IBM®

ENVISION

DECISIONS

Lotusphere® 2005

Lotusphere 2005

ENVISION DECISIONS

Advanced LDAP Infrastructure Design (Updated!)

Chris Miller
Director of Messaging and Collaboration
Connectria

Spam — Susan
Workplace Messaging — Chris
LDAP →
irus — Kyle
Backups — Karen

Agenda

- How many phone books can be delivered to my door?
- All in one shopping or drive across town?
- My house is made of twigs, what about yours?
- If I had wanted the soup I would have ordered it

LDAP Product Selection

- What do the terms mean?
  - LDAP compatible
  - LDAP compliant
  - LDAP ready
  - LDAP certified
  - LDAP V3

Federation and Aggregation

Federation and Aggregation

- Federation
  - Referrals and redirections to original directories for information not found in the original directory
    - Remember: referrals are strictly utilized to tell a LDAP lookup where another host is that might have the necessary information

Federation and Aggregation

- Aggregation
  - Collecting objects and attributes into a single source
  - Simple central management for user accounts
  - But….expanding the schema can be difficult to accommodate everyone

Lotus.
Excedrin
Advil
LIQUI-GELS
EXTRA STRENGTH
TYLENOL
Caplets
500 mg

LDAP Architecture

- Centralized directory services
  - Gather round the campfire
- Redundant directory services
  - One potato, two potato
- Distributed directory services
  - Where every server has a home
- Filtered directory services
  - search based directory services enhanced

Search Filters and Bases

- Search Filter
  - Define the objectClass(es) and attribute(s) used to search for users in the directory
  - The finer you are able make these filters the better performance and easier security implementation
- Search base
  - Where do we begin a search in the LDAP tree of the directory

Aggregated Architecture Issues

- The inherent flexibility of LDAP means that each of you implement it slightly different.
  - Compound that across divisions or new companies being merged
  - Randomly confusing and created organizational hierarchy
  - Selected and utilized LDAP attributes vary across implementations
  - Wild schema customizations

LDAP Security

- What data is stored in the directory?
- Where is the server shared beyond the walls of your organization?
- When is directory synchronization and maintenance performed?
- Why do users need editor access to the directory?
- Who has the access to update directory information?

Access Control

- Access Control Lists (ACLs) are maintained much like the theory you utilize now in Domino
  - Sample ACL section from OpenLDAP

```
access to attrs=userPassword
by self write
by anonymous auth
by * none
access to *
by * read
```

Security Considerations

- What data is stored in the directory?
- Where is the server shared beyond the walls of your organization?
- When is directory synchronization and maintenance performed?
- Why do users need editor access to the directory?
- Who has the access to update directory information?

Authentication Mechanisms

- Basic username and password
  - Plain text passing of information
  - All network traffic is viewable
- SSL
  - Common certificates are required
  - Fully qualified names are required

Authentication Mechanisms

- SASL (Simple Authentication Security Layer)
  - A user is identified and authenticated to a server
  - Once authentication occurs a security layer is inserted
- TLS
  - Provides transport protection of communication
  - Does not prevent fake servers without a common certificate

Authentication Mechanisms

- Binding DN for authentication
  - Can follow SSL, SASL and utilize TLS
  - A distinguished name must be provided along with a password
- Anonymous access can be granted using SSL and TLS

Vendors and Their Claims

- As you plan, your enterprise must understand how the vendor’s scalability claims are developed and supported
- As you plan, you must have a realistic understanding of your own scalability needs.
  - Is a bigger claim always the better claim?

