Directory Services on OS/390

Using the LDAP Server on OS/390

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "as-is" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environment do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly.

Users of this document should verify the applicable data for their specific environments. It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country or not yet announced by IBM. Such references or information should not be construed to mean that IBM intends to announce such IBM products, programming, or services.

Trademarks

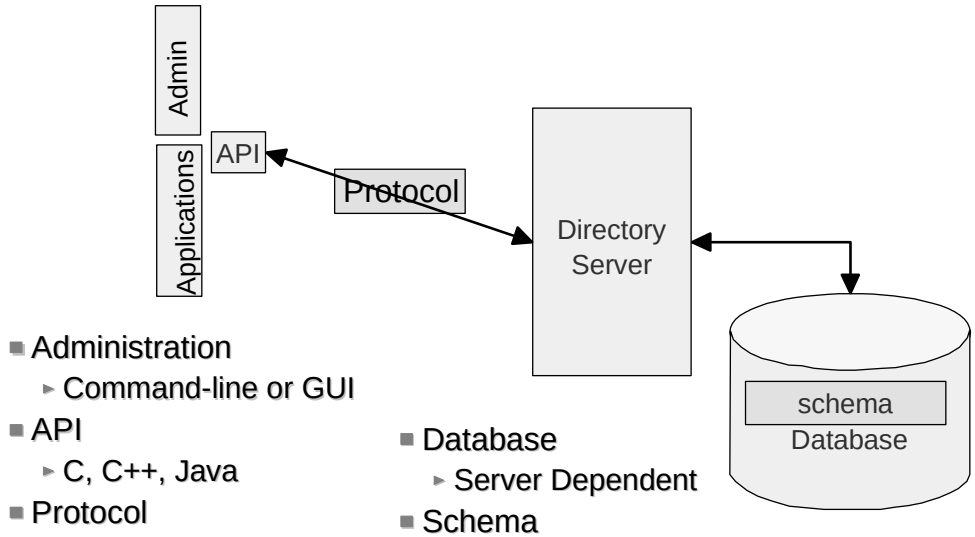
What are we going to talk about?

- Directory Services and LDAP
- Configuration of the OS/390 LDAP server
- LDAP services available on OS/390
- LDAP and RACF
- Authentication to the LDAP server
- SSL within the LDAP environment
- LDAP access control lists
- Password Encryption Support

Directory Services and LDAP

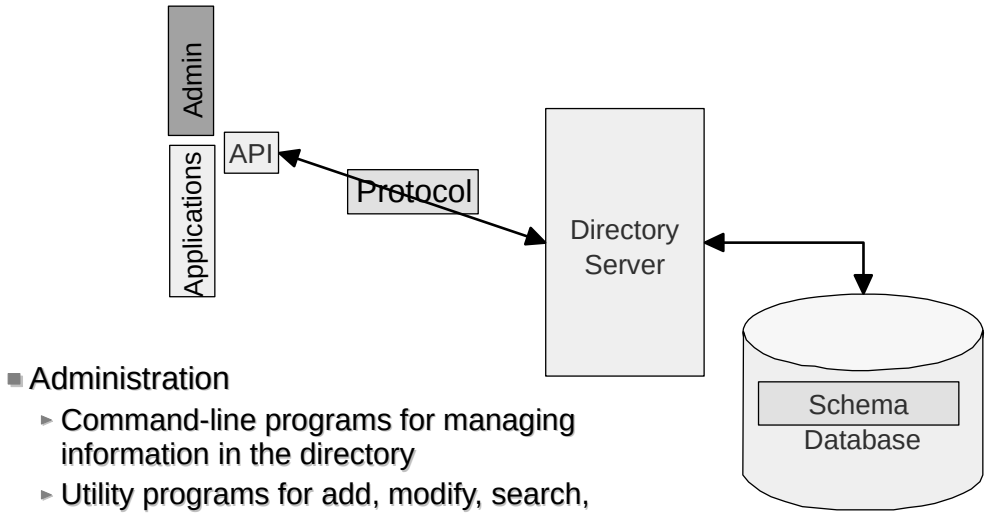
- LDAP - Lightweight Directory Acces Protocol
- Directory Server - a program that stores information in "directory format"
- Directory Service - a distributed set of Directory Servers which, together, give the illusion of a single Directory Server.
- Directory "format" is based on an X.500 data model:
  - Directory Service contains a hierarchy of entries
  - Each entry contains attributes
  - Each attribute contains 1 or more values
- The format of entries is defined by the Directory Schema.

Directory Services and LDAP



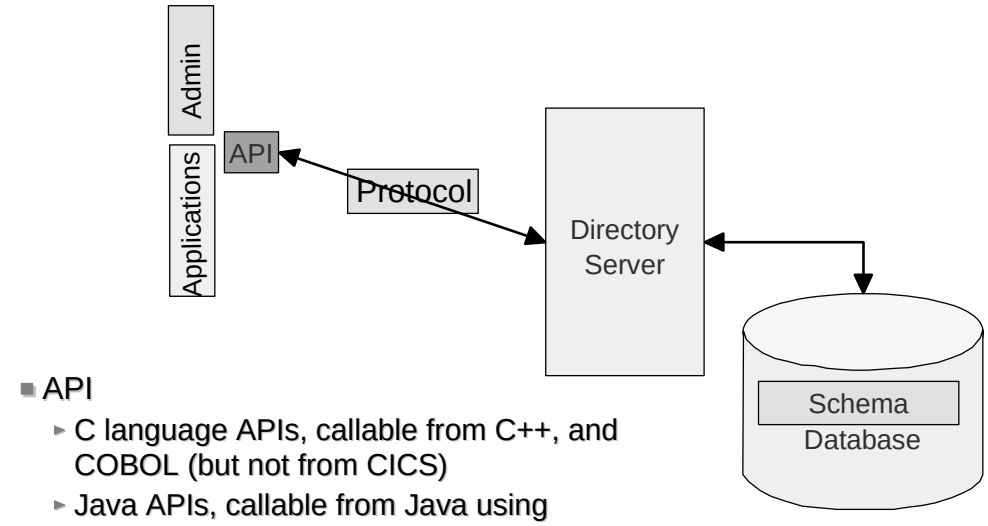
- Administration
  - Command-line or GUI
- API
  - C, C++, Java
- Protocol
  - LDAP
- Database
  - Server Dependent
- Schema
  - Database Dependent

