Directory Services on OS/390 and z/OS (Vanguard Session 61)

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

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

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.

What are we going to talk about?

- Directory Information model
  - Hierarchy of entries
  - Object classes
  - Attributes
- Directory Servers and a Directory Service
- OS/390 LDAP Client/Server Overview
  - Features
  - Differences Between releases
  - Capabilities
  - Usage

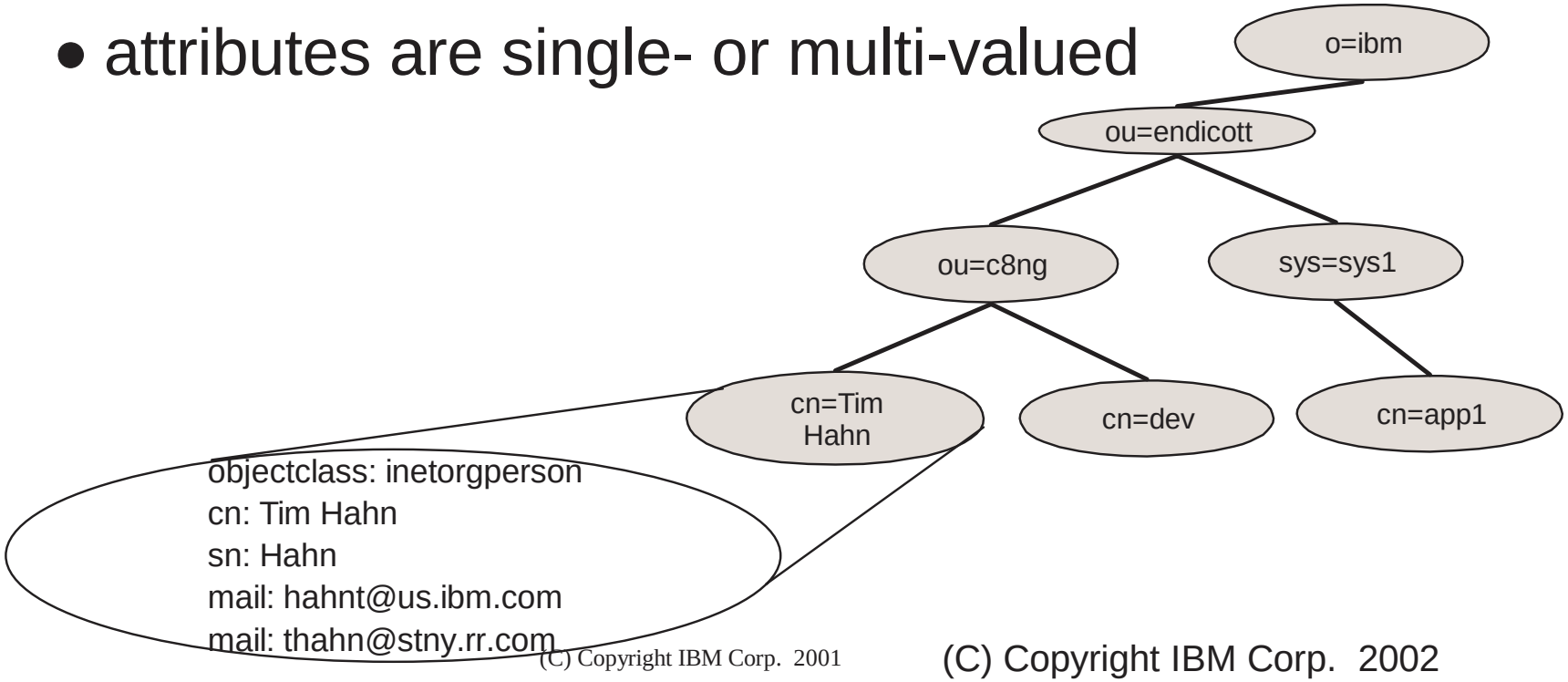
What is LDAP?

- 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

(C) Copyright IBM Corp. 2001

Directory Information Model

- An LDAP Directory is formed by a hierarchy of "entries"
- Each "entry" has:
  - a name (called a distinguished name)
  - a structure (called an "object class")
  - attributes
    - attributes are single- or multi-valued

