts and responds to LDAP protocol requests
  - Supports DB2 backing store(s) and access to RACF
  - OS/390 R10 scalability improvements
  - OS/390 R10 "V3" schema support
  - z/OS R1 LDAP configuration utility
- Server ships as ALWAYS ENABLED in z/OS Security Server
- For customers to use LDAP clients or server, MUST install z/OS Security Server

Features of the OS/390 LDAP Server (pre-V2R10)

- OS/390 R5
  - Secure communications using SSL
  - Multiple Concurrent Servers
- OS/390 R7
  - Sysplex Support
  - DB2 and RACF backing stores
  - Extended group searching for access control checking
- OS/390 R8
  - LDAP V3 protocol support (partial) - rootDSE, certificate bind, V3 referrals, UTF-8

Features of the OS/390 LDAP Server with V2R10 & z/OS R1

- OS/390 V2R10
  - LDAP V3 protocol support (more complete)
    - Schema publication and update
    - Many more syntaxes and matching rules
    - Case Sensitive attributes in distinguished names
    - limited Modify DN support
  - Scalable backend/TDBM
    - Small/fixed DB2 data model allows for tuning
    - Allows multiple DB instances
    - Access control check performance improvements
    - New bulkload utility for TDBM
- z/OS R1
  - LDAP configuration utility
  - Native Authentication

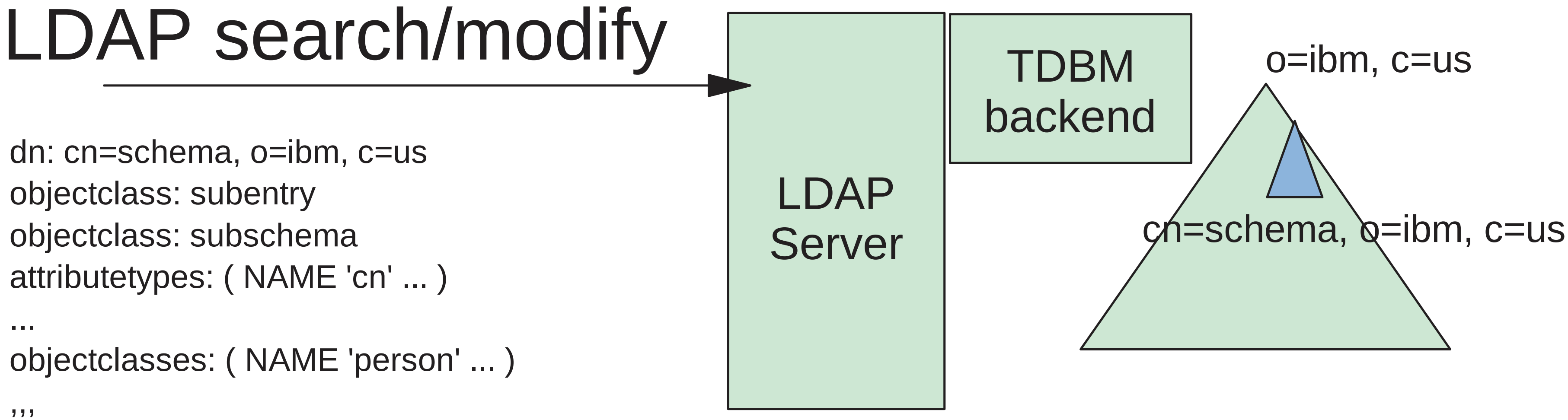
Features of the z/OS R2 LDAP Server

- z/OS R2
  - LDAP Server
    - concurrent session scalability (up to 64K sessions)
    - access to additional RACF USER profile fields
    - access/update of RACF USER-GROUP connections
    - Kerberos-based authentication (SASL GSSAPI)
  - LDAP Client
    - DNS locate capability for LDAP C/C++ client
    - Client search result caching for LDAP C/C++ client
    - Kerberos-based authentication (SASL GSSAPI)

Schema pub & update

- Schema publication per RFC 2251-2252 - TDBM and SDBM backends
- Schema appears as an entry in the directory
  - Attribute types
  - Object Classes
  - Matching Rules
  - Syntaxes
- Schema update via LDAP protocol (LDAP MODIFY operation) - TDBM only
- Server ships schema definitions for a large number of known schemas (for use with TDBM, SDBM schema is unmodifiable)

Schema pub & update

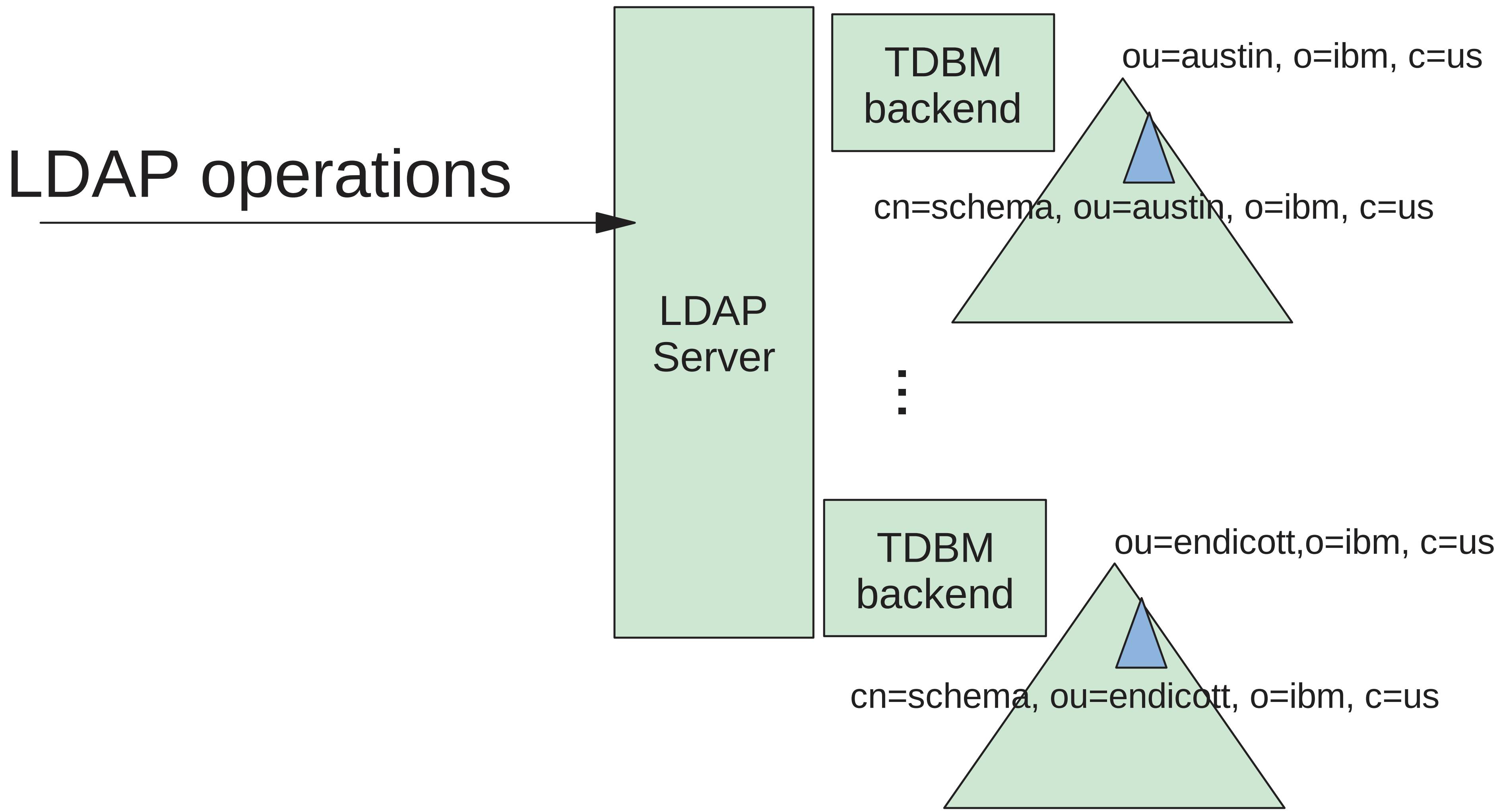


dn: cn=schema, o=ibm, c=us
objectclass: subentry
objectclass: subschema
attributetypes: (NAME 'cn' ...)
...
objectclasses: (NAME 'person' ...)
,,,

Scalable Backend/TDBM

- New database implementation to support higher scalability
  - Uses a small/fixed number of DB2 tables
  - Concurrent search/update
- Allows multiple "instances" of backends to be enabled
  - Use this to "partition" your tree
- Schema is backend "instance" specific
- Minimal configuration options
- All attributes are "indexed"
- **NOTE: RDBM to be removed - USE TDBM!**