LDAP Services on OS/390



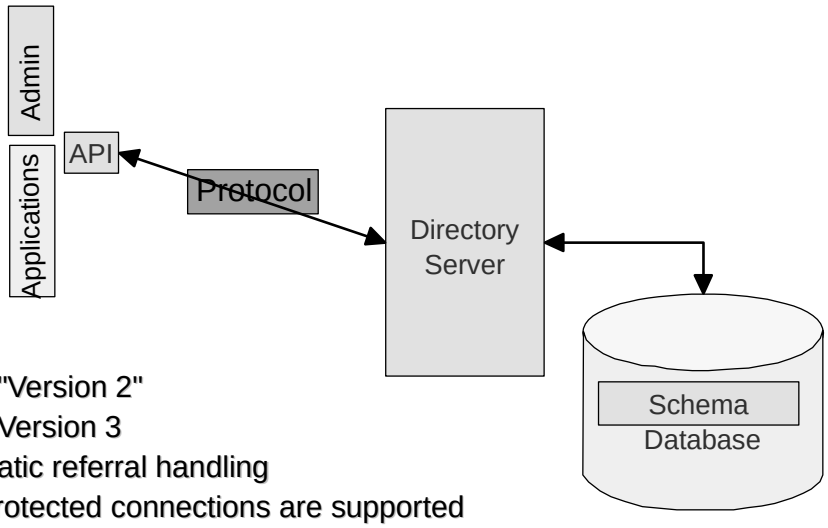
- Administration
  - Command-line programs for managing information in the directory
  - Utility programs for add, modify, search, delete of directory content

LDAP Services on OS/390



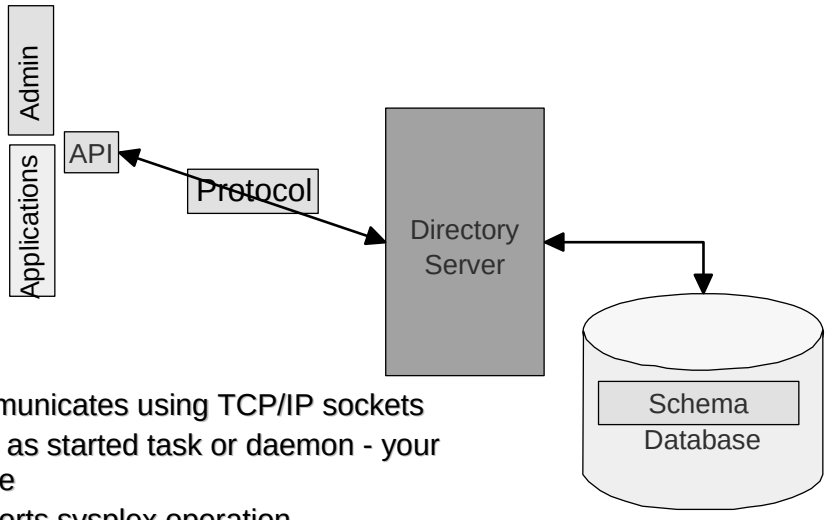
- API
  - C language APIs, callable from C++, and COBOL (but not from CICS)
  - Java APIs, callable from Java using JavaSoft's JNDI programming interface

LDAP Services on OS/390



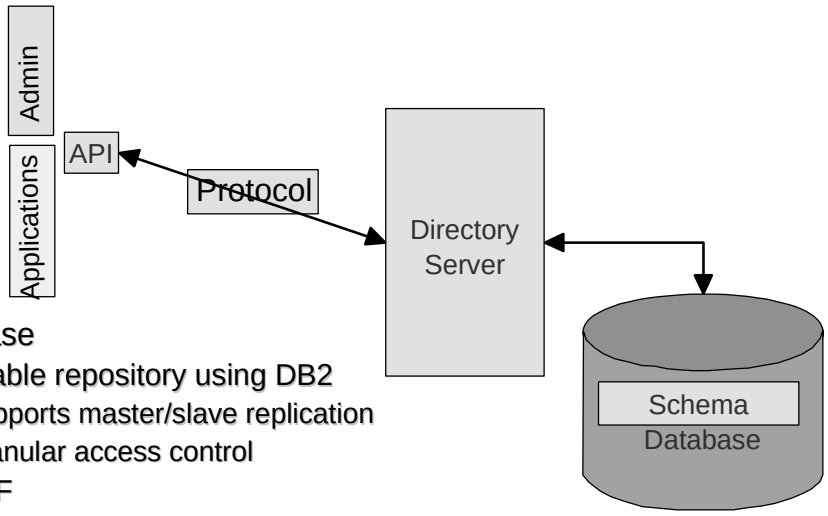
- Protocol
  - LDAP "Version 2"
  - LDAP Version 3
  - Automatic referral handling
  - SSL-protected connections are supported