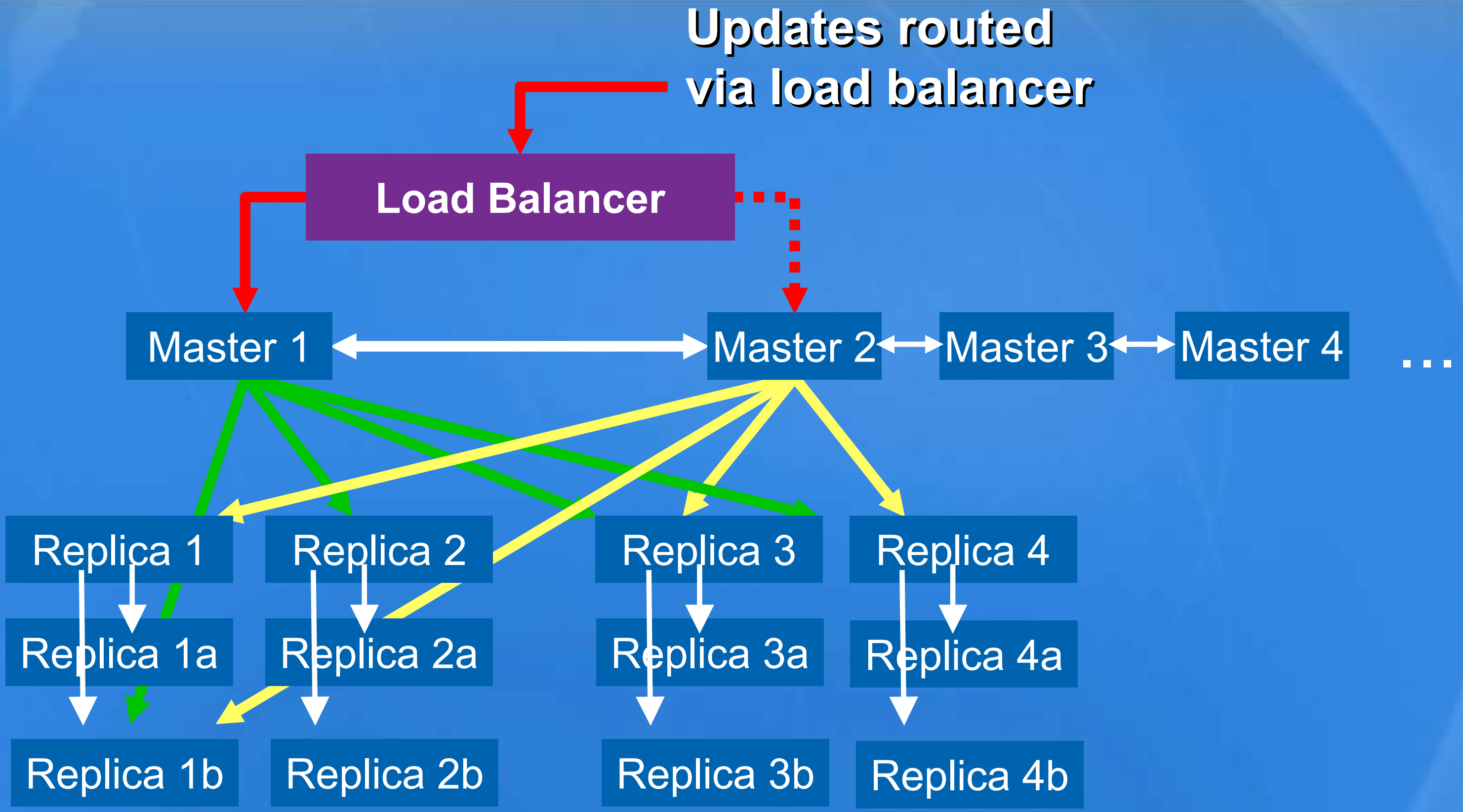
Scalability Options

- Options for distributed directories either load balanced or master/slave architecture
  - Directory replication
    - Multiple servers contain the same data
  - Directory partitioning
    - Unique and non-overlapped data per directory
    - Referrals fall under this architecture
- Mixing these is allowed……

Scalability Options

- Utilize load balancing hardware to spread the load across clustered servers
  - What is required to reach this scaling?
  - Drawbacks?
- Utilize a master/slave architecture to provide directory updates to read only directory servers
  - What is required to reach this scaling?
  - Dearbacks?