Scalable backend/TDBM



LDAP operations

LDAP Server

TDBM backend

ou=austin, o=ibm, c=us

cn=schema, ou=austin, o=ibm, c=us

⋮

TDBM backend

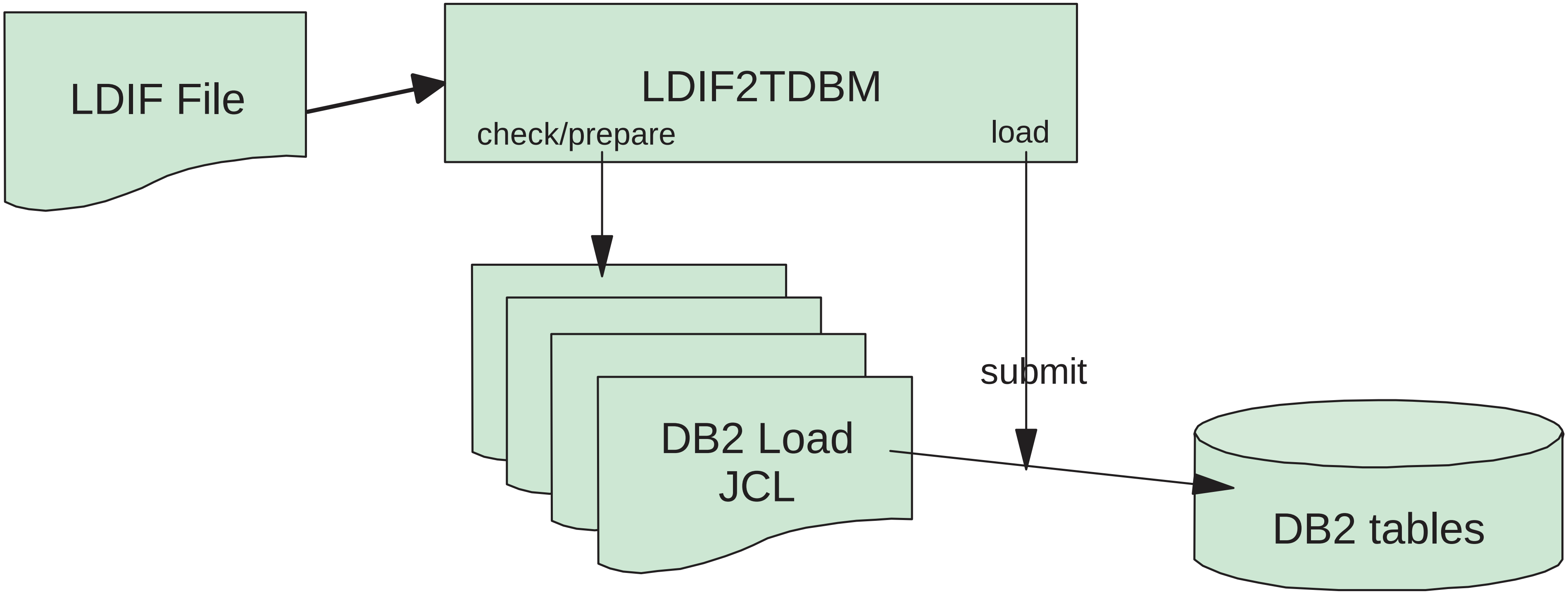
ou=endicott,o=ibm, c=us

cn=schema, ou=endicott, o=ibm, c=us

Bulk load utility - ldif2tdbm

- Scalable backend requires new bulk load command ldif2tdbm to replace the ldif2db command.
- ldif2tdbm load uses DB2 LOAD facility to increase bulk load speed
- ldif2tdbm "check" step can be done while LDAP server is running
- ldif2tdbm "prepare" and "load" steps can be done while LDAP server is operating in "read-only" mode
- From TSO, use LDF2TDBM

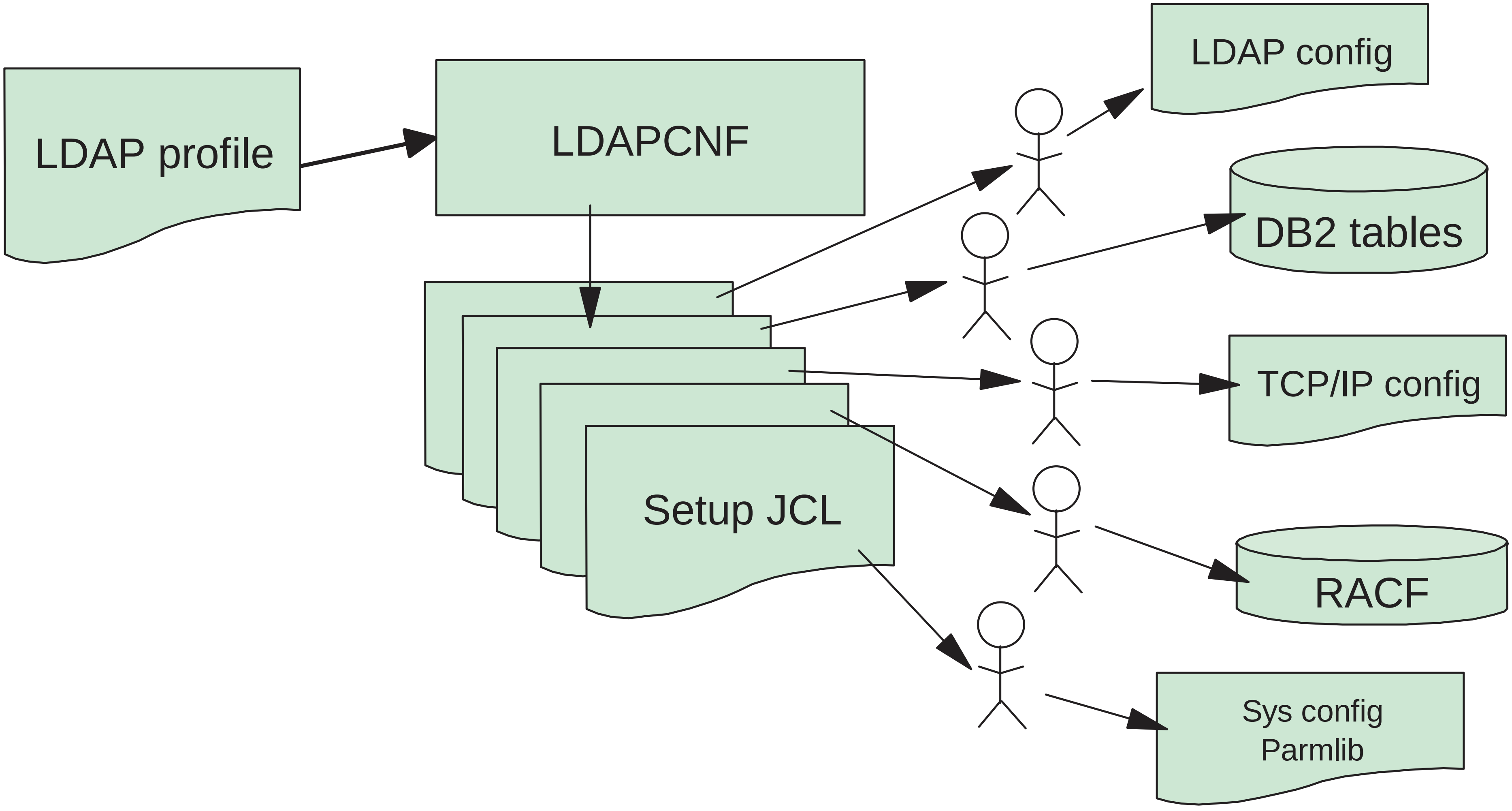
Bulk load utility - block diagram



LDAP Configuration Utility

- Streamlines implementation of LDAP servers on a system
- Input is a set of parameter files
- Output is a set of batch jobs (JCL)
- Batch jobs should be verified by
  - Network Administrators
  - Database Administrators
  - Security Administrators
  - System Programmers
  - LDAP Administrators
- Once acceptable, batch jobs should be submitted which will create the necessary configurations and settings for the server

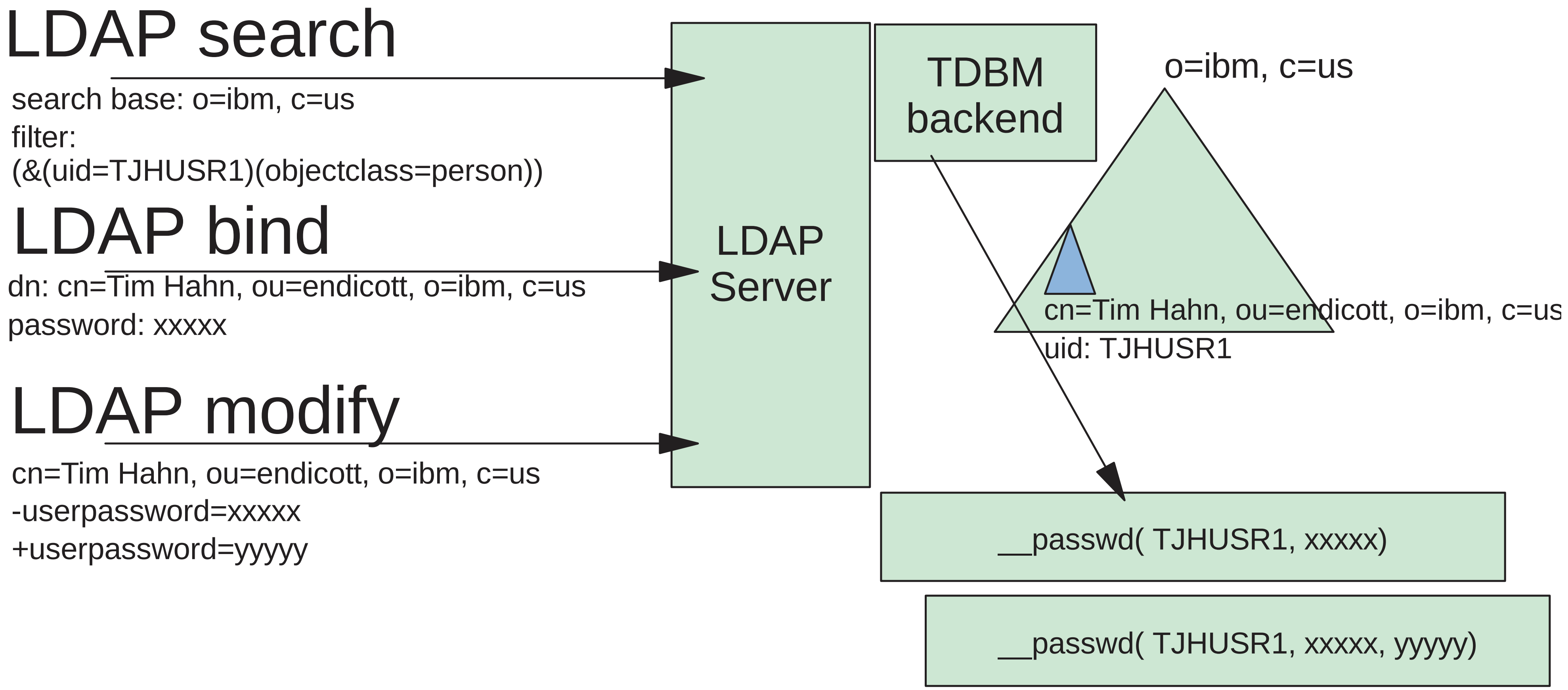
LDAP Configuration Utility



Native Authentication (OW47596)