LDAP Services on OS/390



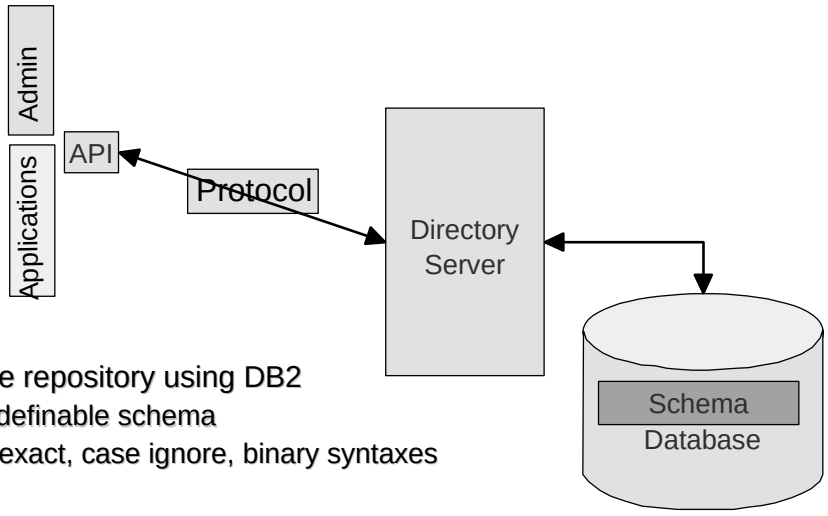
- Server
  - Communicates using TCP/IP sockets
  - Runs as started task or daemon - your choice
  - Supports sysplex operation

LDAP Services on OS/390



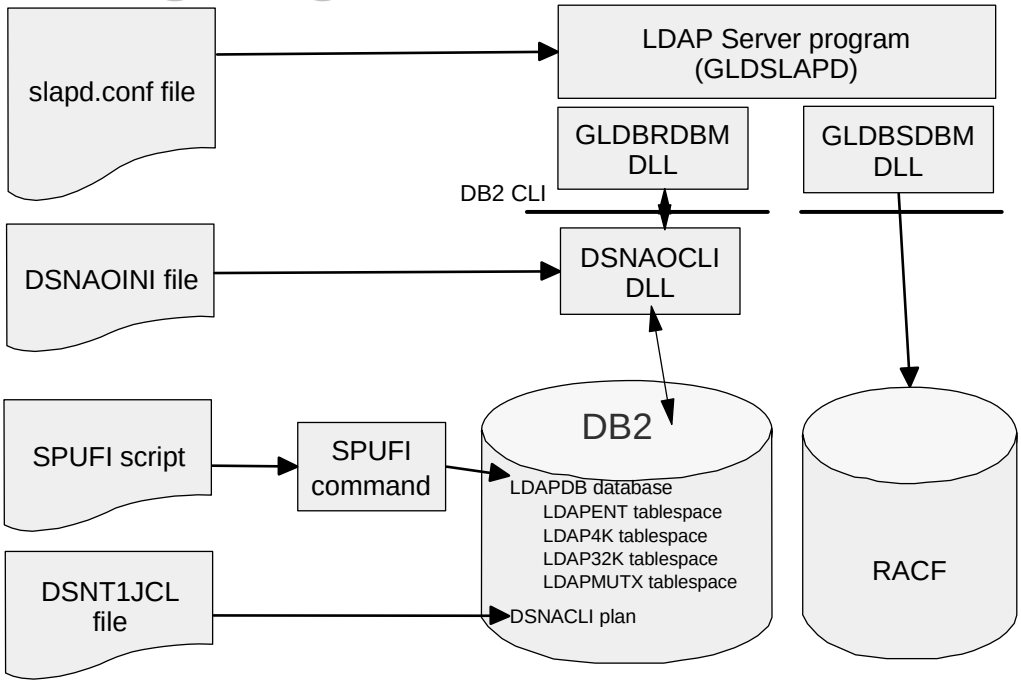
- Database
  - Scalable repository using DB2
    - supports master/slave replication
    - granular access control
  - RACF
    - add, modify, delete users and groups
    - bind (authenticate to RACF)

LDAP Services on OS/390

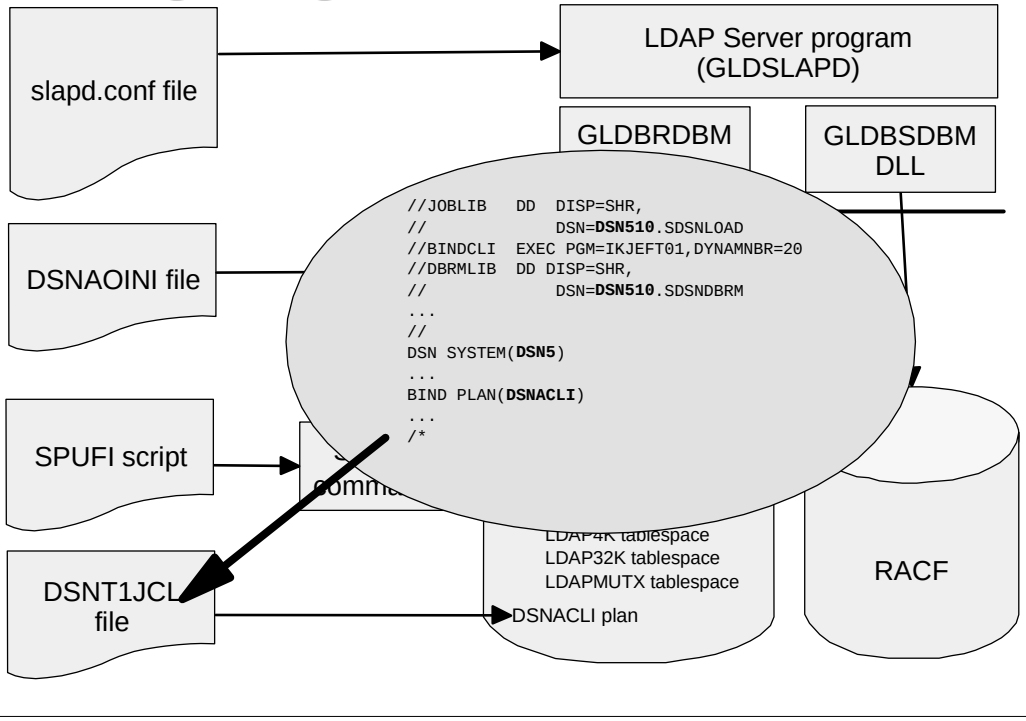


- Schema
  - Scalable repository using DB2
    - user-definable schema
    - case exact, case ignore, binary syntaxes
  - RACF
    - fixed schema based on RACF
    - most attributes are case-insensitive strings