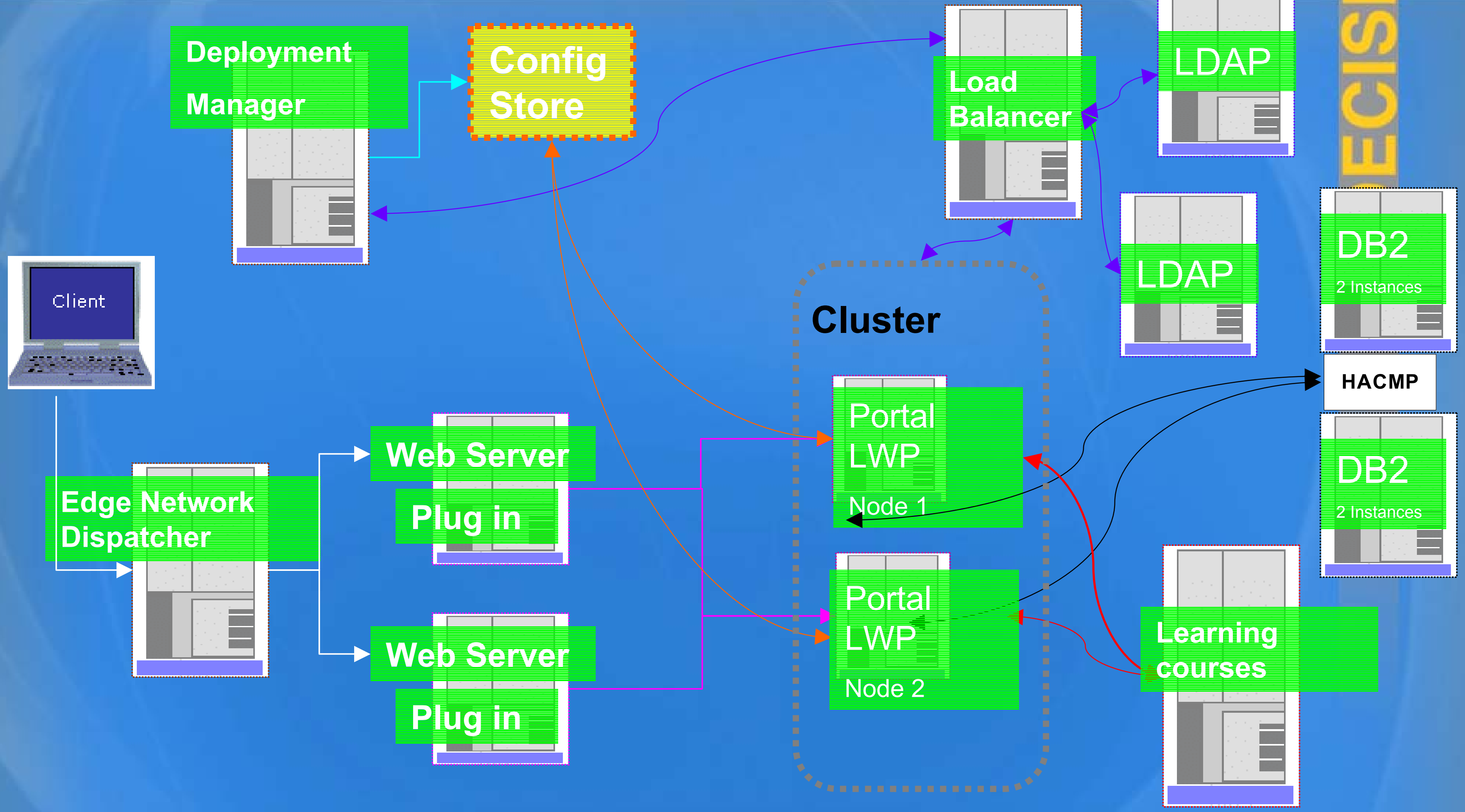
Reliability and Availability



- Multi-master capability, potentially dozens of masters.
- Cascaded Replication permits replication over a WAN without redundant transmission. Subtree replication acts on only certain subtrees.