- Allows appropriately set up directories to take advantage of SAF-accessed password strength and control
- Allows web-based login using SAF-accessed password and LDAP
- Relies upon proper set up of information in both SAF security server and DB2-based backing store (TDBM)
- How it works:
  - If configured, if `uid` value in TDBM directory entry matches OS/390 userid, then password check is done using `passwd()` service

Native Authentication



LDAP search

search base: o=ibm, c=us

filter:
(&(uid=TJHUSR1)(objectclass=person))

LDAP bind

dn: cn=Tim Hahn, ou=endicott, o=ibm, c=us

password: xxxxx

LDAP modify

cn=Tim Hahn, ou=endicott, o=ibm, c=us

-userpassword=xxxxx

+userpassword=yyyyy

LDAP Server

TDBM backend

o=ibm, c=us

cn=Tim Hahn, ou=endicott, o=ibm, c=us

uid: TJHUSR1

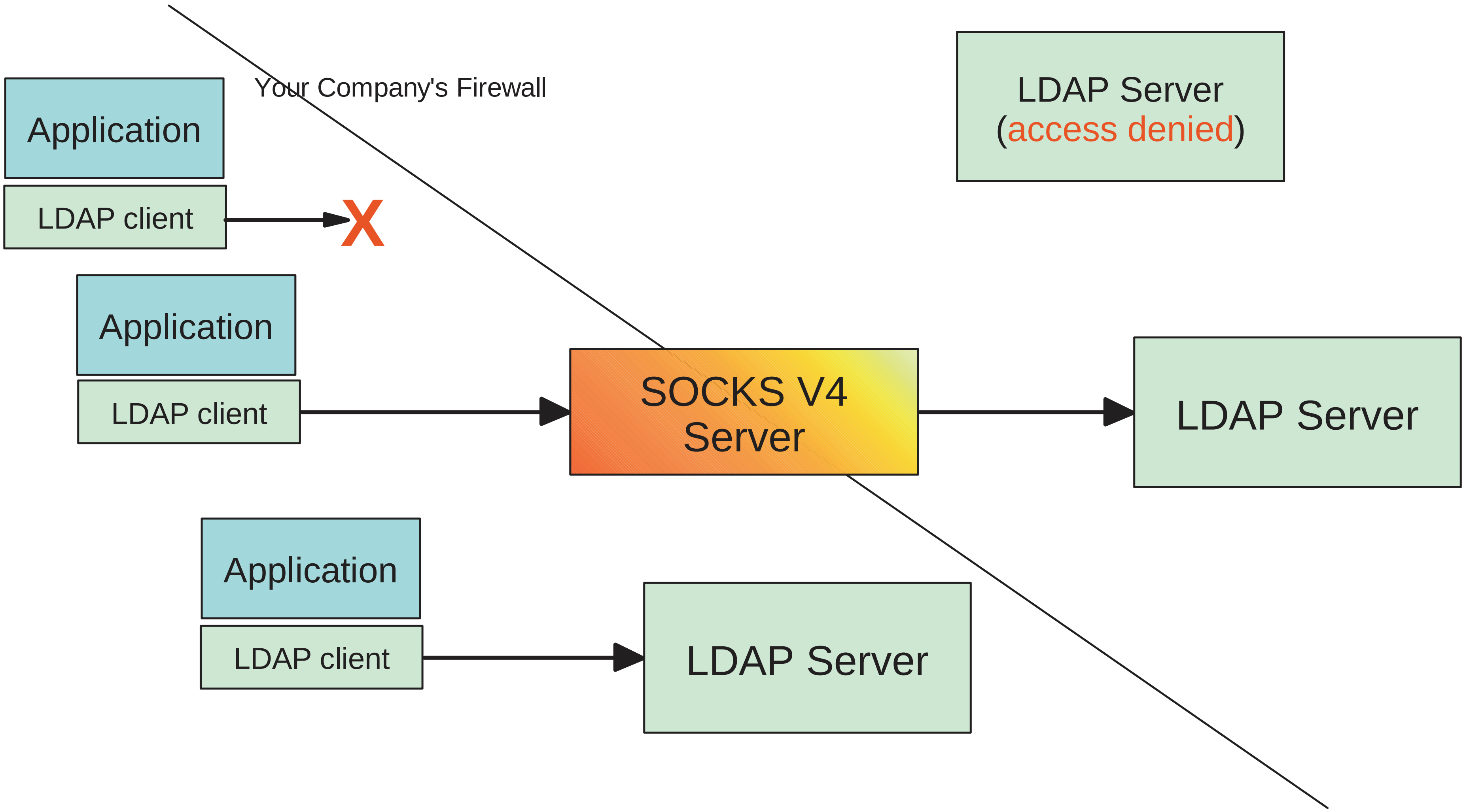
__passwd(TJHUSR1, xxxxx)

__passwd(TJHUSR1, xxxxx, yyyyy)

LDAP Client SOCKS support

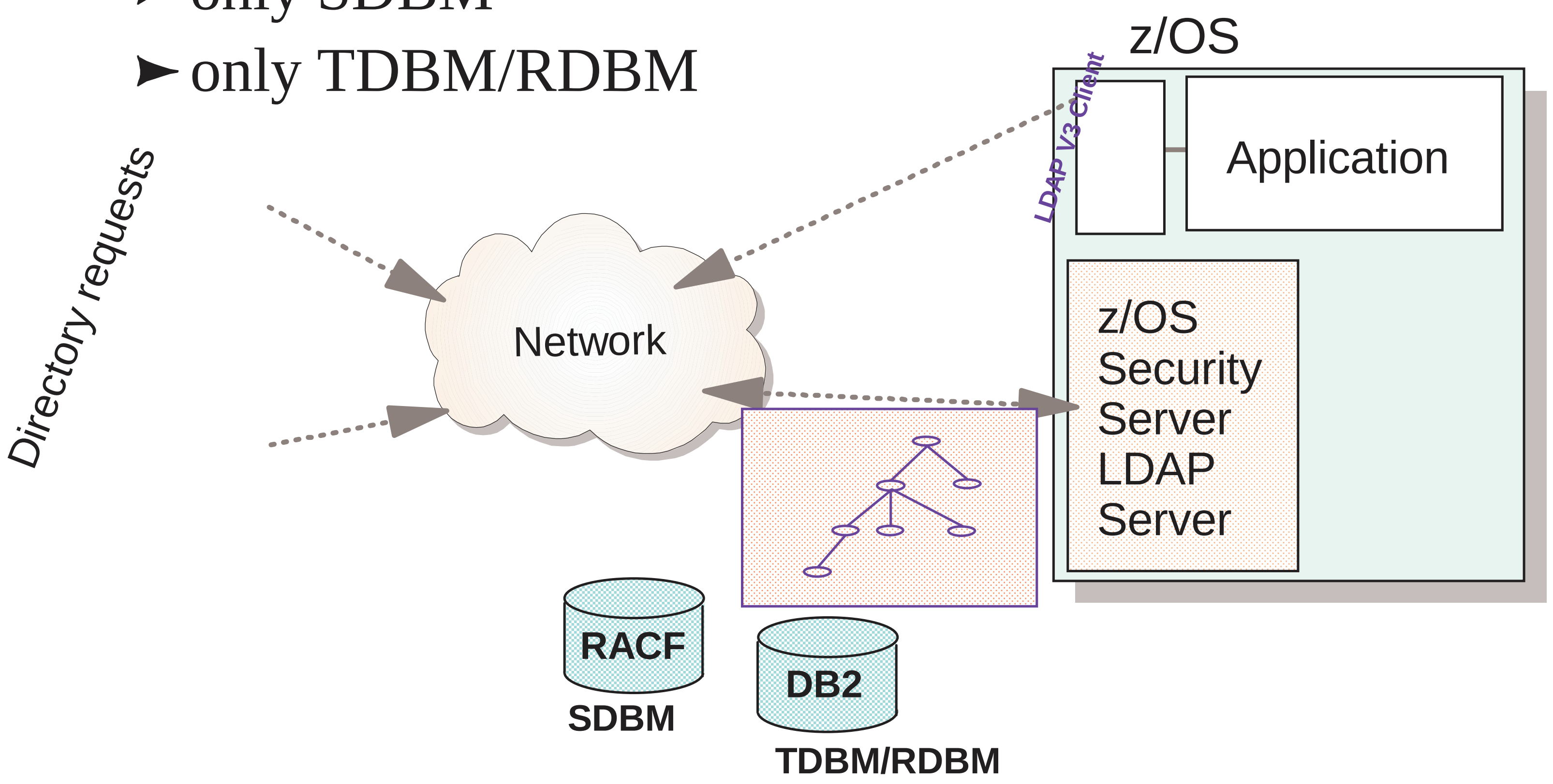
- ➤ LDAP C language client on z/OS now supports accessing servers through a SOCKS server
- ➤ LDAP servers on the Internet can now be contacted, searched, and updated from applications running on z/OS
- ➤ Useful for applications which must lookup Certificate Revocation Lists (CRLs)
- ➤ Configured using environment variables and optional socks.conf configuration file