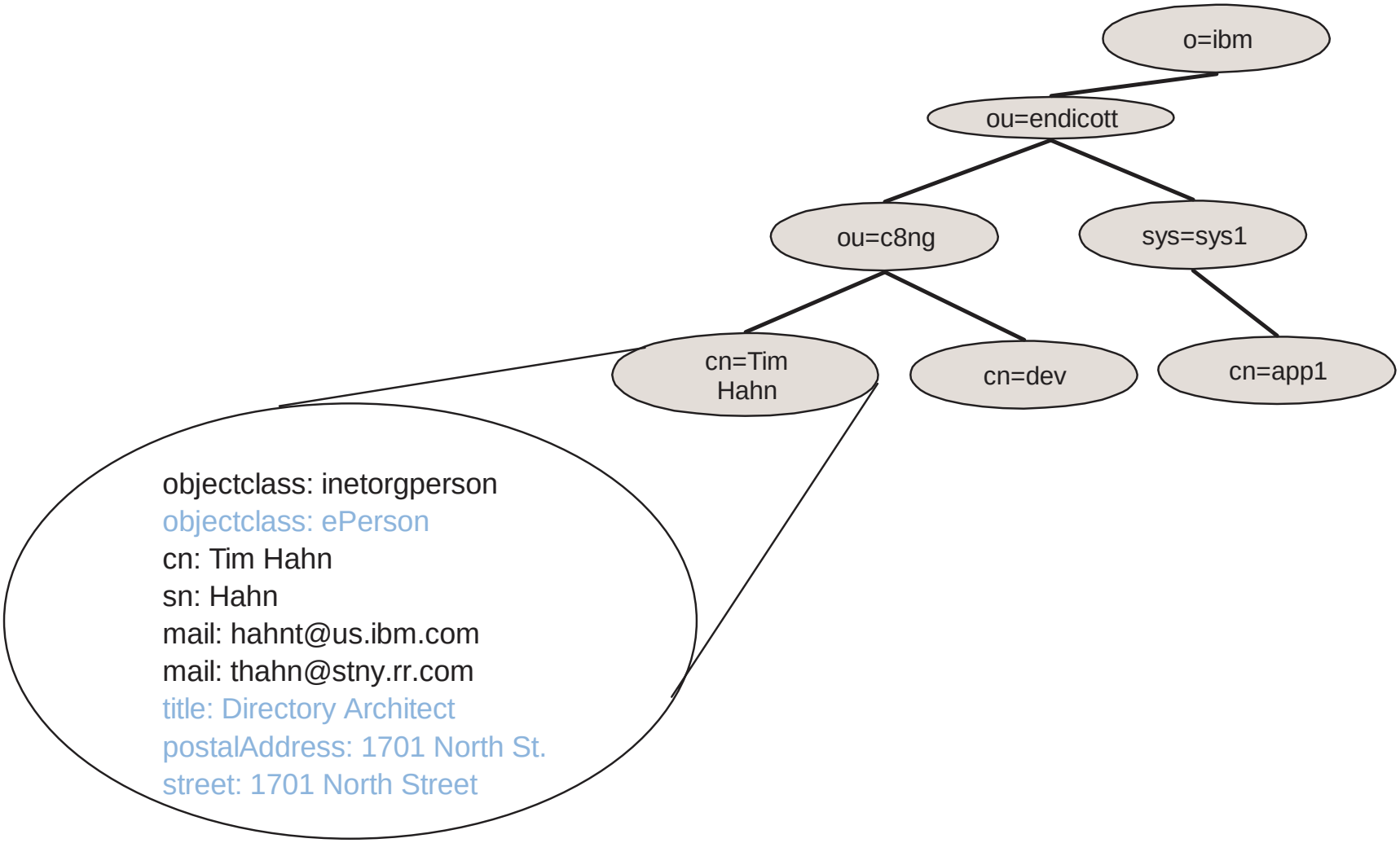


Directory Information Model

- An Entry's "object class" defines
  - structure of an entry
  - attributes that MUST be present in an entry
  - attributes that MAY be present in an entry
- An individual Entry in the directory can take on the form of multiple object classes
  - The attributes in the entry are the UNION of those defined for individual object classes

(C) Copyright IBM Corp. 2001

Directory Information Model



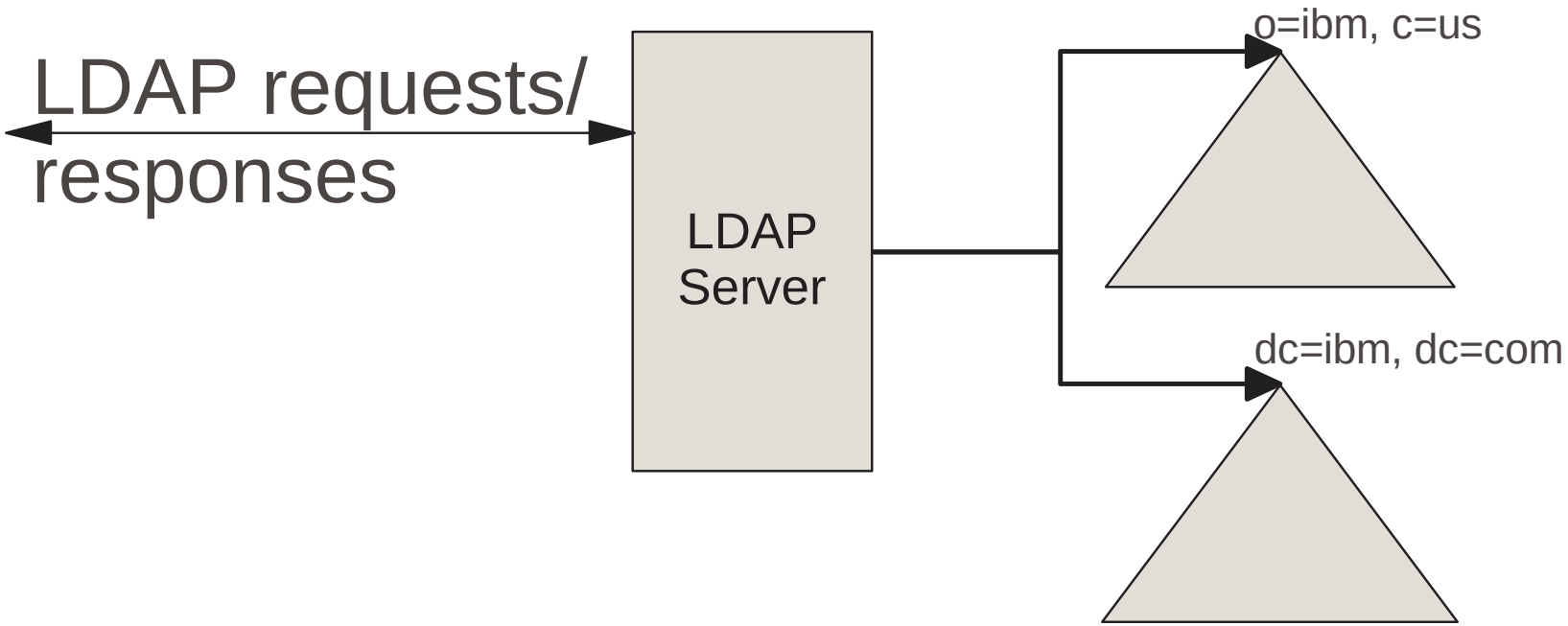
Directory Information Model

- Attributes are defined by their name, syntax, and matching rule(s)
  - Syntax refers to the type of data stored in attribute values
    - Examples: directoryString, binary, integer
  - Matching Rules define how equality and ordering comparisons are performed on attribute values
    - Examples: caseIgnoreMatch, caseExactMatch, octetStringMatch
- Different attributes within an entry may be more "sensitive" than others within an entry
  - Example: common name (cn) vs. uid vs. userPassword