Source: IBM Software University

Layers of Redundancy



Source: *Jeff Jablonowski-ISSL*

LDAP Partitioning and Referrals

- **Partitioning**
  - Preferred if directory is very large, if applications require local workgroup data, and/or if replication might result in a high load in WAN
  - Unique, non-overlapping naming contexts (sub trees)
  - Name space is linked together by Referral mechanism
- **Referrals**
  - Client requests information from read-only server
  - Read only returns referral to master (read/write) server
  - Client resends request to master
  - Master returns information to client

LDAP Replication

- Directory servers are kept in sync
  - Replication can be either
    - Full: propagating the entire DIT to another node
    - Partial: involves propagating one or more sub trees
- Replicas can be read-only, updatable, or both
  - Single Master
  - Cascaded
  - Peer-to-Peer

Working with any schema

- Consistency across all schemas is key to a stable LDAP infrastructure
- Proactively place the Notes Distinguished Name into the remote LDAP directories that will be utilized
    - This allows for simpler security management
    - Integration for presence
    - Create (or utilize an open existing attribute) for placement of the Notes DN

LDAP and Sametime

- When a Sametime server is configured to use an LDAP directory, Sametime uses search filters to resolve user names. (Filters found in Sametime Administration Tool.)
- Search filter for resolving person names:
  - (&(objectclass=organizationalPerson)(|(cn=%s*)(givenname=%s*)(sn=%s*)(mail=%s*)))
- Search filter to use when resolving a user name to a distinguished name:
  - &(objectclass=organizationalPerson)(|(cn=%s)(givenname=%s)(sn=%s)(mail=%s))
- 200 character limit in search string!!!!

LDAP and Sametime

- For performance reasons, you should limit your search filters to the following LDAP attributes in Person Doc:
  - cn - mapped to the Full Name field
  - givenname - mapped to the First Name field
  - sn - mapped to the Last Name field
  - mail - mapped to the Internet Address field
  - uid - mapped to the Shortname/UserID field

