Active Directory at the University of Michigan

Data Population and Kerberos Interoperability

presented at the Internet 2 Early Adopters Workshop
November, 2000

MaryBeth Stuenkel  maryb@umich.edu
LAN/NOS/Groupware Services  www.umich.edu/~lannos/win2000
Existing Infrastructure

- Uniqname – every faculty, staff, student assigned a unique 3-8 character identifier
- OpenLDAP enterprise directory
- MIT Kerberos user identity
  - based on uniqname
  - used for directory maintenance, email, IFS filespace
- DNS Structure based upon University Organizational Chart (governed by policy)
W2K Implementation Goals

- Provide an infrastructure that allows for distributed administration within a single forest infrastructure
- Enable transparent user access to resources throughout campus
- Automatically populate AD with data from enterprise directory
- Provide single signon via Kerberos
- Integrate with existing BIND DNS infrastructure
Structure of U-M Active Directory Forest

Forest Root
adsroot.itcs.umich.edu

Engin Tree
ad.engin.umich.edu

Other Tree
xx.yy.umich.edu

OU=People

OU=UMich

OU=Organizations

Campus Tree
ads.itcs.umich.edu

Departmental OUs
Populating Active Directory

- OpenLDAP directory entries update AD
  - Initial feed/bulk load
  - Automatic updates of changes and new entries
  - Out-of-band updates
- Schema mapping
- Mapping of W2K user principle to MIT realm
- Updates are one-way only, changes made in AD are never passed back to OpenLDAP
Updating AD User Entries from the U-M OpenLDAP Directory

Stage 1: Initial Feed / Bulk Load of Active Directory

Various Authoritative Data Services
  add, rename, change, delete User

User change self

OpenLDAP Master/Slave
  Extract Program
  U-M Directory (LDAP)
  U-M Directory LDIF Extract

Windows 2000 Member Server
  LDIF Transform Program
  Filter Students, Faculty and Staff
  Use U-M uniqname as CN of User's AD Distinguished Name
  User Attribute Mapping
  some multi-values to single-valued
  Some attributes won't map, i.e. address
  W2k user principal to MIT Kerberos principal

Windows 2000 Domain Controller
  Active Directory

approximately 110,000 User objects in OU=People,OU=UMICH
C:\WINNT\system32\ldifde.exe /? for help
parallel departmental OU=Organizations, OU=UMICH contains
partial organizational hierarchy, for delegated OUs

Mary Beth Stuenkel
maryb@umich.edu
http://www.umich.edu/~lannos/win2000

Various Campus Administrators
  add, rename, change, delete User

LDIFDE Bulk Update Utility
Updating AD User Entries from the U-M OpenLDAP Directory

Stage 2: Continuous Update of Active Directory

OpenLDAP Master

```
| "slapd" LDAP daemon          |
| U-M Directory (master)       |
| Replication Log             |
| "slurpd" replication daemon |
```

Windows 2000 DC 1

Active Directory

```
AD replication is peer-to-peer, so any DC in W2k domain may be used for replication.

AD schema extension attribute umichAdUMDirToADSyncFlag set to keep track of user add/change/delete operations from U-M Dir.

Possible to track U-M Dir --> AD changes with W2k service.

Updates are one-way, U-M Dir to AD.
```

OpenLDAP Slave

```
| replication "slapd" LDAP daemon |
| U-M Directory (copy)            |
| Replication Log                 |
| modified "slurpd" replication daemon |
```

Windows 2000 DC 2

Active Directory

```
```

Modified "slurpd" reads replication log for add/change/delete user events.

At this time, the Common Name (CN) attribute must be translated to a U-M unique. Example: "DN: CN=Babs Jensen, OU=herOrg,..." to "DN: CN=bjensen,OU=People,..."

LDAP multi-valued attribute order not defined, so splitting U-M Dir multi-valued to multiple AD attributes results in arbitrary assignment of "primary" AD attribute value. Example: telephonenumber ==> telephonenumber and otherTelephonenumber(s)

LDAP authentication to AD via Kerberos SASL based mechanism (GSSAPI).

W2k LDAP and kpassword service discovery via DNS SRV records. To add AD user, first bind to any W2k DC, add user via LDAP, set random password on same W2k DC via Kerberos, then reset userAccountControl attribute on same W2k DC to "password never expires" via LDAP.

