POWERED BY HP...
HP e3000

LDAP C-SDK/iX on MPE/iX

LDAP

Lightweight Directory Access Protocol

HEWLETT® PACKARD

Status of LDAP C-SDK/iX

- LDAP C-SDK/iX was ported to MPE/iX from the open source of Netscape Directory SDK Version 3 for C without SSL authentication.
- Compliant to the IETF LDAPv3 standard.
- Downloadable from Jazz for MPE/iX 6.0 since December, 1999.
- Released in MPE/iX 6.5.
- Bundled in OS with standard support.

What is LDAP?

- Lightweight Directory Access Protocol to LDAP directories.
- LDAP server manages network directories and processes access requests.
- LDAP client sends access requests through standard protocol and API.

Why LDAP?

- Open standard protocol offers directory connectivity across heterogeneous platforms.
- Generic API makes application transportable.
- Directory repository sharable, replicable and independent of vendors.

Features of LDAP Services

- Via standard protocol and API, heterogeneous clients interoperate with heterogeneous servers.
- Runs over TCP/IP.
- Object-oriented hierarchical directory structure.
- Data replication provides reliability and high availability advantages.
- Flexible querries.

What's In Directories?

Descriptive information of:

- Person, addresses, email, organizations, job title, phone#
- Users, groups, accounts, passwords, ACL
- URLs, pointers to photos, documents & objects
- Network resources: servers, printers, faxes, disk drives, backup devices, tools, applications, domain names, IP addresses
- Public keys, digital certificates

Directory Data

Inappropriate:

- large, unstructured objects, e.g., image, audi/video files
- rapidly changing information
- to be accessed only once or by one audience

Appropriate:

- URLs, pointers to objects, descriptive information
- frequent reads, infrequent writes
- accessed by many from different physical locations
- expressible in attribute-data format: “surname=Smith“

LDAP Applications

Applications	Directory Data
Yellow Page, address book, corporate directory	people, business, emails, organization, phones
web search engine, browser	document URLs
certificate server, system mgt., authentication services	public keys, digital certificates
network administration account management	users, accounts, passwords, aliases, ACL, servers
network device sharing	printers, faxes, disk drives, backup devices
network name server, firewall/proxy server	IP addresses, node names, server aliases
CORBA application, enterprise database application	distributed objects and databases

Major Players

- **U-M LDAP**
  - pioneered by University of Michigan
  - freeware supported by OpenLDAP
- **Netscape Directory Server**
  - bundled with HP-UX since 10.20
  - ClientSDK is open source freeware.
- **Microsoft Active Directory in Windows 2000**
  - tied to login authentication.
- **Novell Directory Service (NDS)**
  - runs in Novell client/server environment.

Trends of Directory Services

- LDAP is dominating network directory services.
- LDAP services are integrated with operating systems.
- LDAP services are used in login authentication and network account management.
  - HP-UX uses LDAP server as account management and network information server.
  - Microsoft Active Directory is depolyed for signle-signon authentication.
- Metadirectories are emerging for integrating and managing enterprise directories.
- LDAP branches out as a lightweight database protocol.

What is LDAP C-SDK/iX?

- LDAP client API in C to access directories on LDAP servers.
- Used by applications to query and update directory information.
- Command tools for simple queries and testing.
- Enables directory accesses from HP e3000 platform.