SOCKS Support



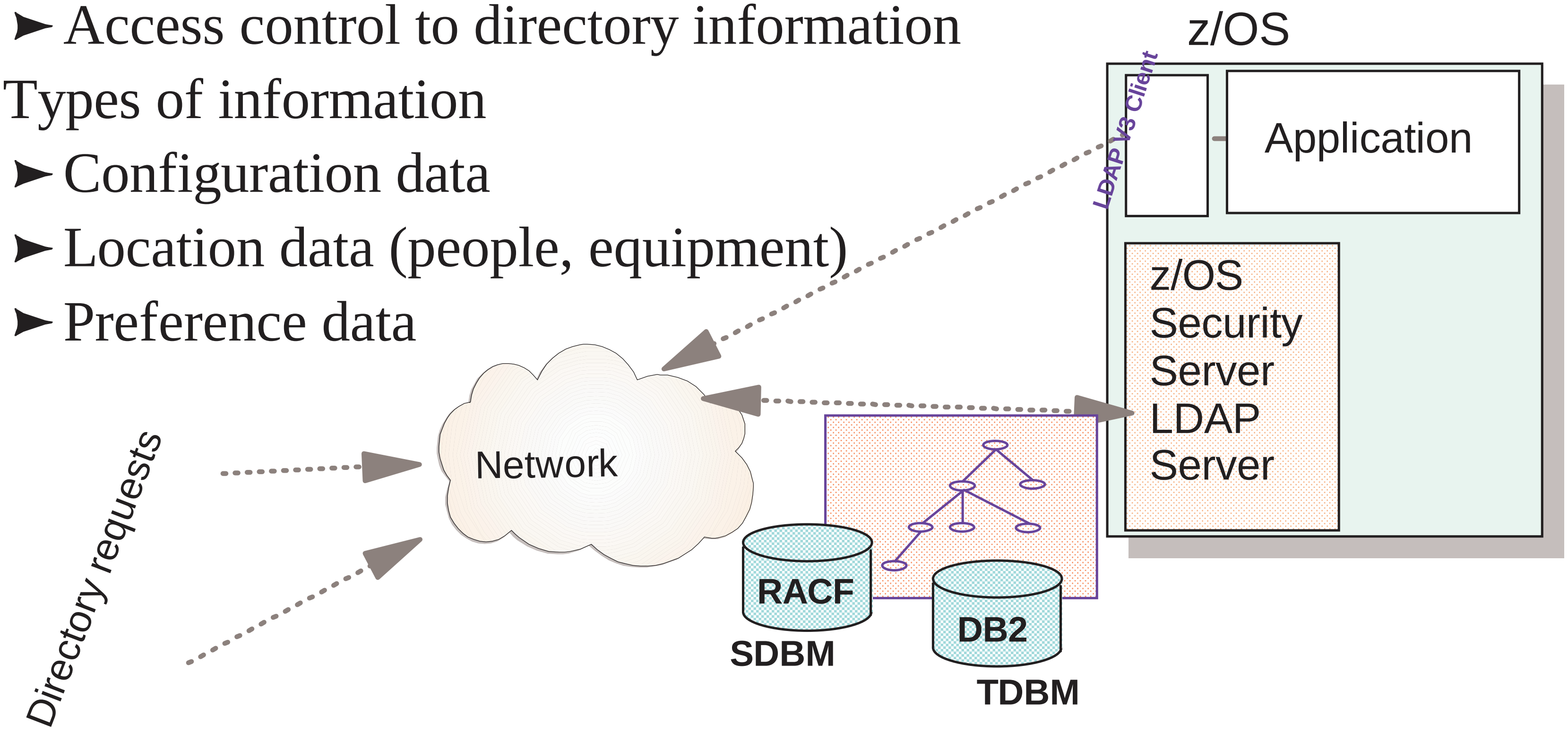
LDAP Server Configurations

- ➤ LDAP Server can run with
  - ➤ both SDBM (RACF) and TDBM/RDBM (DB2)
  - ➤ only SDBM
  - ➤ only TDBM/RDBM

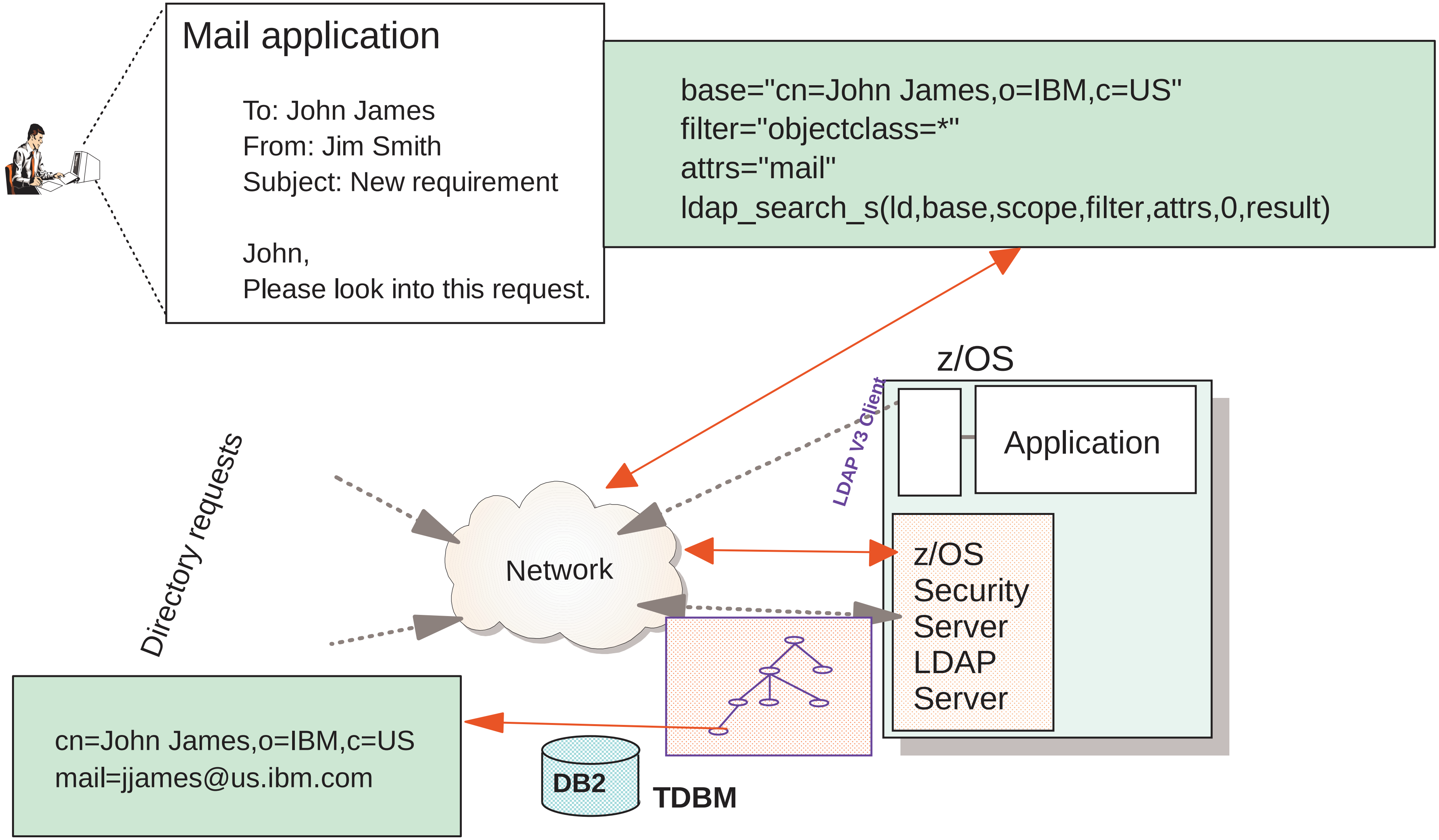


LDAP Server Usage

- As a Security Tool
  - Authenication of Users
  - Support for Digital Certificates and Public Key
  - RACF (OS/390 only) Access
  - Access control to directory information
- Types of information
  - Configuration data
  - Location data (people, equipment)
  - Preference data



Customer Scenario
E-mail Lookup



Mail application

To: John James
From: Jim Smith
Subject: New requirement

John,
Please look into this request.

```
base="cn=John James,o=IBM,c=US"
filter="objectclass=*"
attrs="mail"
ldap_search_s(ld,base,scope,filter,attrs,0,result)
```