Switch to new W2k DC only upon slurpd startup, or failure (network, timeout, W2k DC failure, etc.)
<table>
<thead>
<tr>
<th>Attribute</th>
<th>IDAPDisplayName</th>
<th>Require</th>
<th>isSingle</th>
<th>Mapped from:</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>nDAPDisplayName</td>
<td>require</td>
<td>TRUE</td>
<td>uid + path (cn=bjensen,ou=people,ou=umich,dc=...)</td>
</tr>
<tr>
<td>Common-Name</td>
<td>dn</td>
<td>yes</td>
<td>N/A</td>
<td>uid</td>
</tr>
<tr>
<td>User-Principal-Name</td>
<td>userPrincipalName</td>
<td>yes</td>
<td>TRUE</td>
<td><a href="mailto:uniqname@umich.edu">uniqname@umich.edu</a> (<a href="mailto:bjensen@umich.edu">bjensen@umich.edu</a>)</td>
</tr>
<tr>
<td>SAM-Account-Name</td>
<td>sAMAccountName</td>
<td>yes</td>
<td>TRUE</td>
<td>uid (bjensen)</td>
</tr>
<tr>
<td>Alt-Security-Identities</td>
<td>altSecurityIdentities</td>
<td>FALSE</td>
<td></td>
<td>Kerberos:<a href="mailto:uid@umich.edu">uid@umich.edu</a> (<a href="mailto:Kerberos.bjensen@umich.edu">Kerberos.bjensen@umich.edu</a>)</td>
</tr>
<tr>
<td>Display-Name</td>
<td>displayName</td>
<td>TRUE</td>
<td></td>
<td>cn (Babs Jensen)</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
<td>FALSE</td>
<td></td>
<td>use AD displayName, derived from cn</td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td>TRUE</td>
<td></td>
<td>sn</td>
</tr>
<tr>
<td>Title</td>
<td>title</td>
<td>TRUE</td>
<td></td>
<td>1st value of title</td>
</tr>
<tr>
<td>E-mail-Addresses</td>
<td>mail</td>
<td>TRUE</td>
<td></td>
<td>1st value of mail</td>
</tr>
<tr>
<td>Other-Mailbox</td>
<td>otherMailbox</td>
<td>FALSE</td>
<td></td>
<td>all mail values after first</td>
</tr>
<tr>
<td>Telephone-Number</td>
<td>telephoneNumber</td>
<td>TRUE</td>
<td></td>
<td>1st value of telephonenumber</td>
</tr>
<tr>
<td>Phone-Office-Other</td>
<td>otherTelephone</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of telephonenumber</td>
</tr>
<tr>
<td>Phone-Home-Primary</td>
<td>homePhone</td>
<td>TRUE</td>
<td></td>
<td>1st value of homephone</td>
</tr>
<tr>
<td>Phone-Home-Other</td>
<td>otherHomePhone</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of homephone</td>
</tr>
<tr>
<td>Phone-Mobile-Primary</td>
<td>mobile</td>
<td>TRUE</td>
<td></td>
<td>1st value of mobile</td>
</tr>
<tr>
<td>Phone-Mobile-Other</td>
<td>otherMobile</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of mobile</td>
</tr>
<tr>
<td>Phone-Pager-Primary</td>
<td>pager</td>
<td>TRUE</td>
<td></td>
<td>1st value of pager</td>
</tr>
<tr>
<td>Phone-Pager-Other</td>
<td>otherPager</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of pager</td>
</tr>
<tr>
<td>Facsimile-Telephone-Number</td>
<td>facsimileTelephoneNumber</td>
<td>TRUE</td>
<td></td>
<td>1st value of facsimileTelephoneNumber</td>
</tr>
<tr>
<td>Phone-Fax-Other</td>
<td>otherFacsimileTelephoneNumber</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of facsimileTelephoneNumber</td>
</tr>
<tr>
<td>WWW-Home-Page</td>
<td>WWWHomePage</td>
<td>TRUE</td>
<td></td>
<td>1st value of labeledurl</td>
</tr>
<tr>
<td>WWW-Page-Other</td>
<td>url</td>
<td>FALSE</td>
<td></td>
<td>2nd to Nth values of labeledurl</td>
</tr>
<tr>
<td>umichad-OU</td>
<td>umichadOU</td>
<td>FALSE</td>
<td></td>
<td>ou</td>
</tr>
<tr>
<td>umichad-Role</td>
<td>umichadRole</td>
<td>FALSE</td>
<td></td>
<td>An index &quot;role&quot; attribute, taken from last part of ou values</td>
</tr>
<tr>
<td>umichad-No-Batch-Updates</td>
<td>umichadNoBatchUpdates</td>
<td>TRUE</td>
<td></td>
<td>nobatchupdates</td>
</tr>
<tr>
<td>umichad-Dir-Sync</td>
<td>umichadUMDirToADSyncFlag</td>
<td>FALSE</td>
<td></td>
<td>2 = user added, 4 = user changed, 8 = delete user, 16 = modrdn</td>
</tr>
<tr>
<td>umichad-No-Batch-Updates</td>
<td>umichadNoUMDirUpdates</td>
<td>TRUE</td>
<td></td>
<td>set in Windows 2000</td>
</tr>
</tbody>
</table>
Populating Active Directory