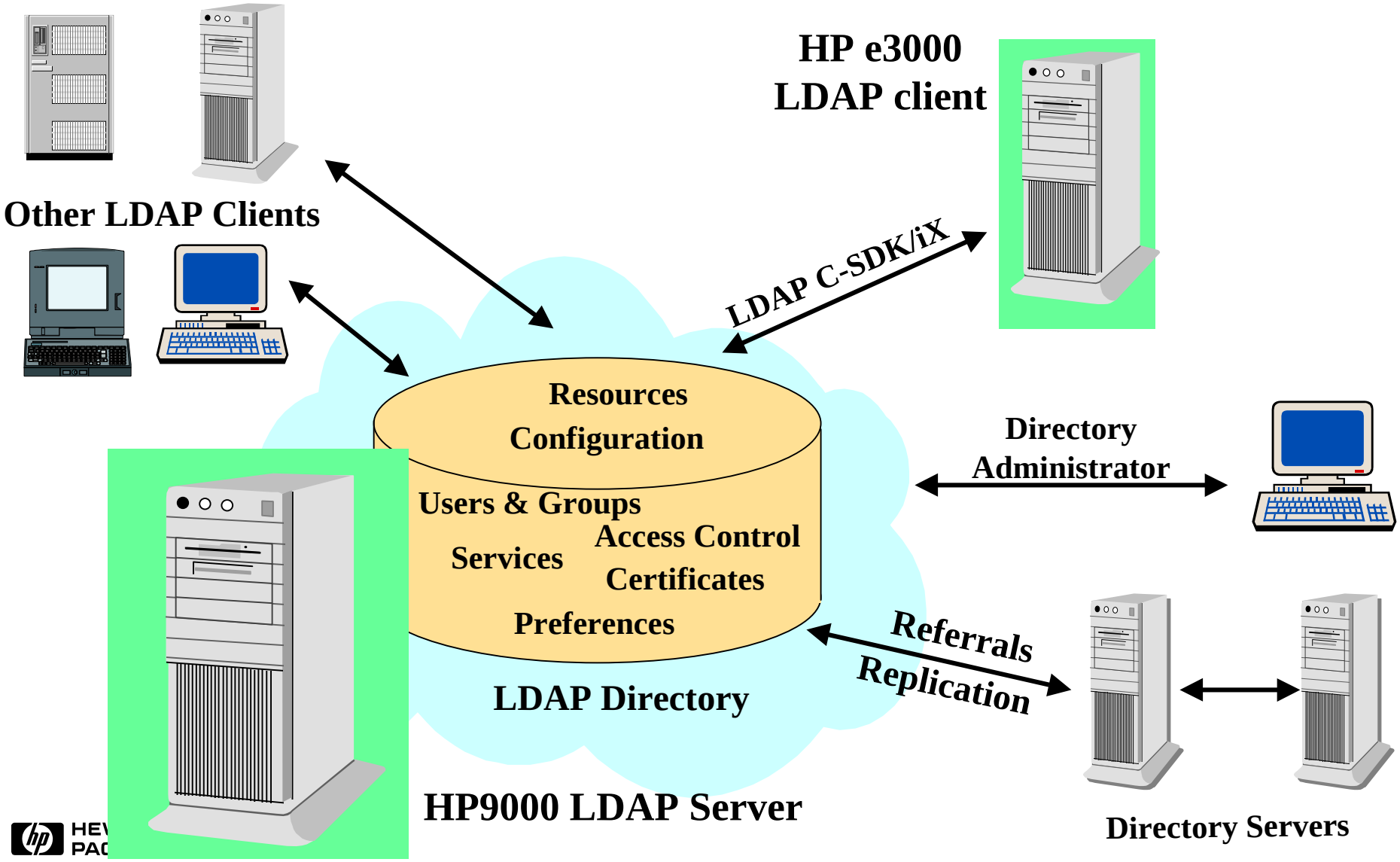
LDAP Client Can:

- Search & retrieve directory entries
- Add new entries
- Delete entries
- Update entries
- Rename entries
- Synchronous wait for the result
- Asynchronously check for the result

LDAP Server Can:

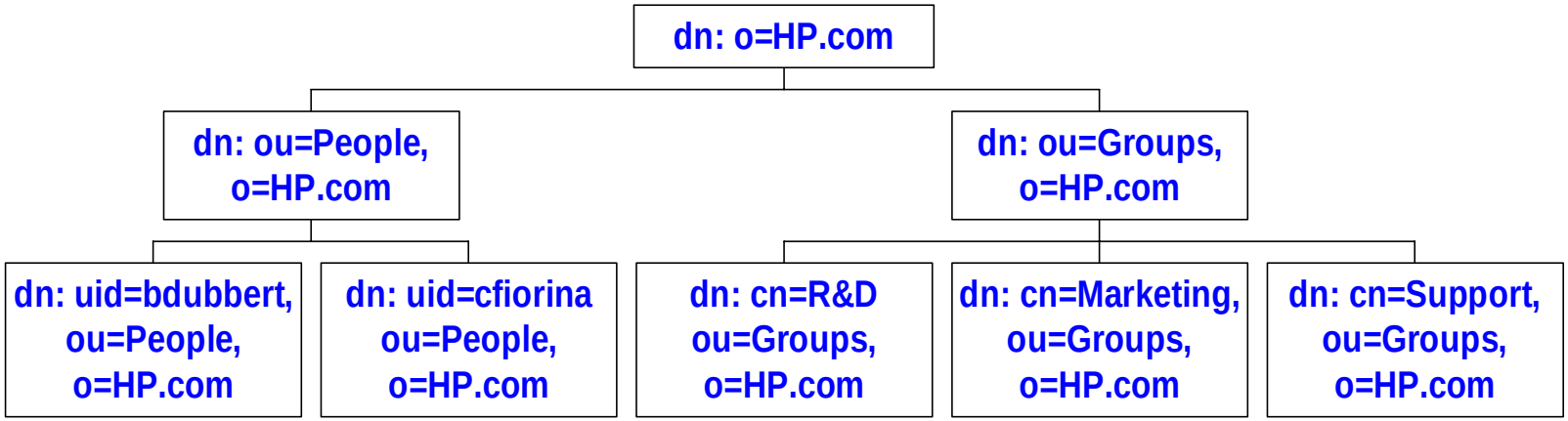
- Perform retrieval/update operations requested by clients.
- Build directory structure.
- Import/export directory data.
- Backup/restore directorires.
- Replicate directory data.
- Make directory referrals to clients.
- Administer access control rules.

Directory Access Via LDAP C-SDK/iX



Directory Hierarchy

- A directory entry is identified by its unique **Distinguished Name (DN.)**
- A directory entry is defined by object classes and attributes.
- Information is associated with a descriptive attribute, e.g., uid=bdubbert.



Directory Schema(1)

- A **schema** defines data representation in the directory.
- A directory schema is comprised of attributes and object classes.
- **ObjectClass** - defines a set of required and optional attributes, e.g. the organizationalPerson object class requires commonName (cn) and surname (sn) attributes.
- **Attribute** - defines attribute name, data type and syntax. e.g., 'telephonenumber' is an attribute type, its data type is case ignored string, multiple values are allowed, and '+1 650 555 1212' is an attribute value.

Directory Schema(2)

- Standard (default) attributes and object classes are defined in slapd.at.conf and slapd.oc.conf configuration files.
- User-defined attributes and object classes are defined in slapd.user_at.conf & slapd.user_oc.conf.
- To extend the schema - either using Directory Console GUI interface on HP-UX or editing the configuration files slapd.user_oc.conf & slapd.user_at.conf,
- OK to add customized elements to the standard schema.
- BUT ... deleting/replacing elements in the standard schema can cause interoperability problem.

Sample Directory Entry

```
dn: uid=cfiorina, ou=People, o=HP.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
ou: Management
l: Palo Alto
uid: cfiorina
mail: cfiorina@hp.com
telephonenumber: +1 650 555 1212
```

LDAP Data Interchange Format (LDIF)

- Used to describe directory entries in text format.
- Used to initially build a directory database.
- Used by the search command to output entries.
- Used by command tools to add/delete large number of entries or describe changes to entries.
- Used by directory servers to import/export the directory data.

LDAP C-SDK/iX Structure

- /usr/local/ldapsdk/ - auto-installed with OS
- /usr/local/ldapsdk/lib/ - libldap.a, liblber.a
- /usr/local/ldapsdk/include/ - ldap.h, lber.h
- /usr/local/ldapsdk/tools/ - command tools: ldapsearch, ldapmodify, ldapdelete
- /usr/local/ldapsdk/examples/ - sample C source of client applications and a makefile
- /usr/local/ldapsdk/docs - Netscape Directory SDK 3.0 for C Programmer's Guide

Client Command Tools

- **ldapsearch** -b basedn [-h host] [-p port] [-H for help] [options] filter [attributes-to-be-retrieved]
- **ldapmodify** [-h host] [-p port] [-f infile] [-D binddn] [-w passwd] [-a for adding entries] [-H ... options]
- **ldapdelete** [-h host] [-p port] [-D binddn] [-w passwd] [-H for help ... options] deleted-dn
- -D specifies the DN permitted to update the entries, e.g., root or directory manager.