(C) Copyright IBM Corp. 2001

Directory Servers

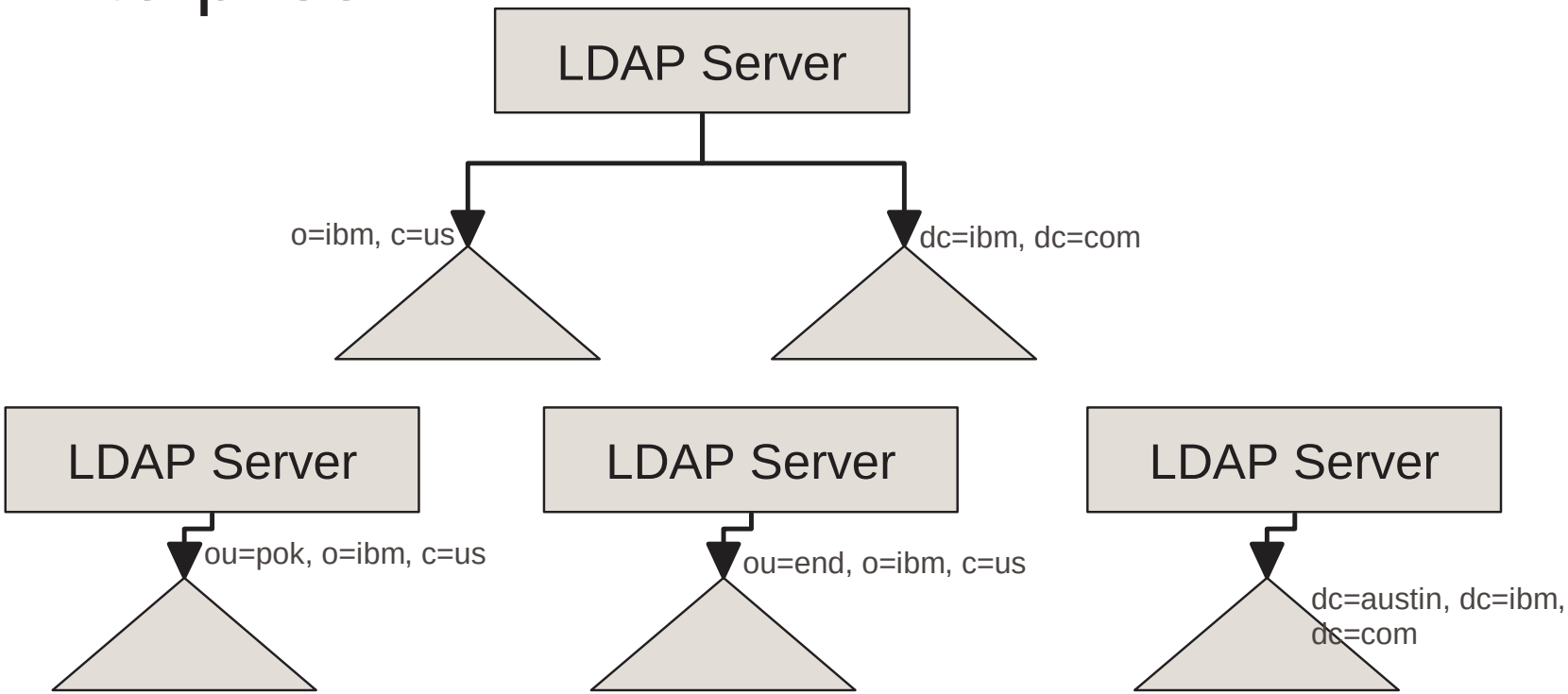
- A Directory Server
  - accepts and responds to directory requests
  - manages a portion (set of "sub-trees") of a directory "namespace"



(C) Copyright IBM Corp. 2001

Directory Service

- A Directory Service
  - is a set of servers which, together, serve a directory "namespace"
  - is a value to the Enterprise, across the Enterprise



OS/390 LDAP Components

- LDAP C/C++ APIs (client)
  - As of V2R8 ships in OS/390 Security Server in same FMID as LDAP Server (HRSL180)
  - 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 (as of 12/2000)

Features of the OS/390 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 OS/390 Security Server

OS/390 LDAP Components

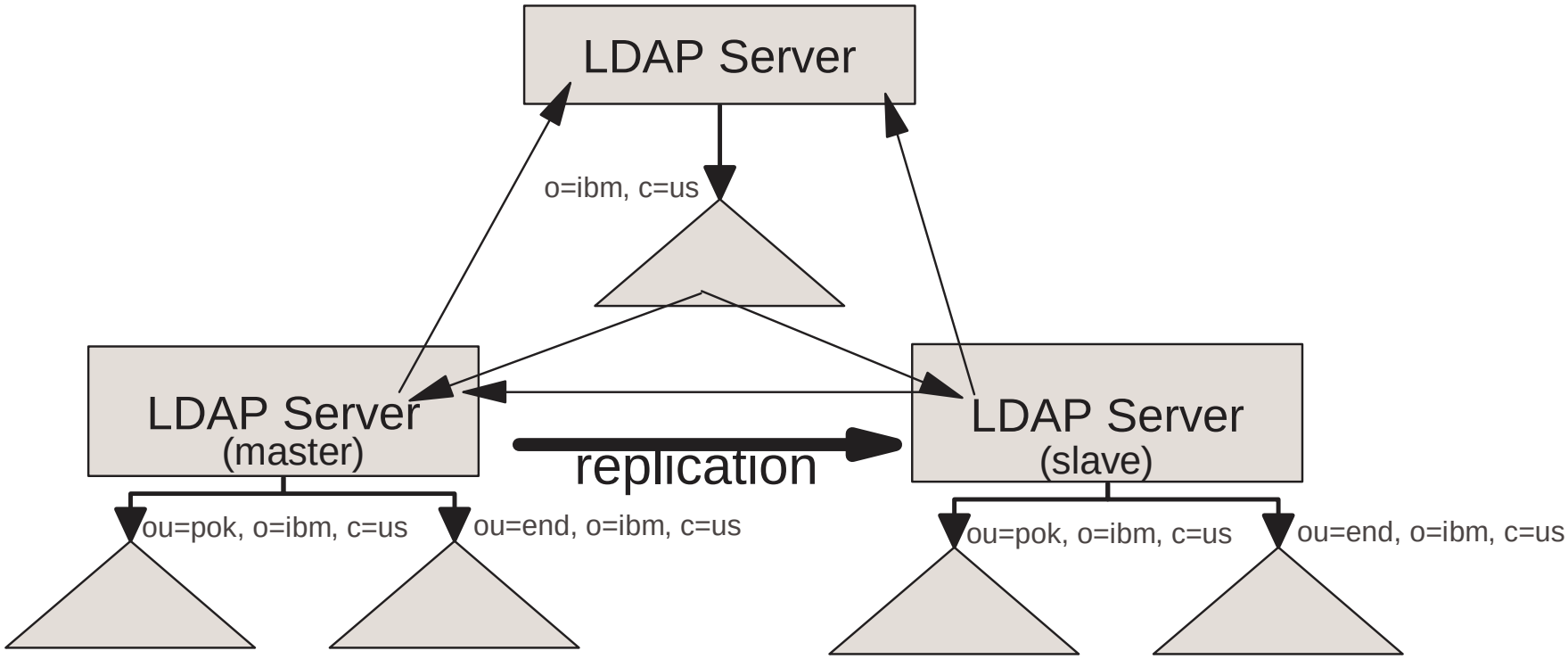
- LDAP Server
  - Accepts and responds to LDAP protocol requests
  - Supports DB2 backing store(s) and access to RACF
  - OS/390 R10 scalability improvements
  - OS/390 R10 "V3" schema support
  - z/OS R1 LDAP configuration utility
  - z/OS R2 Concurrent client scalability
- Server ships as ALWAYS ENABLED in OS/390 Security Server
- For customers to use LDAP clients or server, MUST install OS/390 Security Server