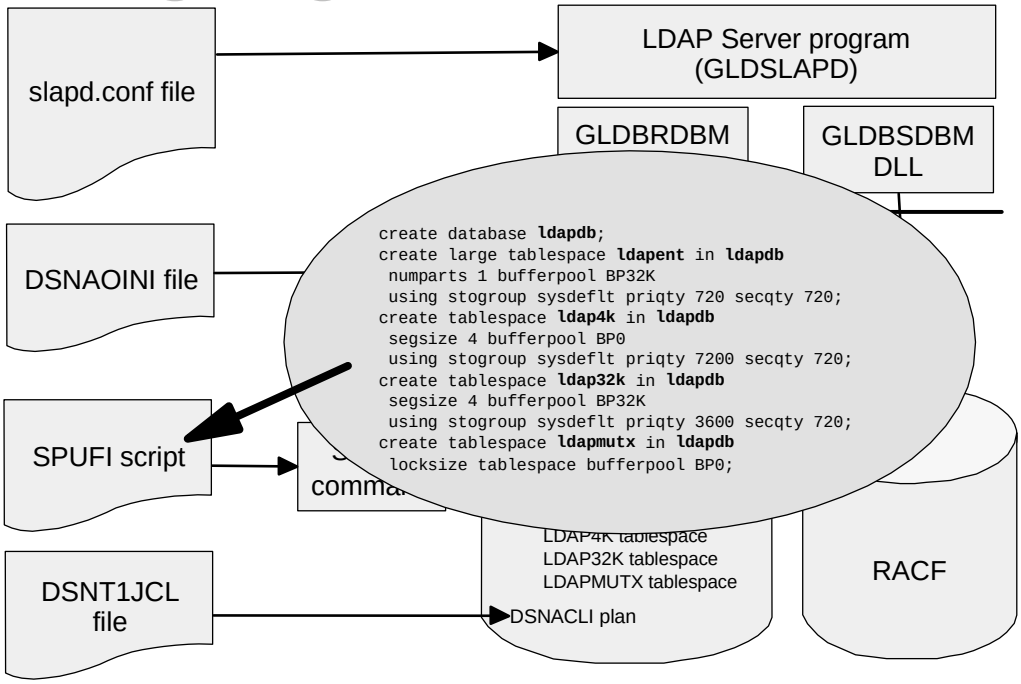
Configuring the LDAP Server



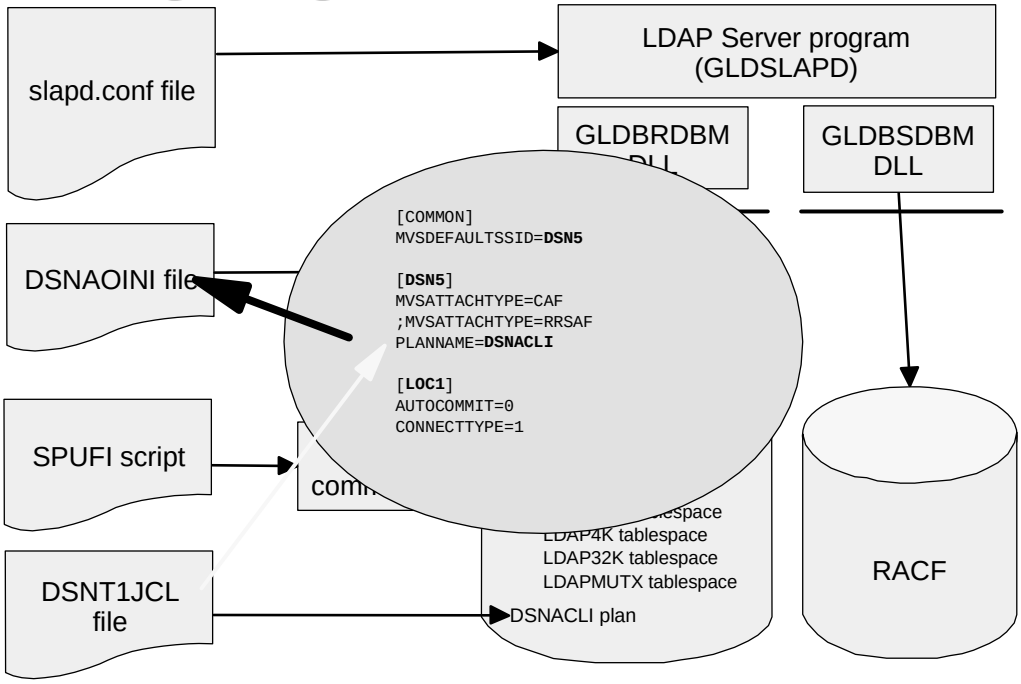
Configuring the LDAP Server



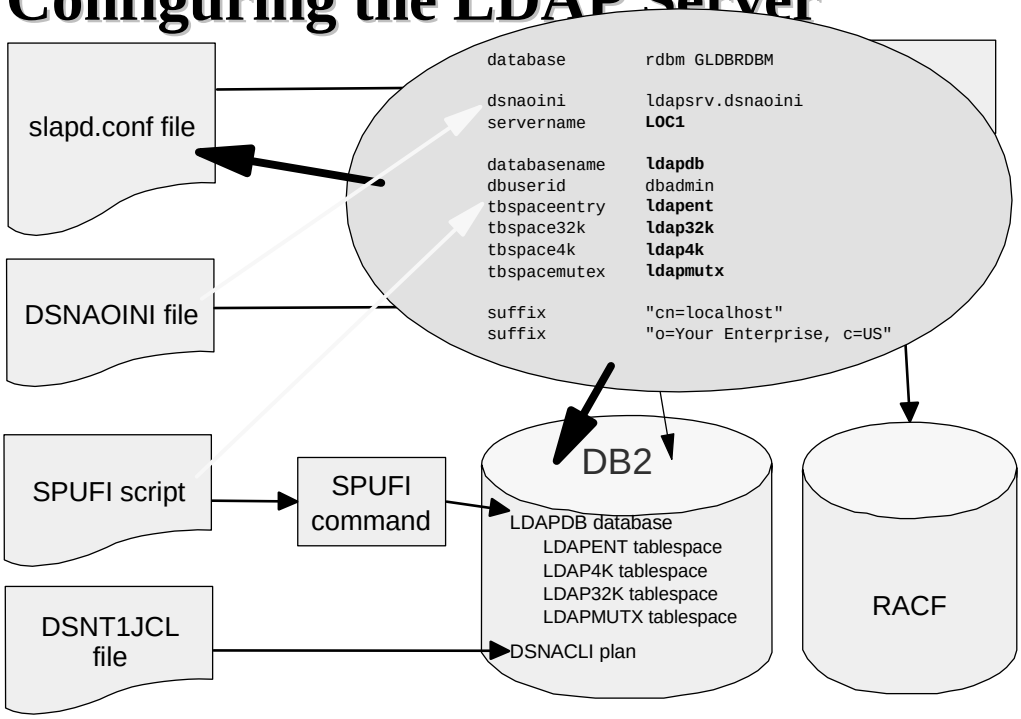
Configuring the LDAP Server



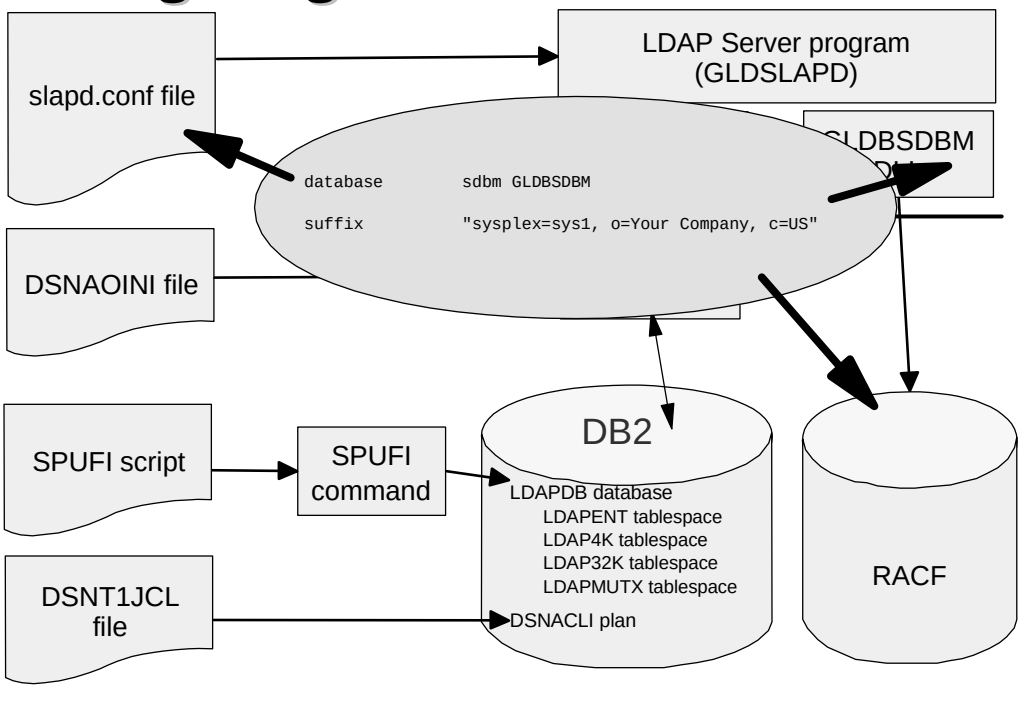
Configuring the LDAP Serve



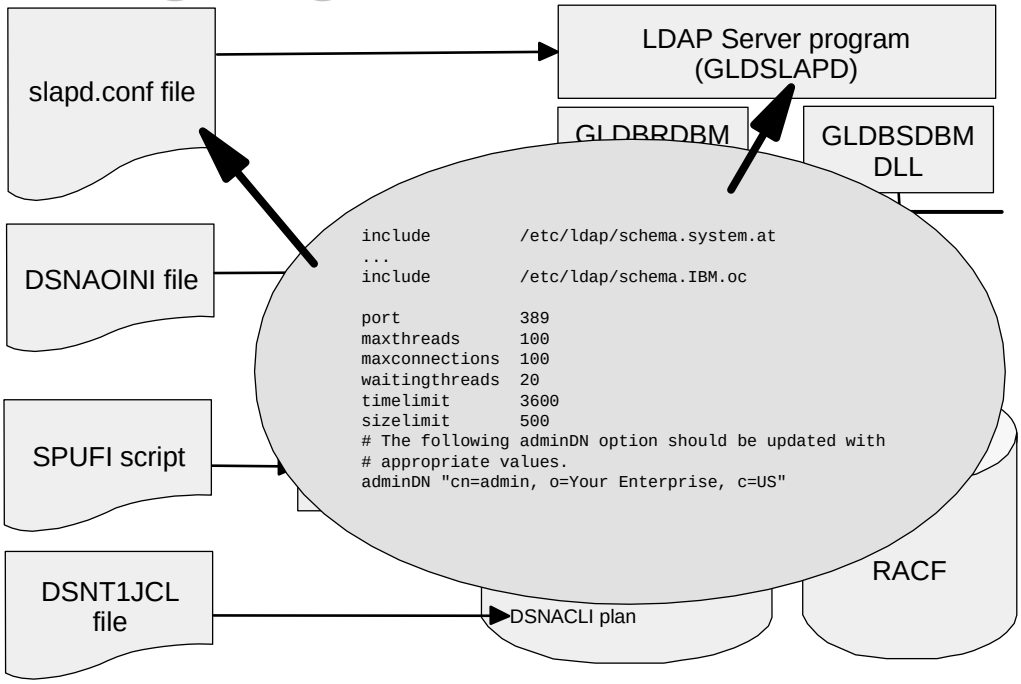
Configuring the LDAP Server



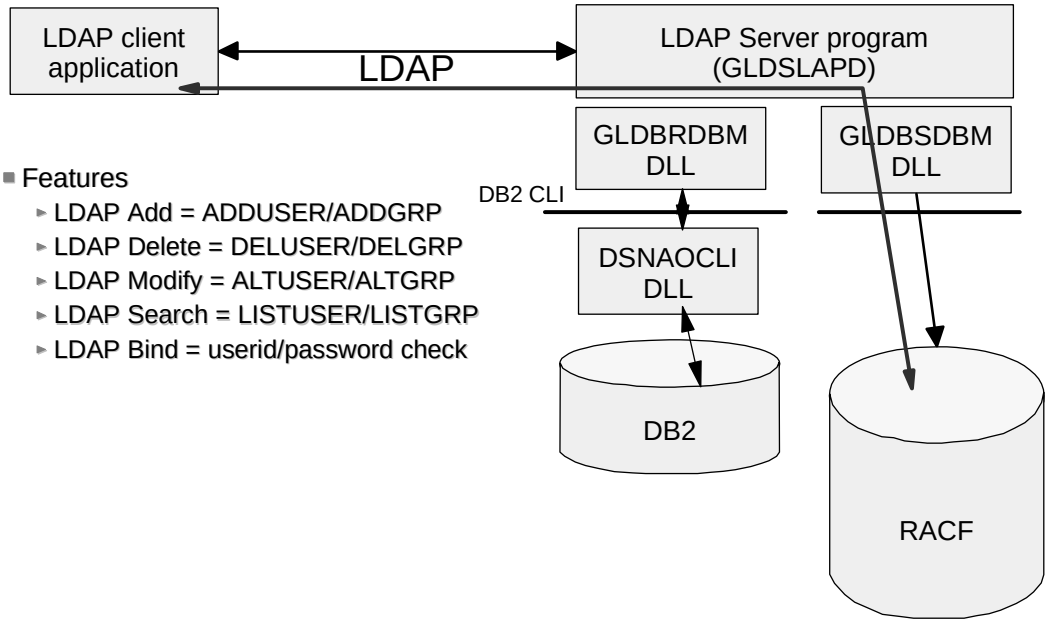