Searching For An Entry

```
ldapsearch -hhost -p389 -b"o=HP.com" "uid=cfiorina"
```

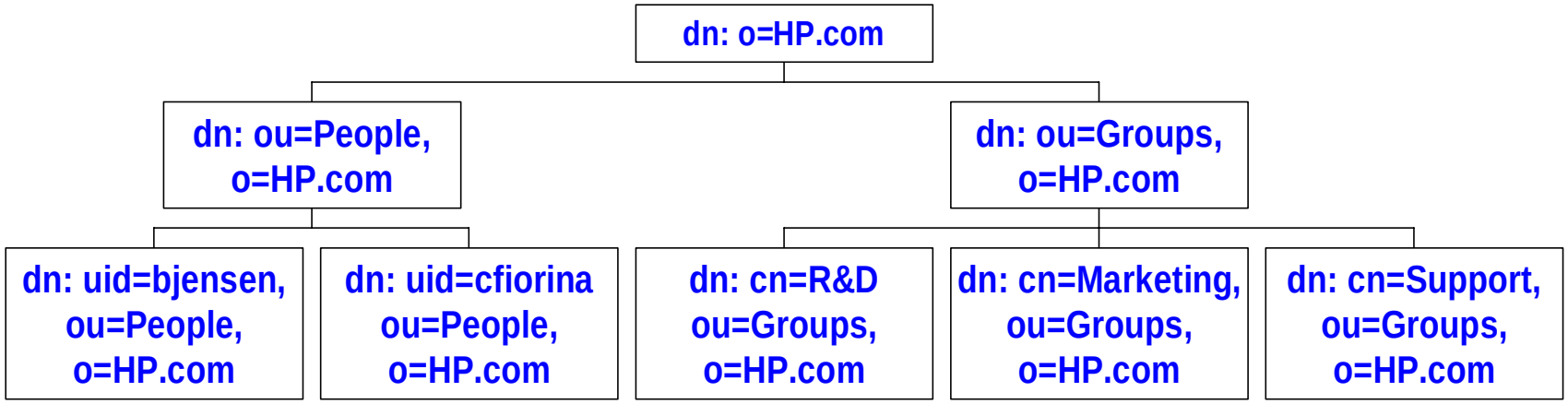
```
dn: uid=cfiorina, ou=People, o=HP.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
ou: Management
l: Palo Alto
uid: cfiorina
mail: cfiorina@hp.com
telephonenumber: +1 650 555 1212
```

Searching A Directory

- Search can start from any base dn (*-b* option), e.g.,

  ldapsearch -hhost -p389 -b"ou=People,o=HP.com" "uid=cfiorina"

  ldapsearch -hhost -b"o=HP.com" "uid=cfiorina"



Adding An Entry

```
ldapmodify -a -h host -D "cn=Directory Manager" -w passwd
dn: uid=cfiorina, ou=People, o=HP.com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
ou: Management
l: Palo Alto
uid: cfiorina
mail: cfiorina@hp.com
telephonenumber: +1 650 555 1212
```

Modifying An Entry

ldapmodify -hhost -p389 -D "cn=Directory Manager"
-finfile -wpassword

catinfile

```
dn: uid=cfiorina, ou=People, o=HP.com
changetype: modify
replace: l telephonenumber
l: Cupertino
telephonenumber: +1 408 555 1212
```

Deleting An Entry

```
ldapdelete -h host -D "cn=Directory Manager" -w passwd
           "uid=bjensen,ou=People,o=HP"

ldapdelete -h host -D "cn=Directory Manager"
           -w passwd -f infile

cat infile
   uid=bjensen, ou=People, o=HP
   uid=csmith, ou=People, o=HP
   uid=djones, ou=People, o=HP
```

LDAP Client-Server Interactions

- Server daemon slapd listens on the LDAP port (default 389.)
- Client binds & authenticates to Server via SOCKET.
- Client sends operation requests (search, add, modify, delete, etc.) to Server.
- Server performs directory operations, then returns results.
- Client retrieves and parses results.
- Client unbinds from Server.