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

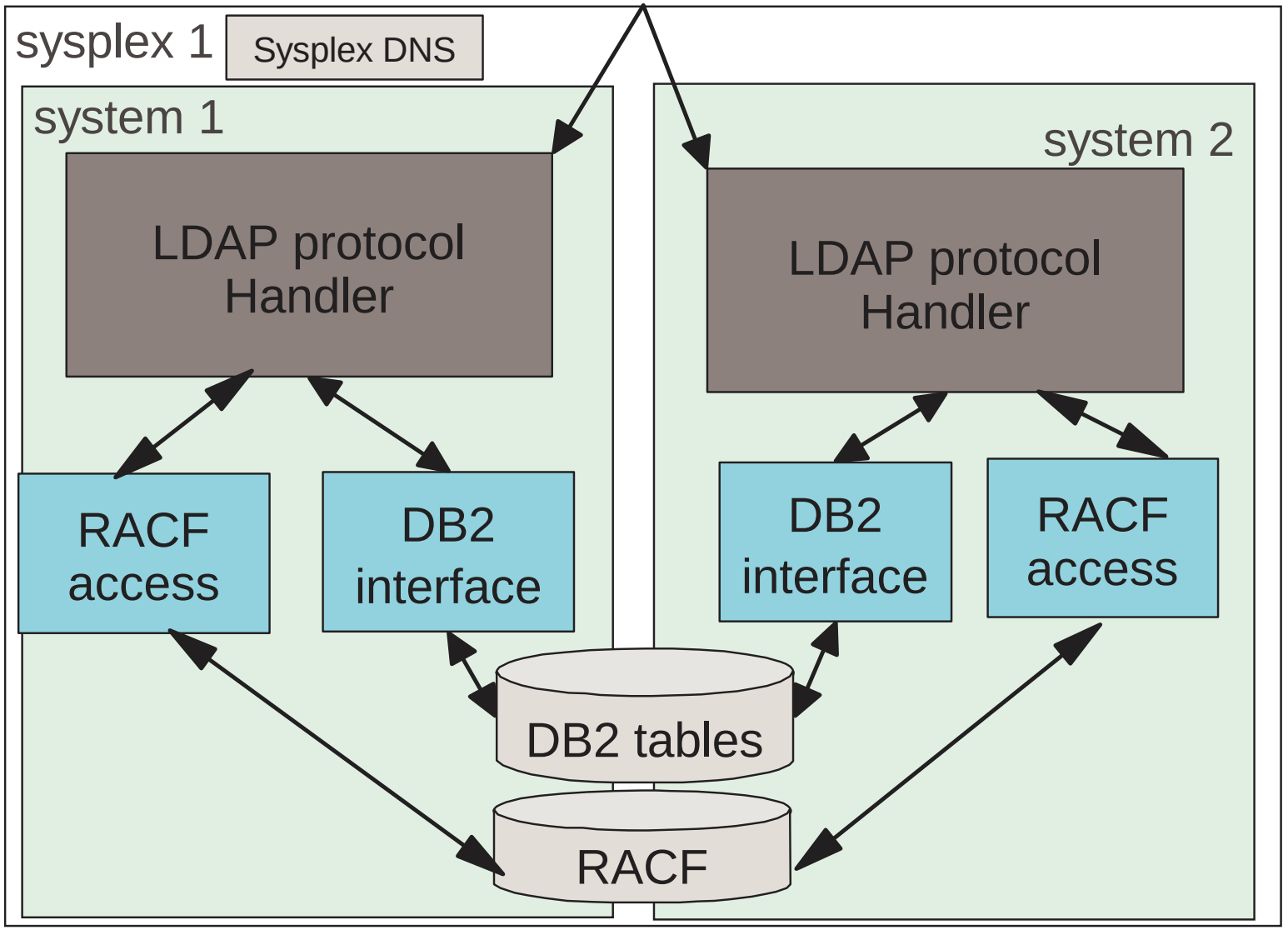
- OS/390 R5
  - Secure communications using SSL
  - Multiple Concurrent Servers
  - Master/Slave replication
- OS/390 R7
  - Sysplex Support
  - DB2 and RACF backing stores
  - Extended group searching for access control checking
- OS/390 R8
  - LDAP V3 protocol support (partial) - rootDSE, certificate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