Configuring the LDAP Server



Configuring the LDAP Server

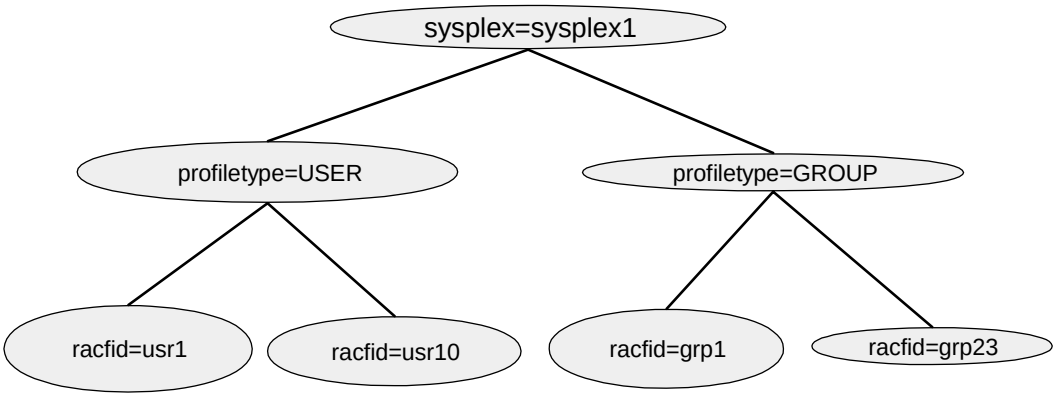


LDAP and RACF



- Features
  - LDAP Add = ADDUSER/ADDGRP
  - LDAP Delete = DELUSER/DELGRP
  - LDAP Modify = ALTUSER/ALTGRP
  - LDAP Search = LISTUSER/LISTGRP
  - LDAP Bind = userid/password check

LDAP - RACF Name-space



How to Use LDAP's RACF Support

- If suffix(Top DN) for RACF access is set to "sysplex=plex1,o=IBM,c=US", then
  - USER profiles are found under:
    - racfid=<userid>, profiletype=USER, sysplex=plex1, o=IBM, c=US
  - GROUP profiles are found under:
    - racfid=<groupid>, profiletype=GROUP, sysplex=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
  - RACF password can be changed if bind password is sent as "oldpw/newpw"
- 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)