Version Compatibility

- **LDAPv3** protocol is backward compatible with **LDAPv2**.
- OK -- if client on LDAPv2, server on LDAPv3.
  Not OK -- if client on LDAPv3, server on LDAPv2.
- LDAP C-SDK/iX can connect to LDAPv2 & LDAPv3 servers.
- By default, LDAP C-SDK/iX uses LDAPv2 protocol to connect to the server.
- To use LDAPv3 features, the application must call ldap_set_option() to set the protocol version to LDAPv3.

Synchronous/Asynchronous Directory Operations

- **Synchronous** - Client waits for the operation to complete, ldap_bind_s(), ldap_search_s().
- **Asynchronous** - Client doesn't wait for the operation to complete, but continues on other tasks, e.g. ldap_bind(), ldap_search().

  Client checks the result later by calling ldap_result(), ldap_parse_result().

API Calling Sequence

- Initialize an LDAP session: ldap_init()
- Query/set the protocol version for client-server version compatibility: ldap_get_option(), ldap_set_option()
- Bind & authenticate to the server: ldap_simple_bind()
- Request LDAP operations: ldap_search(), ldap_add(), ldap_delete_s(), ldap_modify_s(), ...
- Check operation results: ldap_result(), ldap_parse_result()
- Retrieve/sort search results: ldap_first_entry(), ldap_next_entry(), ldap_count_entry(), ldap_sort_entries(), ldap_sort_values(), ldap_create_sort_keylist(), ...
- Close the connection to the server: ldap_unbind()

Running LDAP Server on HP-UX

- Installation: Netscape Directory Server v4 for HP-UX bundled with OS, downloadable from : http://www.software.hp.com .
- Create a directory instance:
  - Customize configuration files: slapd.conf and slapd.ldbm.conf.
  - Extend directory schema if needed.
  - Import directory data: sample data bundled with Server.
  - Start the server daemon ns-slapd.
- Start Administration Server and Directory Console for a GUI administration tool.
- Run client applications/commands.
- Verify error and access logs from Directory Console or log files.

Import/Export A Database

- Import/Export directory database from /to an LDIF file.
- If importing, customize the directory schema, and add the database name to slapd.ldbm.conf, e.g., #suffix o=HP.
- Import by Direcotry Console interface allows appending the imported data to the existing database..
- Import by ns-slapd command overwrites the existing database:

  import: ***ns-sldap ldif2db -Ifrom_ldif_file -fslapd.conf***

  export: ***ns-sldap db2ldif -ato_ldif_file -fm slapd.conf***

References

- **LDAP C-SDK/iX home page**
  http://jazz.external.hp.com/src/ldap/index.html
- **HP Software Depot for Netscape Directory Server**
  http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=J4258BA
- **OpenLDAP freeware home page**
  http://www.OpenLDAP.org/
- **OpenLDAP for MPE/iX:** unsupported freeware ported by Lars Appelof HP; LDAPv2 based implementation
  http://www.editcorp.com/personal/lars_appel/ldap/

References

- **IETF LDAP RFCs: 2251-2257**
  http://info.internet.isi.edu:80/1s/in-notes/rfc
- **Netscape Directory SDK 3.0 for C Programmer's Guides**
  http://developer.netscape.com/docs/manuals/dirsdk/csdk30/index.html
- Manuals **of Netscape Directory Servers**
  http://developer.netscape.com/docs/manuals/directory.html
- **University of Michigan LDAP project**
  http://www.umich.edu/~dirsvcs/

Books on LDAP

- **Programming Directory-Enabled Applications with Lightweight Directory Access Protocol**

  by Timothy A. Howes and Mark C. Smith

- **Understanding and Deploying LDAP Directory Services**

  by Timothy A. Howes and Gordon S. Good