LDAP and Sametime

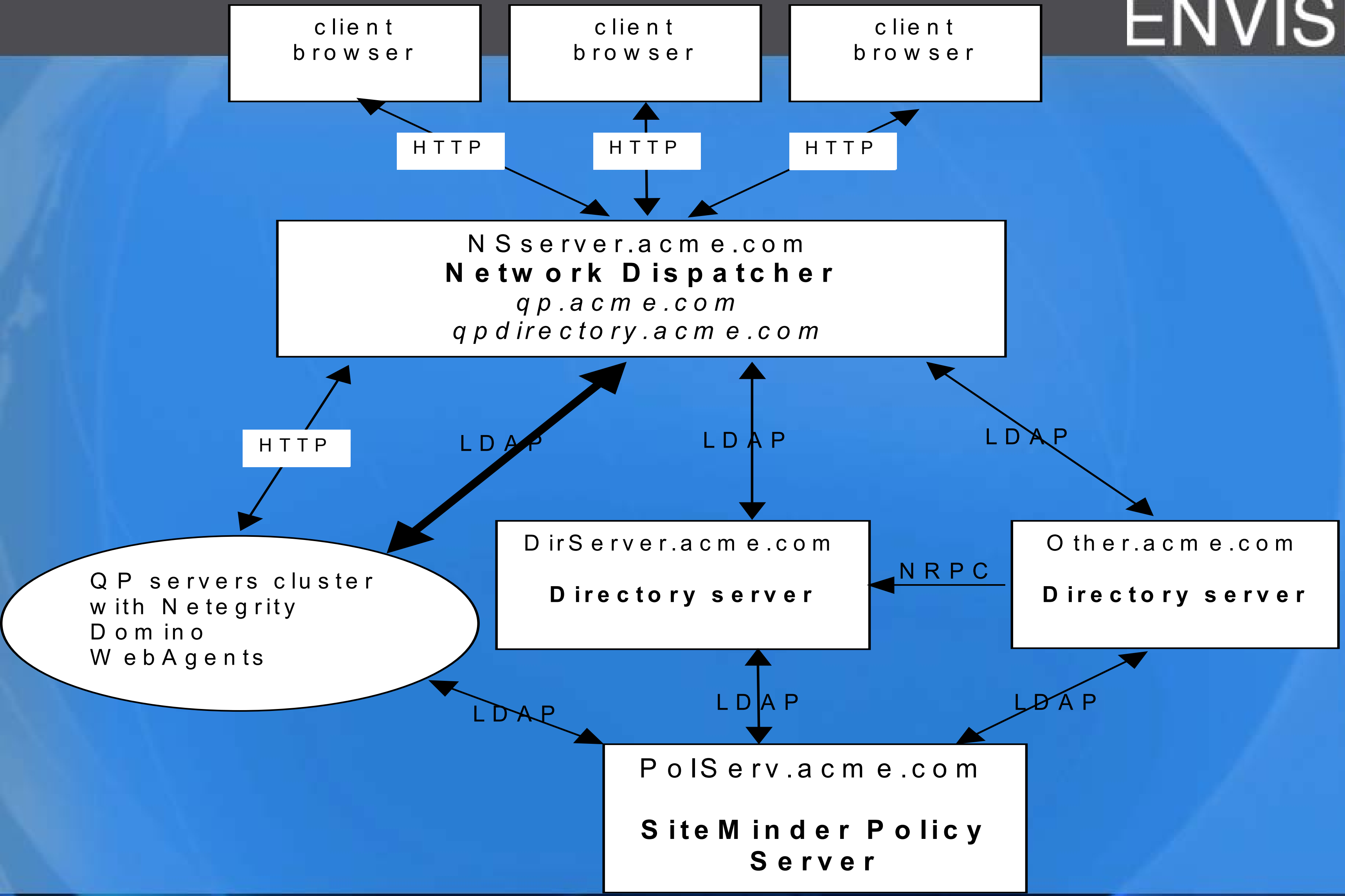
- Changing the display name be changed to be other than the notesmail value?
  - The default display name value can be changed from cn to notesmail. However, if the Person documents have not been updated to include a value for this attribute, users will not be able to login to the Sametime server. To make this change, you will need to open the stconfig.nsf, go to the LDAPserver document, and modify the People field:
    - The attribute of the person entry that defines the internal ID of a Sametime user: The attribute of the person entry that defines the person's name: notesmail.

Sametime and Active Directory

- **After creating the DA database….**
  - **DA by default requires binding and it must follow the format**
    - **Username**: cn=Username, cn=users, dc=domain, dc=com
  - Open stconfig.nsf and modify LDAP values
  - Make sure to verify the proper search filters for use with Active Directory
    - See technote #7002961

LDAP and Quickplace

- The QuickPlace configuration file, QPCONFIG.XML, in section User_Directory/LDAP/Schema, allows you to map specific LDAP attributes
  - However it is not possible to map additional attributes outside of what is found in the qpconfig.xml file



client browser

client browser

client browser

HTTP

HTTP

HTTP

NSserver.acme.com
Network Dispatcher
qp.acme.com
qpdirectory.acme.com

HTTP

LDAP

LDAP

LDAP

QP servers cluster
with Netegrity
Domino
WebAgents

DirServer.acme.com
Directory server

NRPC

Other.acme.com
Directory server

LDAP

LDAP

LDAP

PolServ.acme.com
SiteMinder Policy Server

LDAP and IBM Workplace™

- In Portal 5.1+ and Workplace 2.5, the LDAP Connection Wizard enables security and configures WAS for LDAP (command line still available)

Mapping Websphere Member Manager

If your directory server is...	Take these actions before starting Lotus Workplace for the first time...
IBM Directory Server 4.1	**No action required.**
IBM Directory Server 5.1	**Map the extId attribute to ibm-entryUUID and disable id generation.**
Microsoft Active Directory 2000	**Disable id generation.**
Novell eDirectory	**Map the extId attribute to GUID and disable id generation.**
Sun ONE Directory Server	**Map the extId attribute to nsuniqueid and disable id generation.**