RACF Examples Using LDAP Commands

ldapmodify -h 127.0.0.1 -p 636 -D bindDN -w passwd -f mod.file

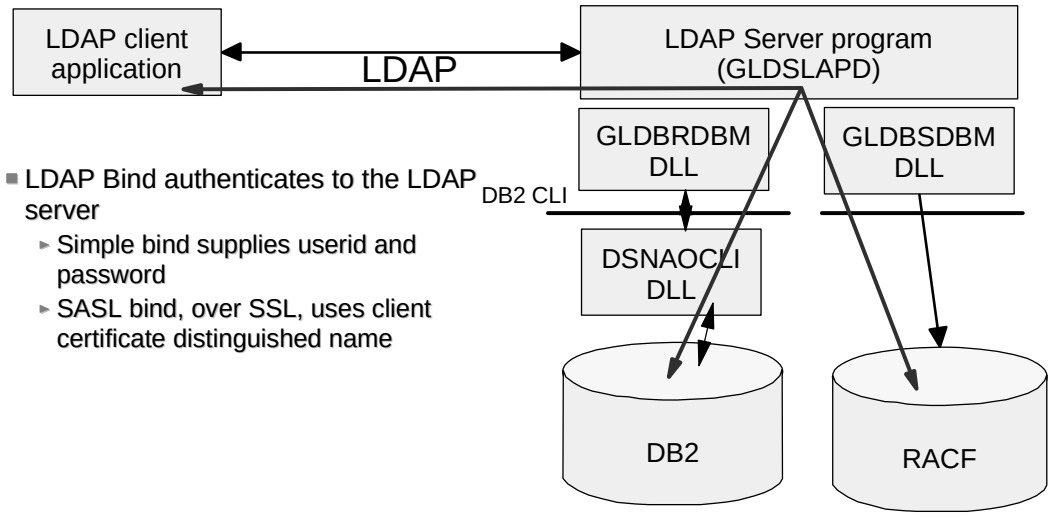
```
dn: racfid=tjh,profiletype=user,sysplex=plex1
changetype: modify
racfOmvsHome: /u/tjh
racfBuilding: 256
SAFDefaultCommand: LOGOFF
```

RACF Examples Using LDAP Commands

**ldapsearch -h 127.0.0.1 -p 636 -D bindDN -w passwd **
-b "racfid=tjh,profiletype=user,sysplex=plex1" "objectclass=*"

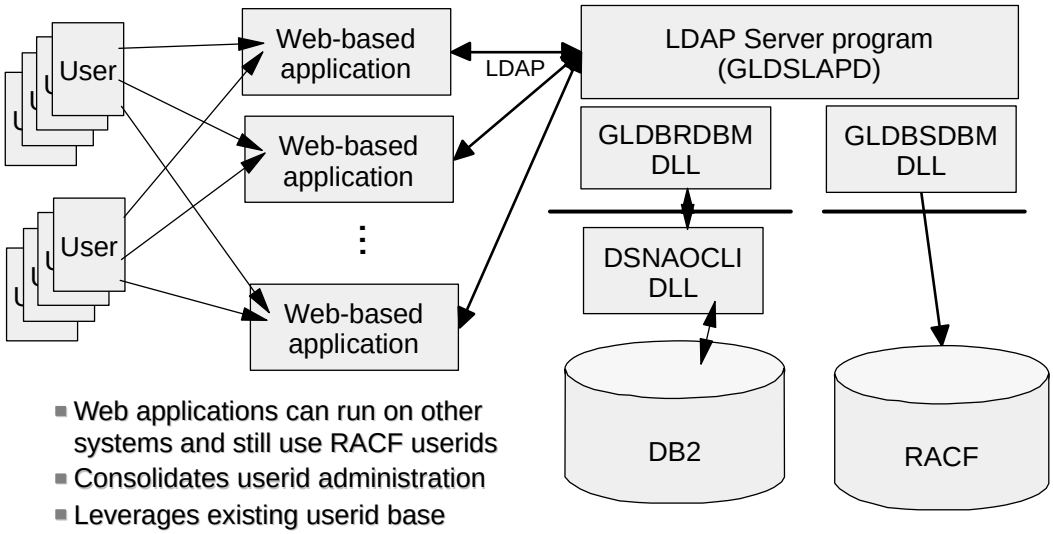
```
racfid=tjh,profiletype=USER,sysplex=plex1
objectclass=racfUser
...
racfid=kareng
racfauthorizationdate=99.134
racfdefaultgroup=racfid=GOODGUYS,profiletype=GROUP,sysplex=plex1
racfattributes =SPECIAL
racfrevokedate=NONE
safaccountnumber=75932
racfomvsuid=0
racfomvshome=/u/tjh
....
```

Authentication to the LDAP server



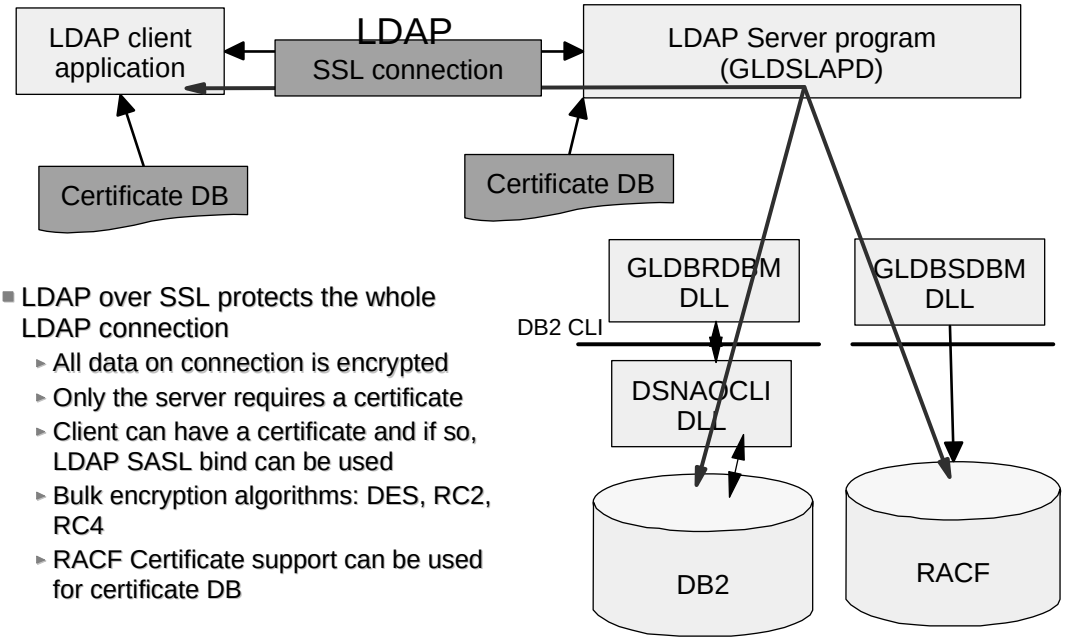
- LDAP Bind authenticates to the LDAP server
  - Simple bind supplies userid and password
  - SASL bind, over SSL, uses client certificate distinguished name