Directory requests

Network

LDAP V3 Client

z/OS

Application

z/OS Security Server LDAP Server

DB2

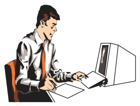
TDBM

cn=John James,o=IBM,c=US
mail=jjames@us.ibm.com

LDAP Usage - Authentication

- Bind identity is RACF userid
  - For access to RACF information
  - For access to DB2 information where ACLs use RACF identities
- Bind identity is Distinguished Name
  - For access to DB2 information
  - Password Encryption available in z/OS LDAP Server

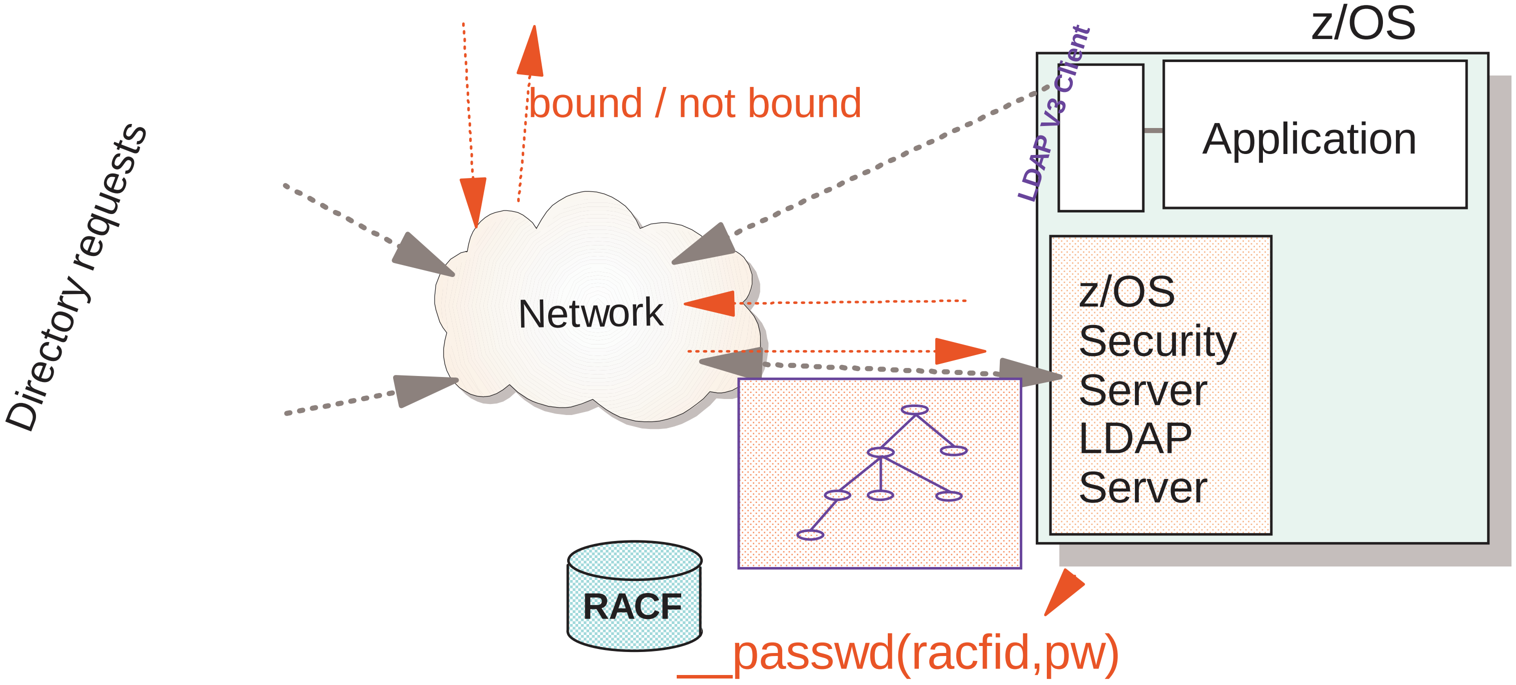
Customer Scenario
User Authentication



Web-enabled application

Enter userid: kareng
Enter password: ******

dn="racfid=kareng,profiletype=user,cn=plex1,o=IBM,c=US"
pw = password
ldap_bind_s(ld,host,port,dn,pw)



z/OS

LDAP V3 Client

Application

bound / not bound

Directory requests

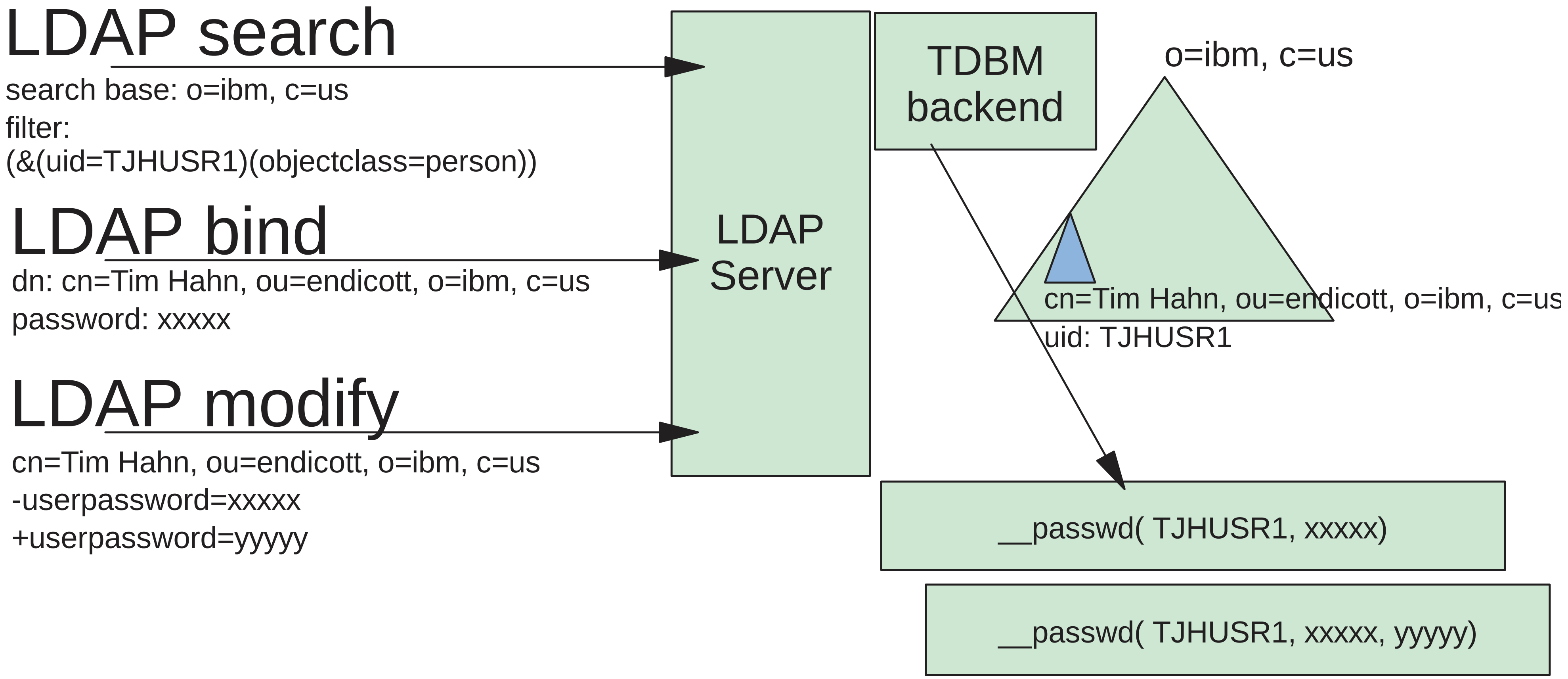
Network

z/OS Security Server LDAP Server

RACF

__passwd(racfid,pw)

Native Authentication



LDAP search

search base: o=ibm, c=us

filter:
(&(uid=TJHUSR1)(objectclass=person))