Namespace Example Using Referrals and Replication

Example using referrals and replication



OS/390 LDAP Server Sysplex Support



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

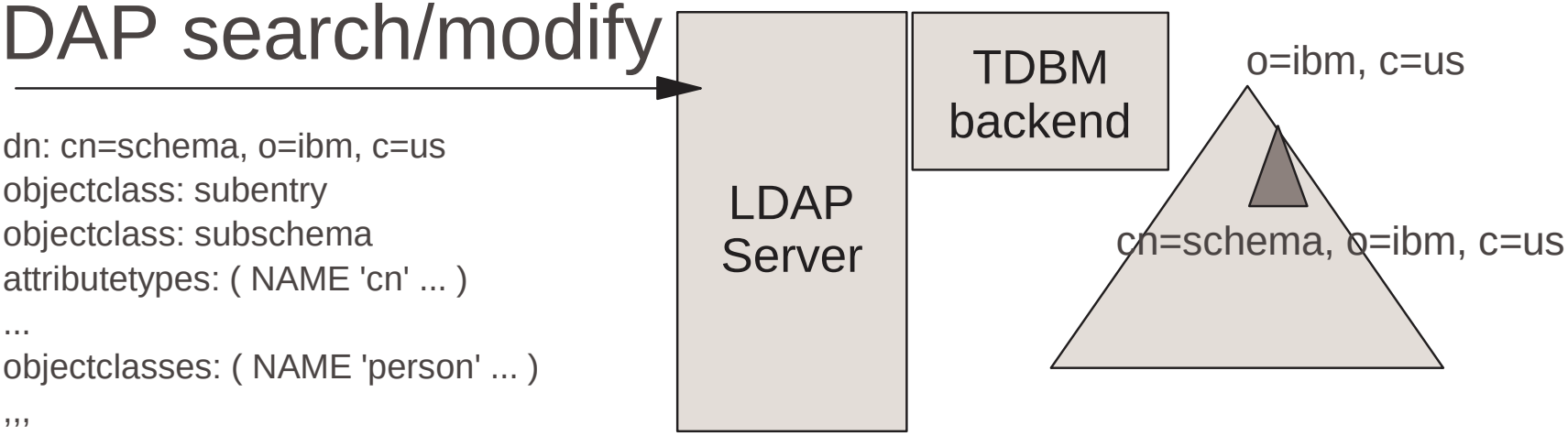
Schema pub & update

- 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)

(C) Copyright IBM Corp. 2001

Schema pub & update

LDAP search/modify

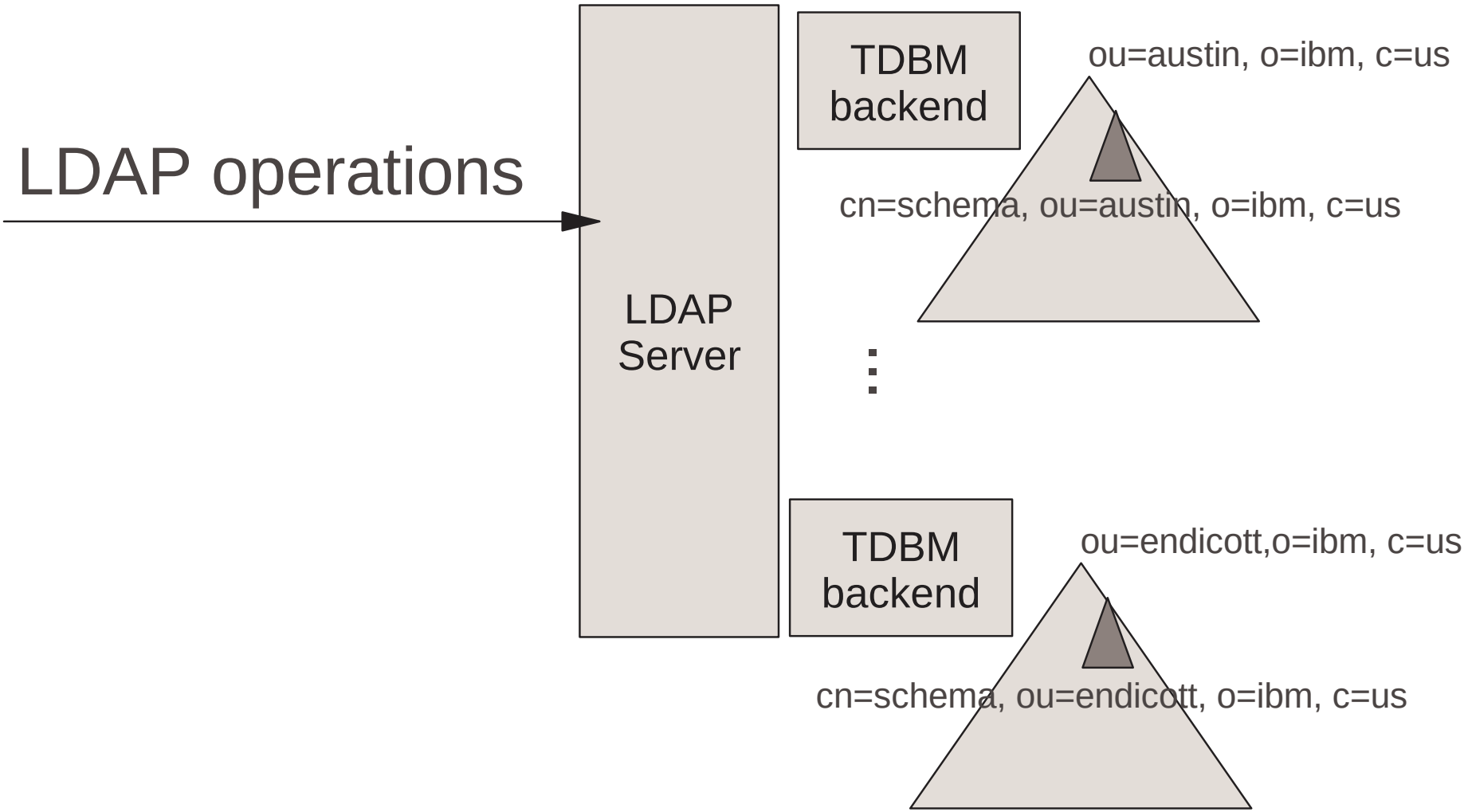


Scalable Backend/TDBM

- 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"