Authentication to the LDAP Server



- Web applications can run on other systems and still use RACF userids
- Consolidates userid administration
- Leverages existing userid base

SSL within the LDAP environment



- LDAP over SSL protects the whole LDAP connection
  - All data on connection is encrypted
  - Only the server requires a certificate
  - Client can have a certificate and if so, LDAP SASL bind can be used
  - Bulk encryption algorithms: DES, RC2, RC4
  - RACF Certificate support can be used for certificate DB

Certificate Bind Support

- Allows applications to use certificates generated by a CA
- Verifies both client and server are who they say they are
- Uses SystemSSL functions(part of OCSF)
- Client application indicates use of a certificate on the bind operation by specifying bind method as ’external’
- Bind DN taken from certificate

Using Certificate Bind

- Prepare server and client for SSL connections
  - Certificates in key databases
  - Mark certificates or CA’s as trusted
  - Add to LDAP Server configuration file: sslAuth serverClientAuth
- Search utility can be called using the certificate, e.g.:

```
ldapsearch -V 3 -S external -Z -K <key.db> \
-P <key.db-pw> -b "o=IBM_POK,c=US" \
"objectclass=*"
```

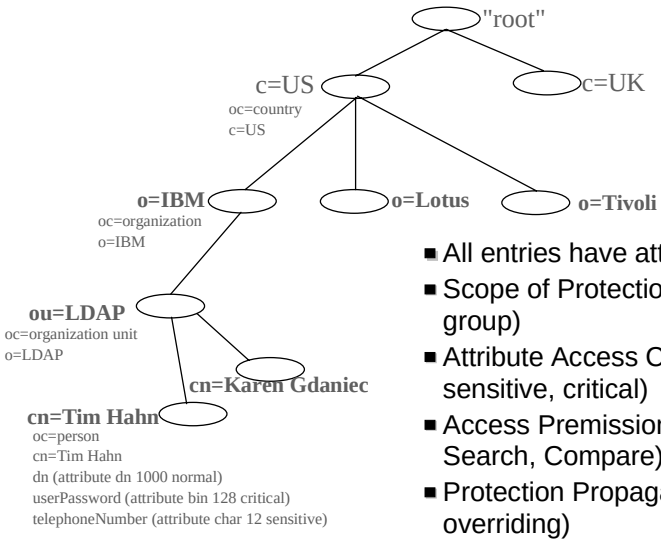
Using Certificate Bind(cont.)

- What happens:
  - SSL handshake occurs when the ssl init API is called
  - Authentication occurs during the handshake and succeeds only if authentication succeeds
  - Bind method is specified as "EXTERNAL" on the bind API call
  - Certificate from handshake is used on bind
  - Bind occurs using DN in the certificate
  - IBM servers gather group membership information based on DN naming context

Protecting the Information in the LDAP Server

- 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:
  - ldapcp
  - ldapmodify
  - ldif2db

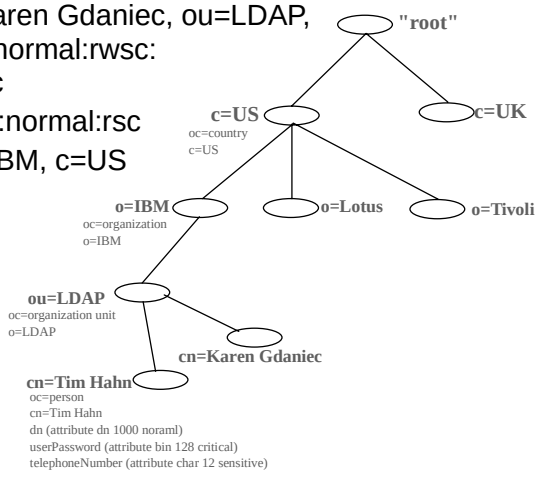
LDAP Directory Content



- 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=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=Anybody:normal:rsc
  - **aclSource:** ou=LDAP, o=IBM, c=US



Access Control and Security Server Access

- Applies to entries stored by the LDAP Server into DB2
- DN containing RACF id can be used in ACL
- Allows Security Server authentication to be extended to the LDAP entries stored in DB2
- Example:
  - dn: John James,o=ABC Company,c=US
  - access-id: racfid=G1USER,profiletype=user, sysplex=sysplex1,o=ABC Company, c=US

Creating ACL with ldif2db

Create ACL Entries for: cn=Karen Gdaniec, ou=LDAP, o=IBM, c=US

```
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,profiltype=user,sysplex=plex1:
    normal:rsc
aclEntry: group:cn=SecurityAdmins, ou=Security, o=IBM,
    c=US:normal:rwsc:sensitive:rwsc:critical:rwsc
aclPropagate:  TRUE
ownerPropagate:  TRUE
```

Password Encryption Support

- For userpassword attribute
- Uses OCSF for encryption methods
- Choice of methods
  - no encryption
  - SHA
  - crypt
  - MD5
  - DES
- Use **pwencryption** configuration file option
- Use db2pwden utility to encrypt existing userpassword attributes

The Enterprise Namespace