LDAP bind

dn: cn=Tim Hahn, ou=endicott, o=ibm, c=us

password: xxxxx

LDAP modify

cn=Tim Hahn, ou=endicott, o=ibm, c=us

-userpassword=xxxxx

+userpassword=yyyyy

LDAP Server

TDBM backend

o=ibm, c=us

cn=Tim Hahn, ou=endicott, o=ibm, c=us

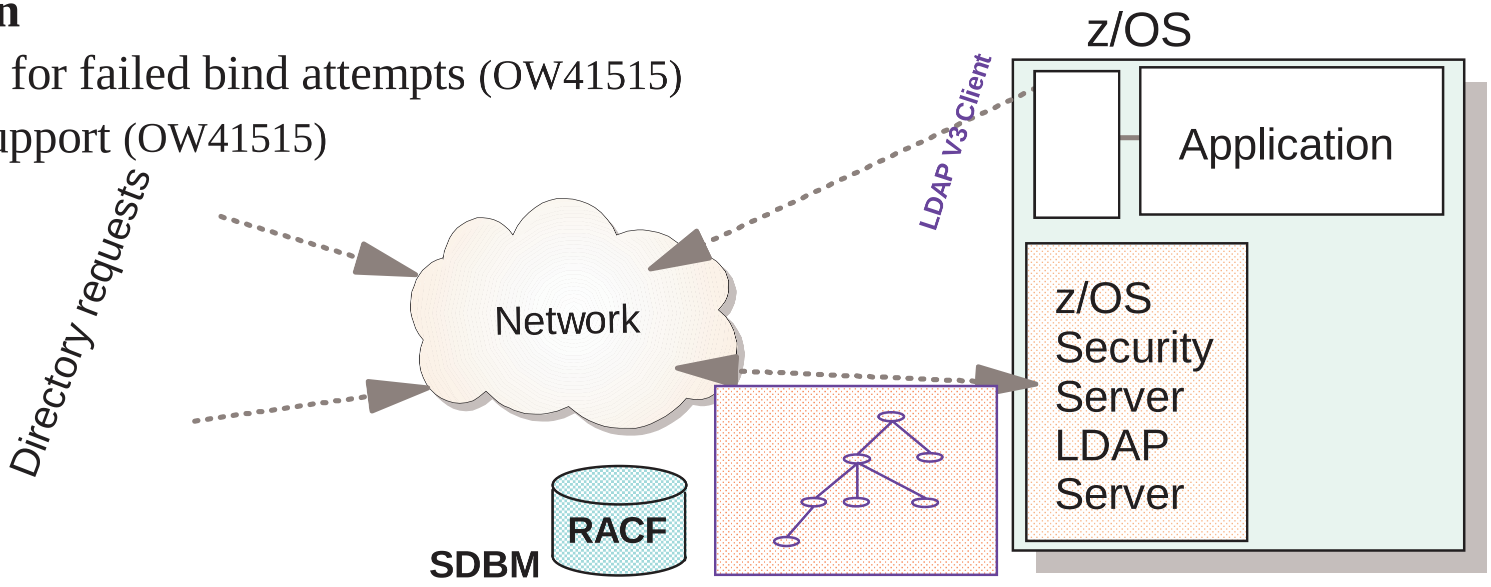
uid: TJHUSR1

__passwd(TJHUSR1, xxxxx)

__passwd(TJHUSR1, xxxxx, yyyyy)

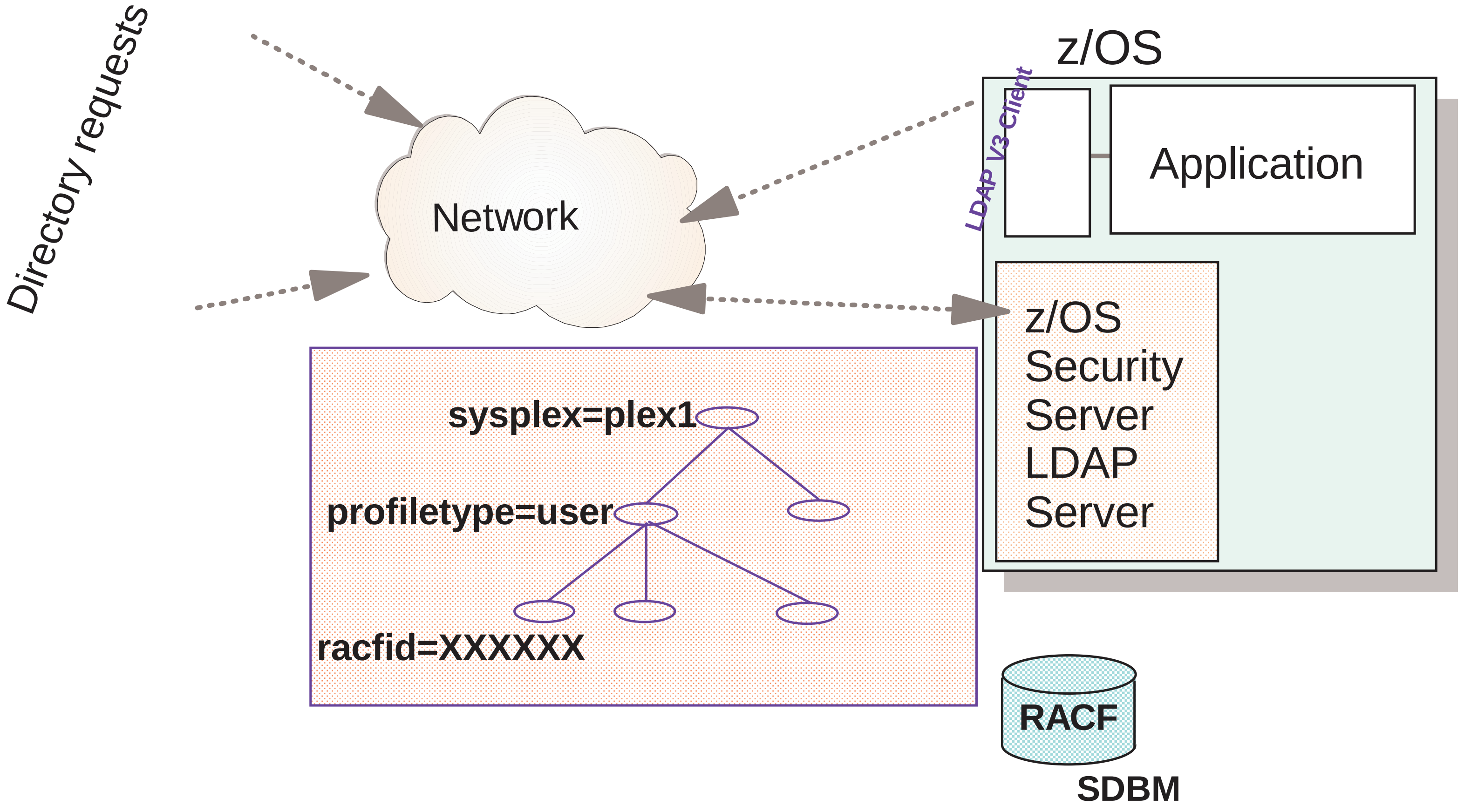
LDAP Usage - Access to RACF Information

- ➤ **User and Group Profile access and update**
- ➤ **Add or Delete Users and/or Groups**
  - ➤ ADDUSER (AU) and DELUSER (DU) Commands
  - ➤ ADDGROUP (AG) and DELGROUP (DG) Commands
- ➤ **Modify and Retrieve Information on Users and/or Groups**
  - ➤ LISTUSER (LU) and ALTUSER (ALU) Commands
  - ➤ LISTGRP (LG) and ALTGROUP (ALG) Commands
- ➤ **Supports LDAP Binds (authentication to LDAP Server) using RACF Password Verification**
  - ➤ Reason code & text for failed bind attempts (OW41515)
  - ➤ Password change support (OW41515)



RACF Namespace Entries

- ➤ Top 3 Entries in Hierarchy are Reserved (Read-Only)
- ➤ with R10, sysplex is no longer required keyword in top DN



How to Use LDAP's RACF Support

- If suffix(Top DN) for RACF access is set to

  `cn=plex1,o=IBM,c=US`

  - USER profiles are found under:

    `profiletype=USER, cn=plex1, o=IBM, c=US`

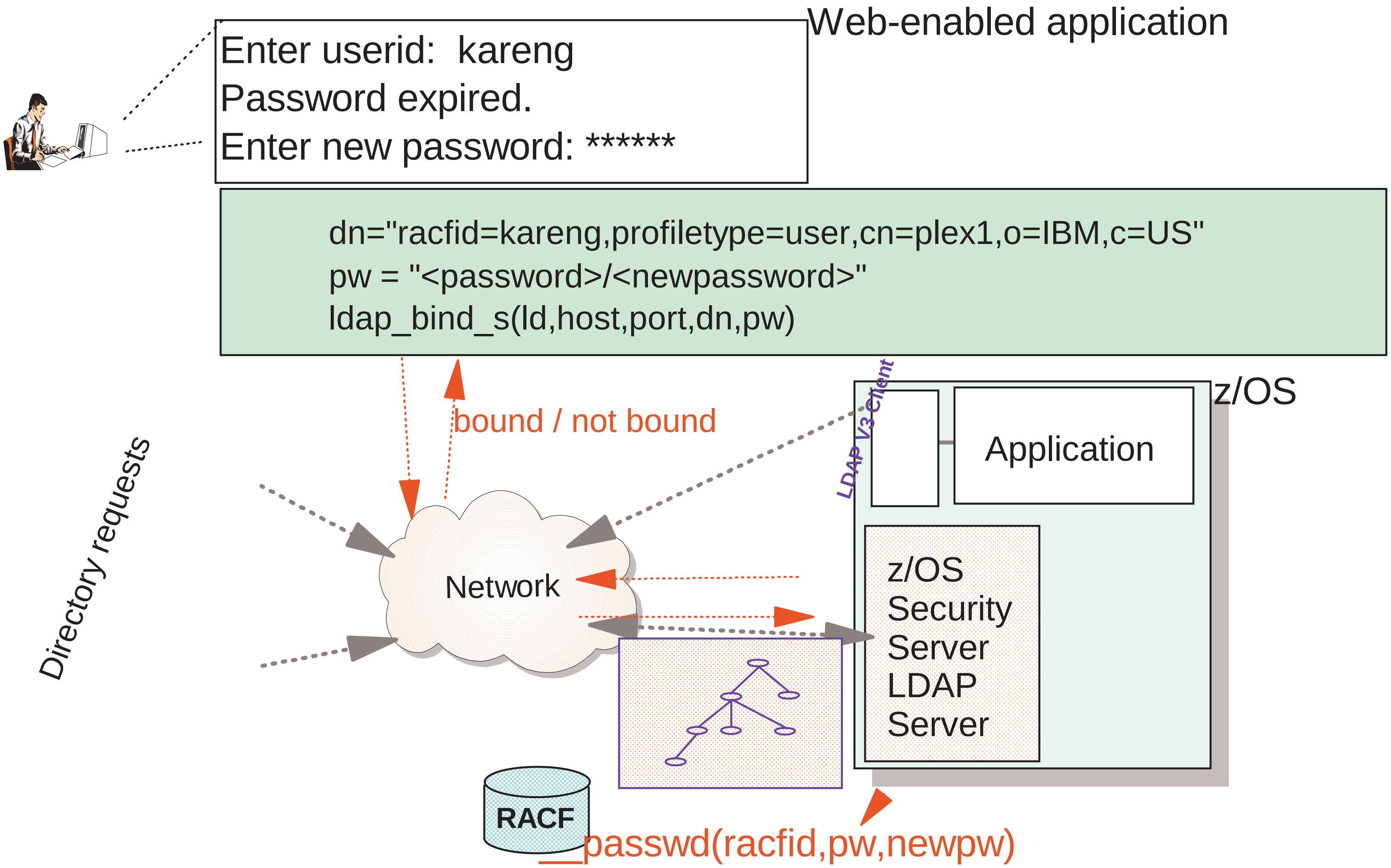
  - GROUP profiles are found under:

    `profiletype=GROUP, cn=plex1, o=IBM, c=US`

How to Use LDAP's RACF Support (cont):

- ➤ A simple bind operation to userid which supplies a password is verified using the Security Server
  - ➤ A simple bind supplying a password in the form:
    password/newpassword
    changes the password via Security Server (APAR OW41515)
- ➤ A sub-tree search operation can be performed (but only to get the names of users and/or groups)
- ➤ A base search (get entry) can be performed for USER and GROUP profiles and the profile information is returned in LDAP format (type = value)

Customer Scenario with password change

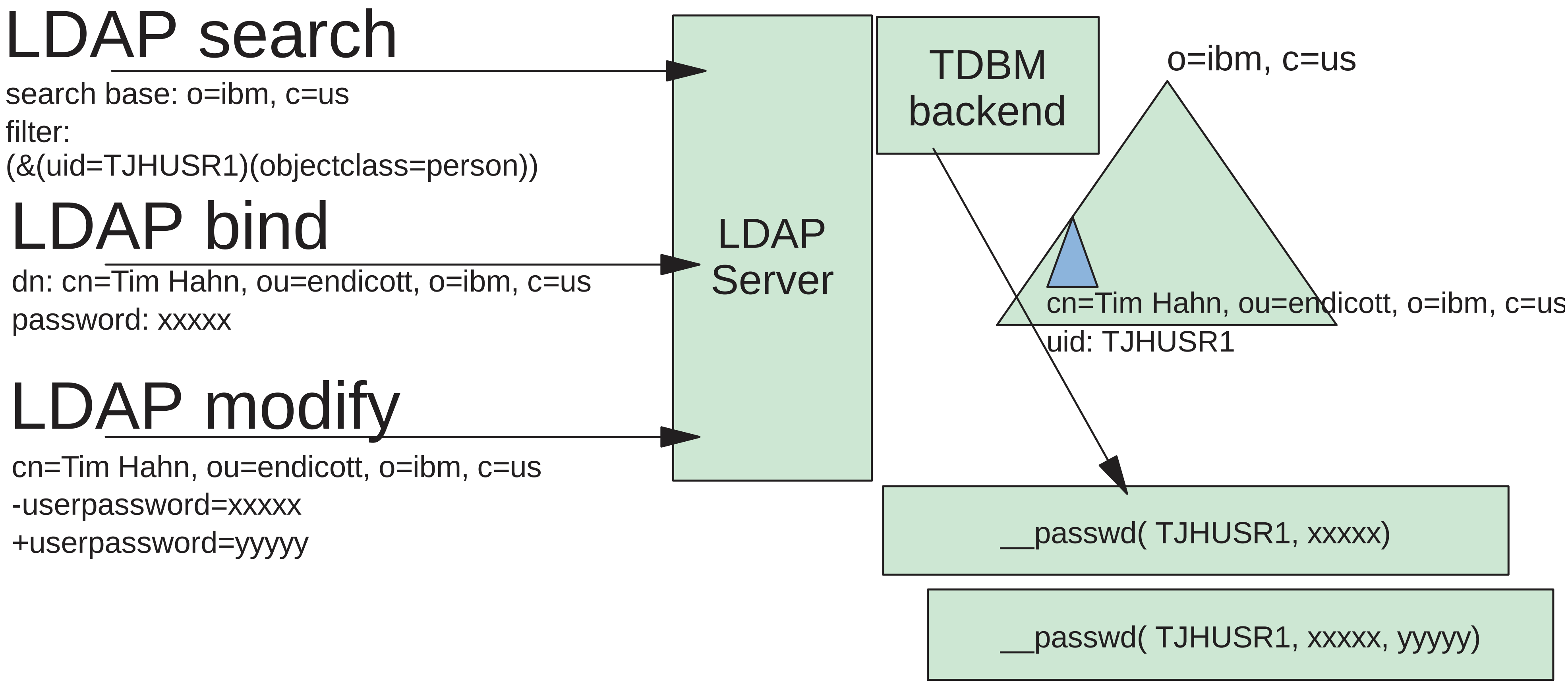


Enter userid: kareng
Password expired.
Enter new password: ******

```
dn="racfid=kareng,profiletype=user,cn=plex1,o=IBM,c=US"
pw = "<password>/<newpassword>"
ldap_bind_s(ld,host,port,dn,pw)
```

Copyright IBM Corp., 1999

Native Authentication



LDAP search

search base: o=ibm, c=us

filter:
(&(uid=TJHUSR1)(objectclass=person))

LDAP bind

dn: cn=Tim Hahn, ou=endicott, o=ibm, c=us

password: xxxxx

LDAP modify

cn=Tim Hahn, ou=endicott, o=ibm, c=us

-userpassword=xxxxx

+userpassword=yyyyy

LDAP Server

TDBM backend

o=ibm, c=us

cn=Tim Hahn, ou=endicott, o=ibm, c=us

uid: TJHUSR1

__passwd(TJHUSR1, xxxxx)

__passwd(TJHUSR1, xxxxx, yyyyy)

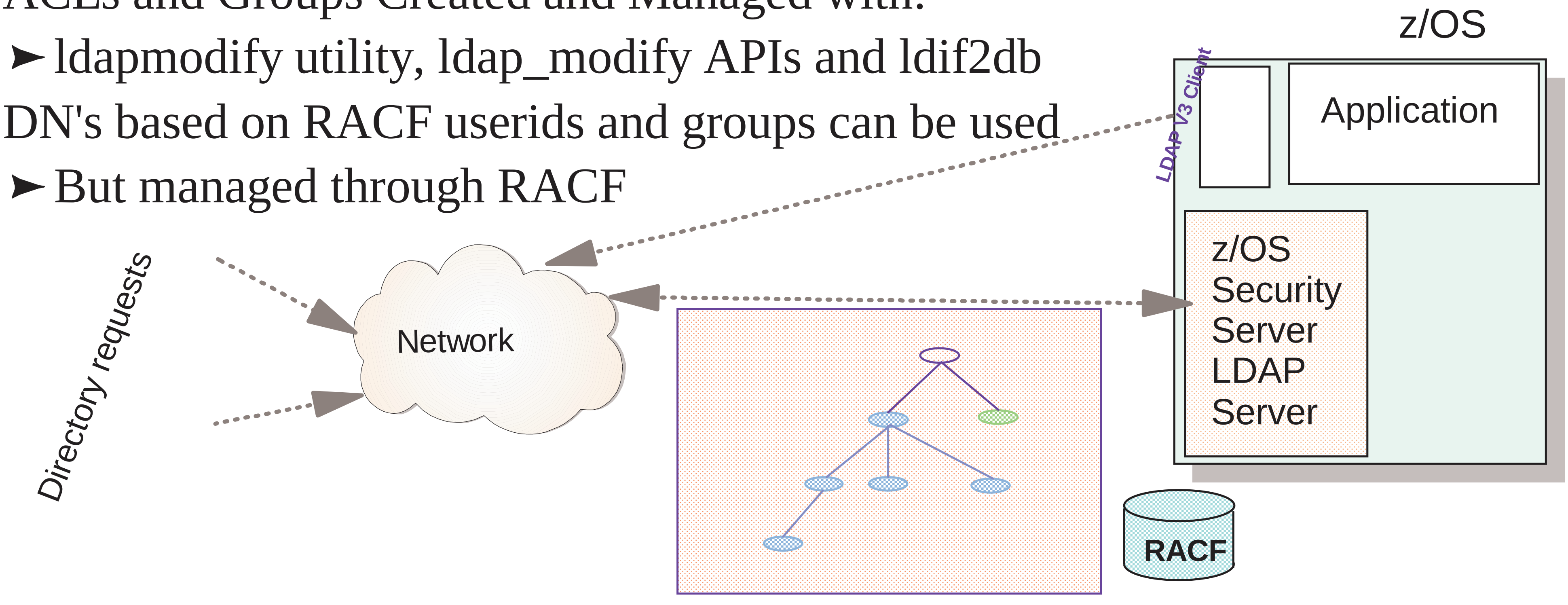
RACF Example Using LDAP Command

```
ldapsearch -h 127.0.0.1 -p 636 -D bindDN -w passwd
  -b "racfid=kareng,profiletype=user,cn=plex1,o=IBM,c=US"
  "objectclass=*"
```