(C) Copyright IBM Corp. 2001

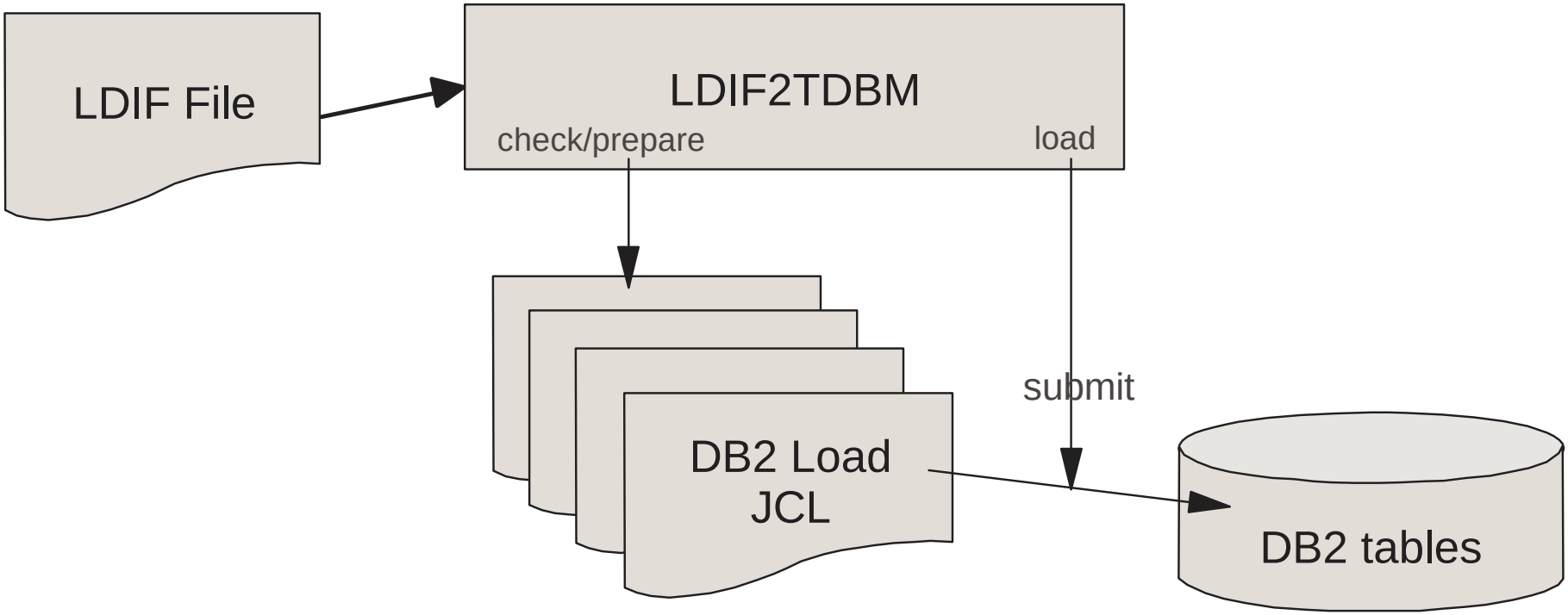
Scalable backend/TDBM



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

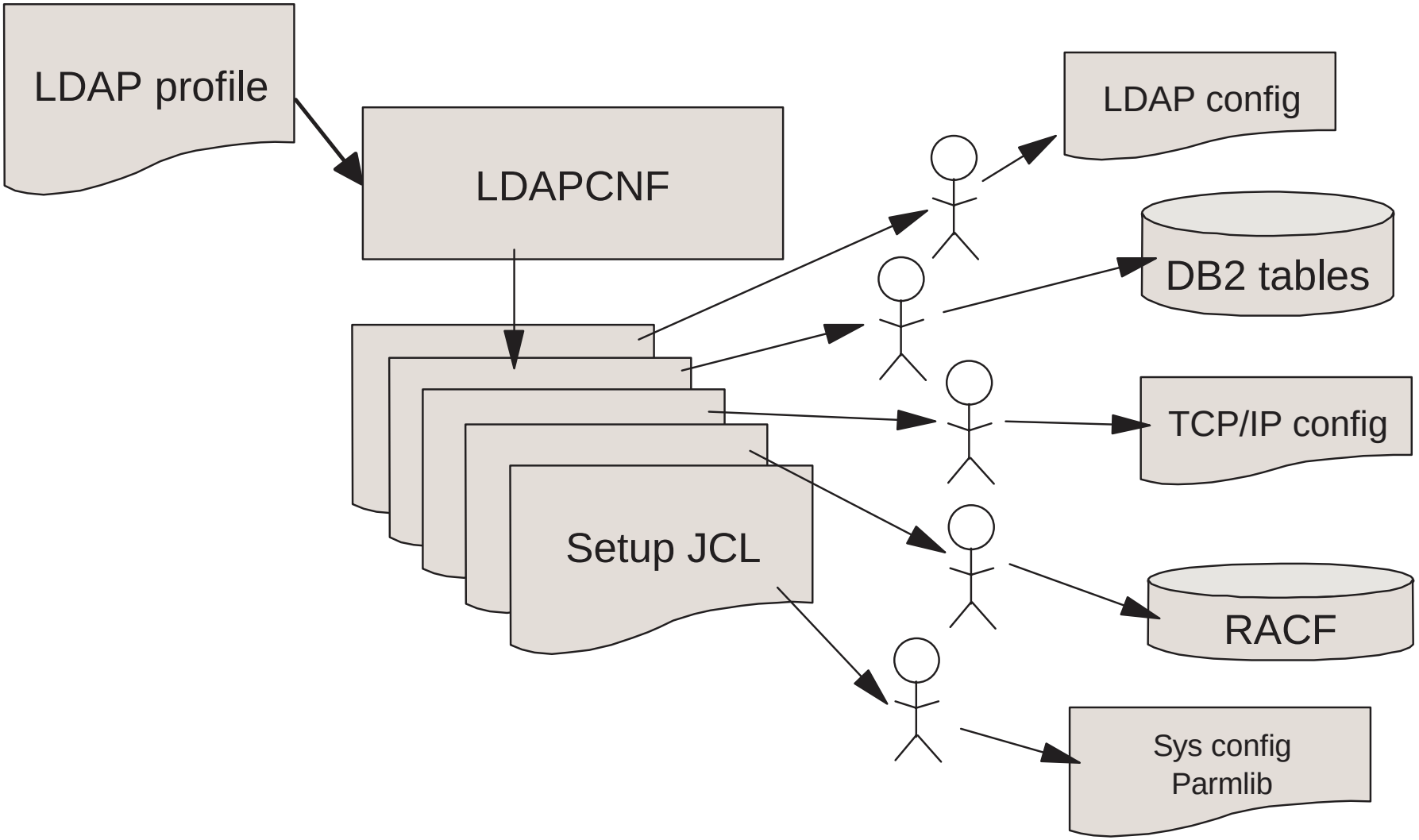