Still left to do:

- Making use of umichadUMDirToADSyncFlag to log/track user add/change/delete operations from OpenLDAP
- Implementing out-of-band updates to OpenLDAP
  - Changes in formats of data feeds
  - Changes to schema of OpenLDAP
- Testing and move to production
Kerberos Interoperability

- **Process**
  - User presents Kerberos username and password and receives MIT initial ticket granting ticket (TGT)
  - User receives MIT service TGT from MIT KDC
  - User receives ADS service TGT from MIT KDC
  - User uses ADS TGT to request LDAP service ticket from AD KDC

- **Details**
  - Kerberos v5, release 1.2.1
  - Kerberos passwords NOT synced with AD passwords, AD password not known by user
  - One-way trust only, AD trusts MIT
Windows 2000 User Login at U-M (simplified)

Login Sequence:

1. Babs enters her U-M uniqname and password.
   W2k login program requests initial ticket granting ticket from MIT KDC.
   MIT KDC sends initial ticket granting ticket:
   krbtgt/UMICH.EDU@UMICH.EDU
   Flags: Initial, Forwardable, Renewable
   Encryption types: ticket: DES-CBC-CRC  key: DES-CBC-MD5

2. W2k login program requests service ticket granting ticket from MIT KDC.
   MIT KDC sends service ticket granting ticket:
   krbtgt/UMICH.EDU@UMICH.EDU
   Flags: Forwarded, Forwardable, Renewable
   Encryption types: ticket: DES-CBC-CRC  key: DES-CBC-MD5

3. W2k login program requests service ticket granting ticket from MIT KDC.
   MIT KDC sends service ticket granting ticket:
   krbtgt/ADS.ITCS.UMICH.EDU@UMICH.EDU
   Flags: Forwardable, Renewable
   Encryption types: ticket: DES-CBC-CRC  key: DES-CBC-MD5

4. W2k login program requests LDAP service ticket from W2k ADS.ITCS.UMICH.EDU domain.
   LDAP/adscd01.ads.itcs.umich.edu@ads.itcs.umich.edu
   Flags: OK-as-delegate, Forwardable, Renewable
   Encryption types: ticket: RSADSI RC4-HMAC  key: RSADSI RC4-HMAC

User object in Active Directory:

Dn: CN=bjensen,OU=People,OU=UMICH,DC=ads,DC=itcs,DC=umich,DC=edu
altSecurityIdentities: Kerberos:bjensen@UMICH.EDU
sAMAccountName: bjensen
userPrincipalName: bjensen@umich.edu
(note: umich.edu suffix to a U-M convention)
description: Babs Jensen
(note: U-M convention to place full name in description, for snap-in visibility)
objectGUID: d44d67a4-9b91-4865-b920-5f10061190c
objectSid: S-1-5-68C8AA52-7FF55B87-462B383-329C3

User "Babs Jensen" logs on at W2k workstation
uniqname = bjensen
Member of "ads.itcs.umich.edu" W2k domain
bjensen@ads.itcs.umich.edu
Member of "umich.edu" Kerberos realm
bjensen@umich.edu
Chooses "UMICH.EDU (Kerberos Realm) from W2k "Log on to" drop-down menu
Kerberos Interoperability

Existing challenges

– Applying group policy to users in People OU via loopback processing on computers not working for MIT KDC-authenticated users
– Preventing namespace collisions with current and future uniqnames through user objects created by departmental OU admins
– What about non-Kerberos supported clients?
Summary

- **Existing infrastructure**
  - Both a challenge and an enabler
  - Has provided a rich environment for collaboration

- **Automatic data population**
  - Coding for initial feed and automatic updates complete
  - Logging changes to AD, coding for out-of-bound updates and more testing to do

- **Kerberos interoperability**
  - Authentication via MIT KDC working
  - Biggest current issue – loopback processing on group policies applied to computer objects
Credits

- Andrew Wilson
- Dave Detlefs
- Paul Turgyen
- Other UMCE staff

- Technical Lead
- Windows Developer
- Web site Developer
- LDAP Developer
- Kerberos Integration
- DNS Integration
- Directory Integration

w2k.support@umich.edu
www.umich.edu/~lannos/win2000