LDAP and Websphere Portal

- The default set-up of Portal does not take into account read-only LDAP directories
- When installing Portal <5.1 or Workplace <2.5:

  wpconfig enable-security-ldap

  enables WAS security and sets LDAP config

LDAP and Websphere Portal

- Portal does not perform user authentication directly against LDAP – WAS does
- Portal does not have official support for LDAP clustering through Websphere Member Manager but it can be done transparently.
  - Technote #1193874

Source: Steven Power of IBM

LDAP and Websphere Portal

- However, Portal is still active against LDAP:
  - Returns user data
  - Can update some user data (e.g., password)
  - Can even create users in LDAP directory if so configured
  - Write-back functions are often not permissible – if not, be sure to remove links to self-service functions:
    - Sign up
    - Password maintenance

Websphere Portal and Active Directory

- If you use Microsoft Active Directory as the LDAP server in a WebSphere Portal environment, directory searches based on the objectClass attribute may not provide best performance, depending on which attribute you use.
- Use objectCategory instead of objectClass to improve MS Active Directory performance. To make use of objectCategory, the LTPA authentication of WebSphere Application Server and the directory search of WebSphere Portal must be adjusted.
  - WAS Admin Console changes required! 1158200

Portal and Workplace LDAP Defaults

LDAP Server:	LDAP Suffix:	User Prefix:	User Suffix:	Group Suffix:
IDS	dc=acme,dc=com	uid	cn=users	cn=groups
Domino	(blank)	cn	o=acme.com	(blank)
MS AD	dc=acme,dc=com	cn	cn=users	cn=groups
SunOne	o=acme.com	uid	ou=people	ou=groups
eDir	o=acme.com	uid	ou=people	ou=groups

Source: Steven Power of IBM

One More Set of Defaults

LDAP Server:	User objectClass:	Group objectClass:	Group Member:	User Filter Attributes:
IDS	inetOrgPerson	groupOfUniqueNames	uniqueMember	uid
Domino	inetOrgPerson	groupOfNames	member	cn, uid
MS AD	user	group	member	cn,samAccountName
SunOne	inetOrgPerson	groupOfUniqueNames	uniqueMember	uid
eDir	inetOrgPerson	groupOfNames	uniqueMember	uid

Source: Steven Power of IBM

LDAP inside of Domino

- Get slides for ID113 for some great opening remarks on Domino and LDAP
- A common schema is the most important part of the configuration Domino enforces
    - The administration server controls the enforcement of the master schema (note the wildcard configuration doc)

LDAP inside of Domino

- Notes.ini variables
  - Schema_Daemon_Reloadtime=number of hours
  - DisableLDAPOnAdmin=1
    - (don’t ever use this if you plan on using LDAP in your environment or change your administration server)

LDAP Inside of Domino

- Can I remap Domino Directory fields to alternate LDAP attributes?
  - Not supported or recommended
  - You should create custom attribute tags and refer directly to those. They may be similar in name but may never match an existing attribute
  - Any LDAP server must have a consistent reference point for accessing directory data

What Does Tivoli Do Anyway?

- IBM Tivoli Directory Integrator has the ability to detect password changes, when a password is changed or created through the use of plug-ins. Directory Integrator can detect password changes for IBM Directory Server, SunOne Directory Server, and IBM Lotus Domino HTTP passwords. The Password Synchronizer for Windows intercepts password changes of user accounts on Windows NT, Windows 2000, and Windows XP operating system.

Summary

- Plan a testing period of various LDAP directory servers
- Plan a security model to allow LDAP lookups without sacrificing unauthorized access
- Plan a consistent schema across everything being integrated
- Plan an architecture that supports scaling, with consideration of management

Thank you for attending!!!

Blogging at
http://www.IdoNotes.com

AOL IM: IdoNotes

Email
IdoNotes@netscape.net