Bulk load utility - block diagram



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

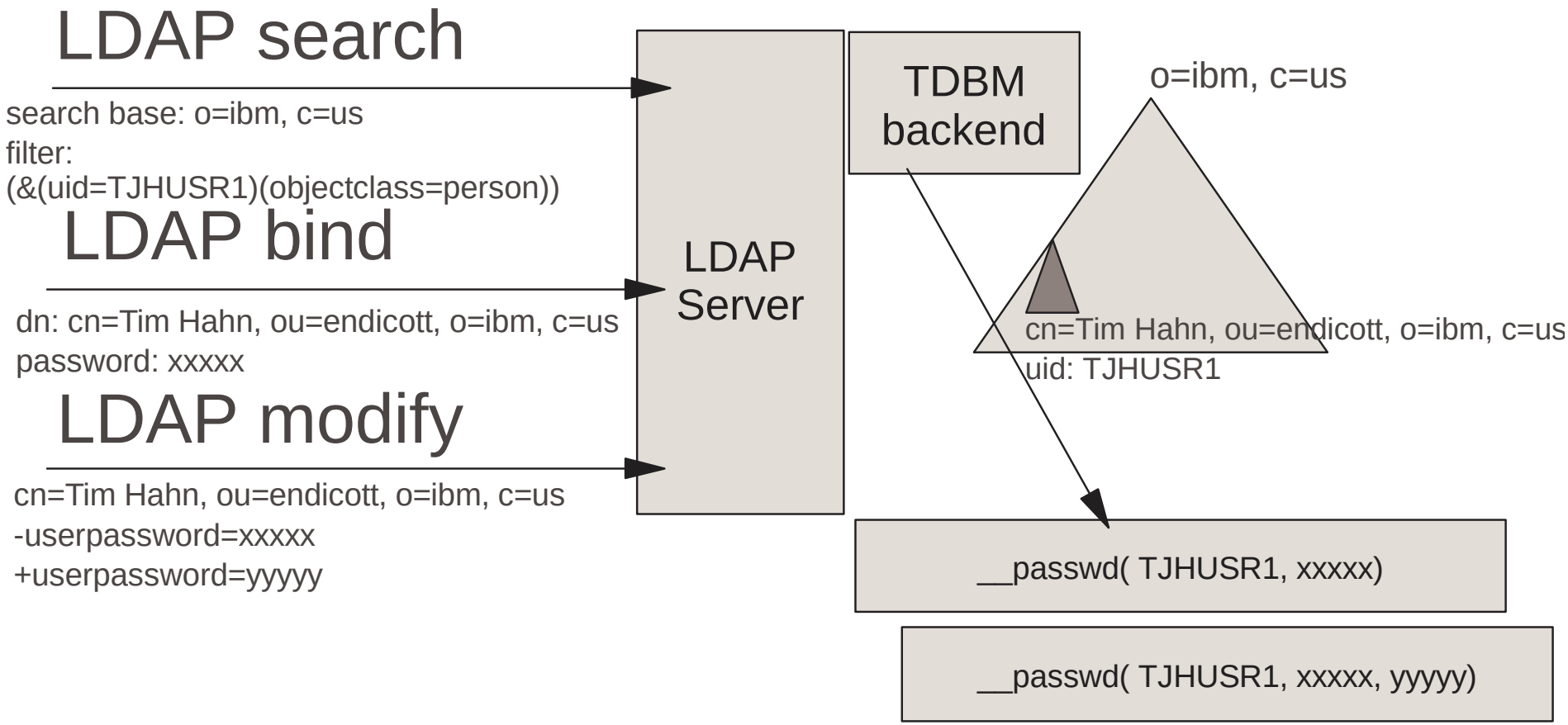


Native Authentication (OW47596)

- 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.