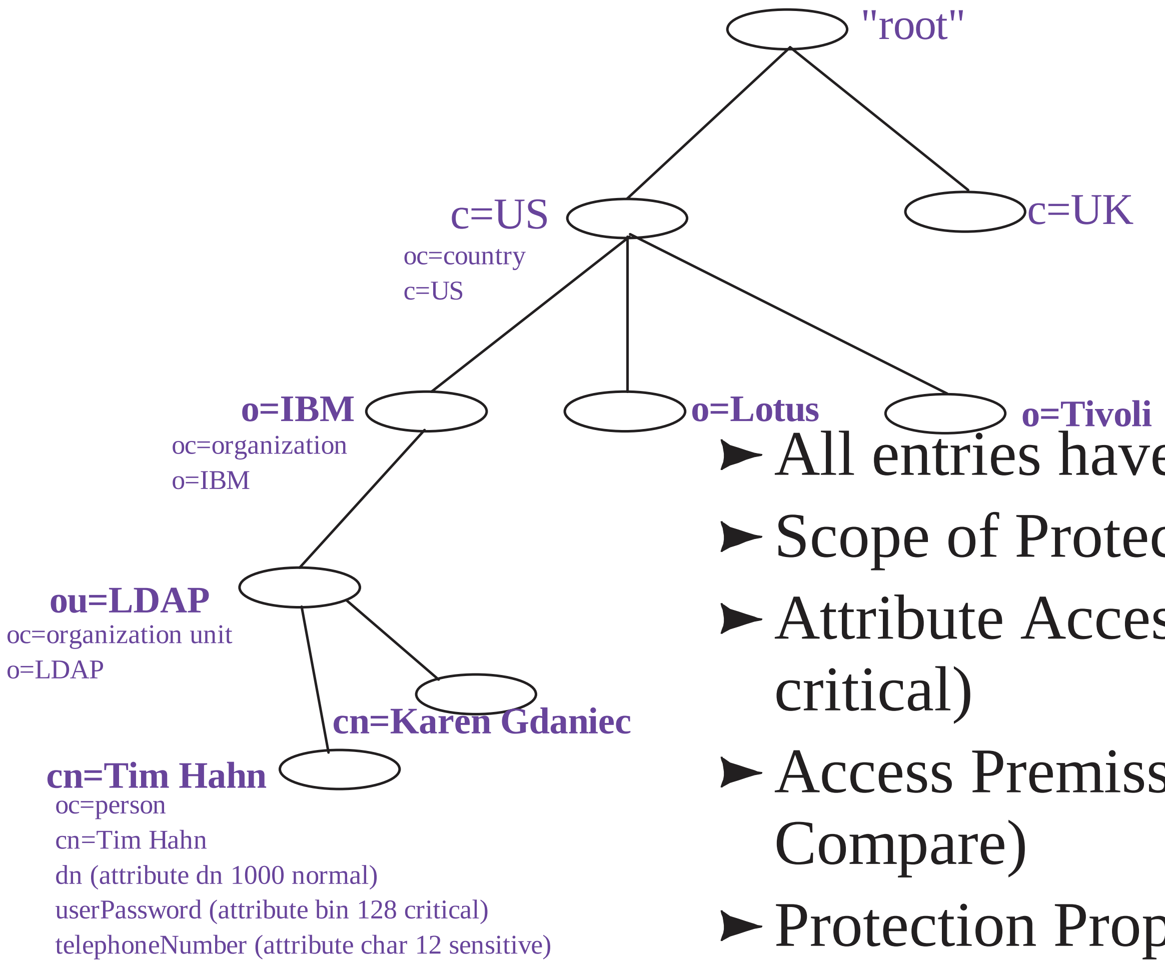
```
racfid=kareng,profiletype=USER,cn=plex1,o=IBM,c=US
objectclass=racfUser
...
racfid=kareng
racfauthorizationdate=99.134
racfdefaultgroup=racfid=GOODGUYS,profiletype=GROUP,cn=plex1,o=IBM,c=US
racfattributes =SPECIAL
racfrevokedate=NONE
safaccountnumber=75932
racfomvsuid=0
racfomvshome=/u/kareng
....
```

LDAP Usage - Access Control to Directory Information

- ACLs = Access Control Lists
- Control Access to Portions of the Directory or Specific Directory Entries
- Each Directory Entry has DN, Set of Attributes with Values
- ACLs and Groups Created and Managed with:
  - ldapmodify utility, ldap_modify APIs and ldif2db
- DN's based on RACF userids and groups can be used
  - But managed through RACF



LDAP Directory Content



"root"

c=US

oc=country
c=US

c=UK

o=IBM

oc=organization
o=IBM

o=Lotus

o=Tivoli

ou=LDAP

oc=organization unit
o=LDAP

cn=Karen Gdaniec

cn=Tim Hahn

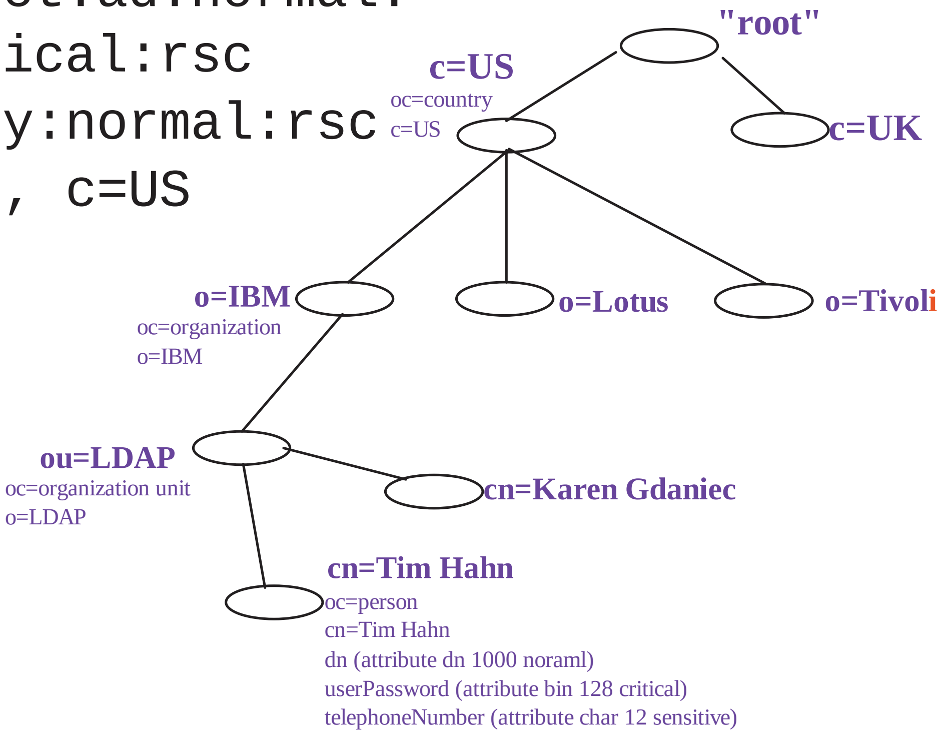
oc=person
cn=Tim Hahn
dn (attribute dn 1000 normal)
userPassword (attribute bin 128 critical)
telephoneNumber (attribute char 12 sensitive)

- All entries have attributes (and values)
- Scope of Protection (access-id or group)
- Attribute Access Class (normal, sensitive, critical)
- Access Premissions (Read, Write, Search, Compare)
- Protection Propagation (propagating or overriding)
- Owner - user or group

ACL Example

- Protection for: **ou=LDAP, o=IBM, c=US**

```
aclPropagate: TRUE
aclEntry: group:cn=LDAPfolks, o=IBM,
 c=US:normal:rcs:sensitive:rsc
aclEntry: access-id:cn=Karen Gdaniec,
 ou=LDAP, o=IBM,c=US:object:ad:normal:
 rwsc:sensitive:rwsc:critical:rsc
aclEntry: group:cn=Anybody:normal:rsc
aclSource: ou=LDAP, o=IBM, c=US
```



Creating ACL with ldif2db

use LDIF form:

```
dn: cn=Karen Gdaniec, ou=LDAP, o=IBM, c=US
objectclass: person
cn: Karen Gdaniec
sn: Gdaniec
aclEntry: access-id:cn=Tim Hahn, ou=LDAP, o=IBM,
 c=US:normal:rwsc:sensitive:wrsc:critical:rsc
aclEntry: access-id:racfid=G1USER,
 profiletype=user,cn=plex1,o=IBM,c=US:normal:rsc
aclEntry: group:cn=SecurityAdmins, ou=Security,
 o=IBM,c=US:normal:rwsc:sensitive:rwsc:
 critical:rwsc
aclPropagate: TRUE
ownerPropagate: TRUE
entryOwner: access-id:cn=Karen Gdaniec,
 ou=LDAP, o=IBM, c=US
```

Access Control and Security Server Access

- Applies to entries stored by the LDAP Server into the DB2 tablese the server manages (same model for RDBM and TDBM)
- DN containing RACF id (userid or group name) can be used in ACL
- Allows Security Server authentication to be extended to the LDAP entries stored in DB2
- Example:

```
dn: cn=John James, o=ABC Company, c=US
aclentry: access-id:racfid=G1USER,profiletype=user,
 cn=sysplex1,o=ABC Company, c=US
```

For More Information

- LDAP RFCs
  - http://sunsite.auc.dk/RFC/rfc/rfc2251.html-rfc2256.html
- z/OS LDAP Documentation
  - SC24-5923-02 z/OS Security Server LDAP Server Administration and Usage Guide
    - http://publibz.boulder.ibm.com/epubs/pdf/glda1a10.pdf
  - SC24-5924-01 z/OS Security Server LDAP Client Application Development Guide and Reference
    - http://publibz.boulder.ibm.com/epubs/pdf/glda2a11.pdf