(C) Copyright IBM Corp. 2001

Native Authentication

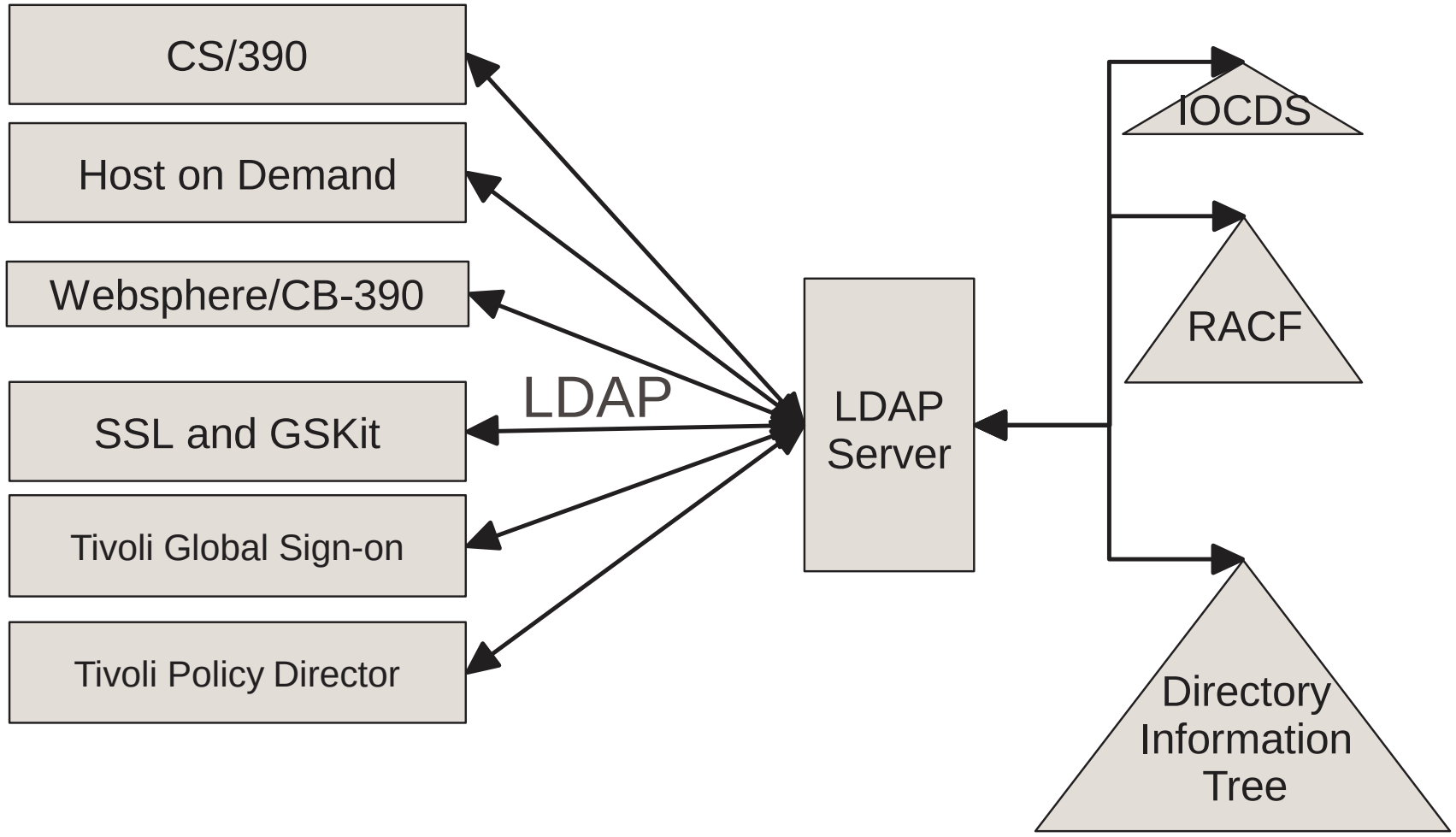


(C) Copyright IBM Corp. 2001

Features added in z/OS V1R2

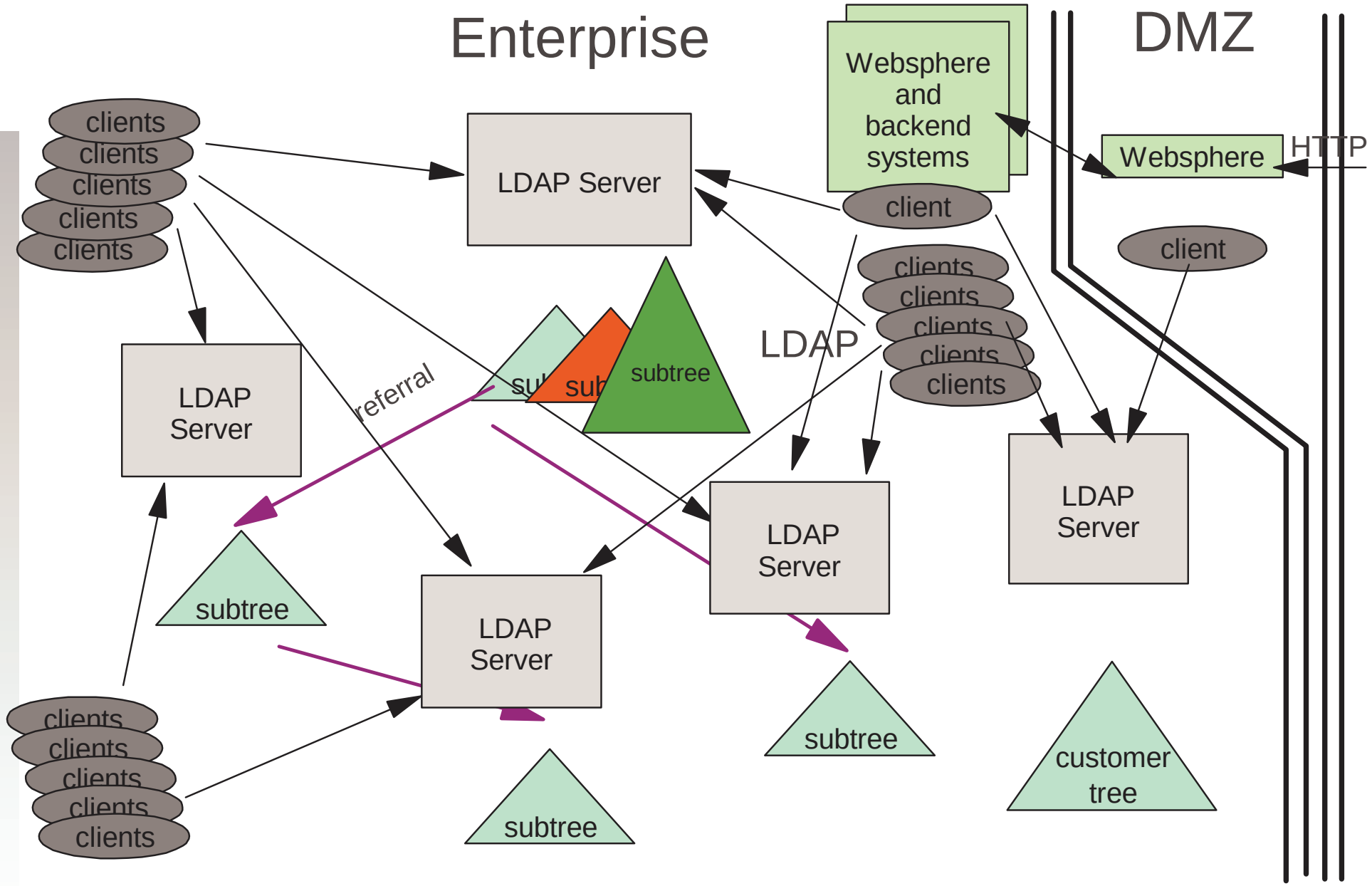
- Also made available on OS/390 V2R10 and z/OS V1R1 via APAR OW50971
- Server Features
  - CONNECT support - add/remove users from groups using RACF access
  - Allow selected attribute-based searching of RACF user/group information
  - Handle over 50,000 concurrent clients
  - Kerberos-based authentication
- Client Features
  - results caching - reduces network requests for repeated searches
  - DNS SRV records for locating LDAP servers
  - Kerberos-based authentication

Directory Usage by IBM Products



(C) Copyright IBM Corp. 2001

Enterprise Namespace



(C) Copyright IBM Corp. 2001

For More Information

- LDAP RFCs
  - http://sunsite.auc.dk/RFC/rfc/rfc2251.html- rfc2256.html
- z/OS LDAP Documentation
  - SC24-5923-02 z/OS V1R2.0 Security Server LDAP Server Administration and Use
    - http://publibz.boulder.ibm.com/epubs/pdf/glda2a11.pdf
  - SC24-5924-01 z/OS V1R2.0 SecureWay Security Server LDAP Client Programming
    - http://publibz.boulder.ibm.com/epubs/pdf/glda1a10.pdf
- Books
  - e-Directories: Enterprise Software, Solutions, and Services
    House, Hahn, Mauget, Daugherty
    ISBN: 0-201-70039-5
    - http://www.awl.com/cseng/titles/0-201-70039-5
  - Understanding LDAP
    - http://www.redbooks.ibm.com
- Contacting me
  - e-mail: hahnt@us.ibm.com