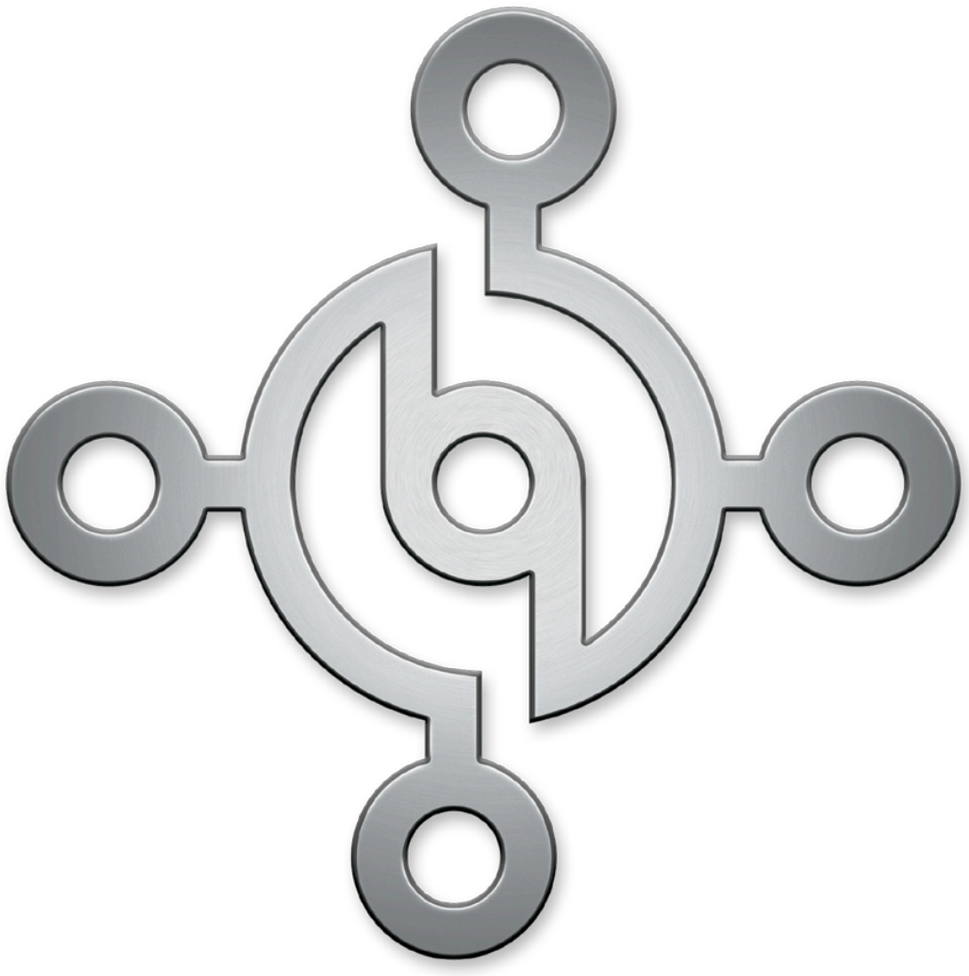
Integrating MacOS X with Novell eDirectory

James Partridge
OUCS
4 February 2005

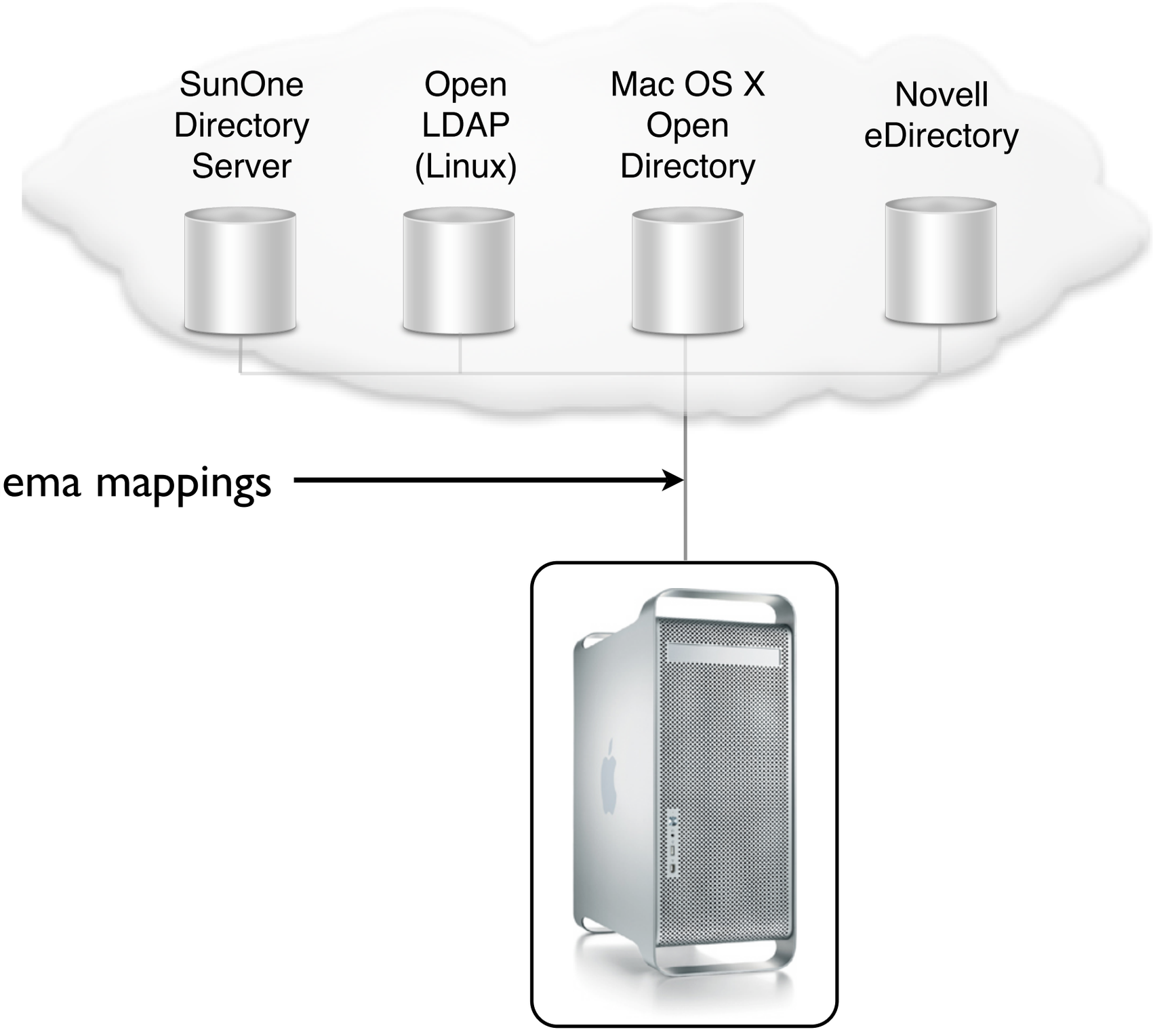
The Problem:

How to integrate Macs into Novell (and other) directory services

Directory Services Architecture

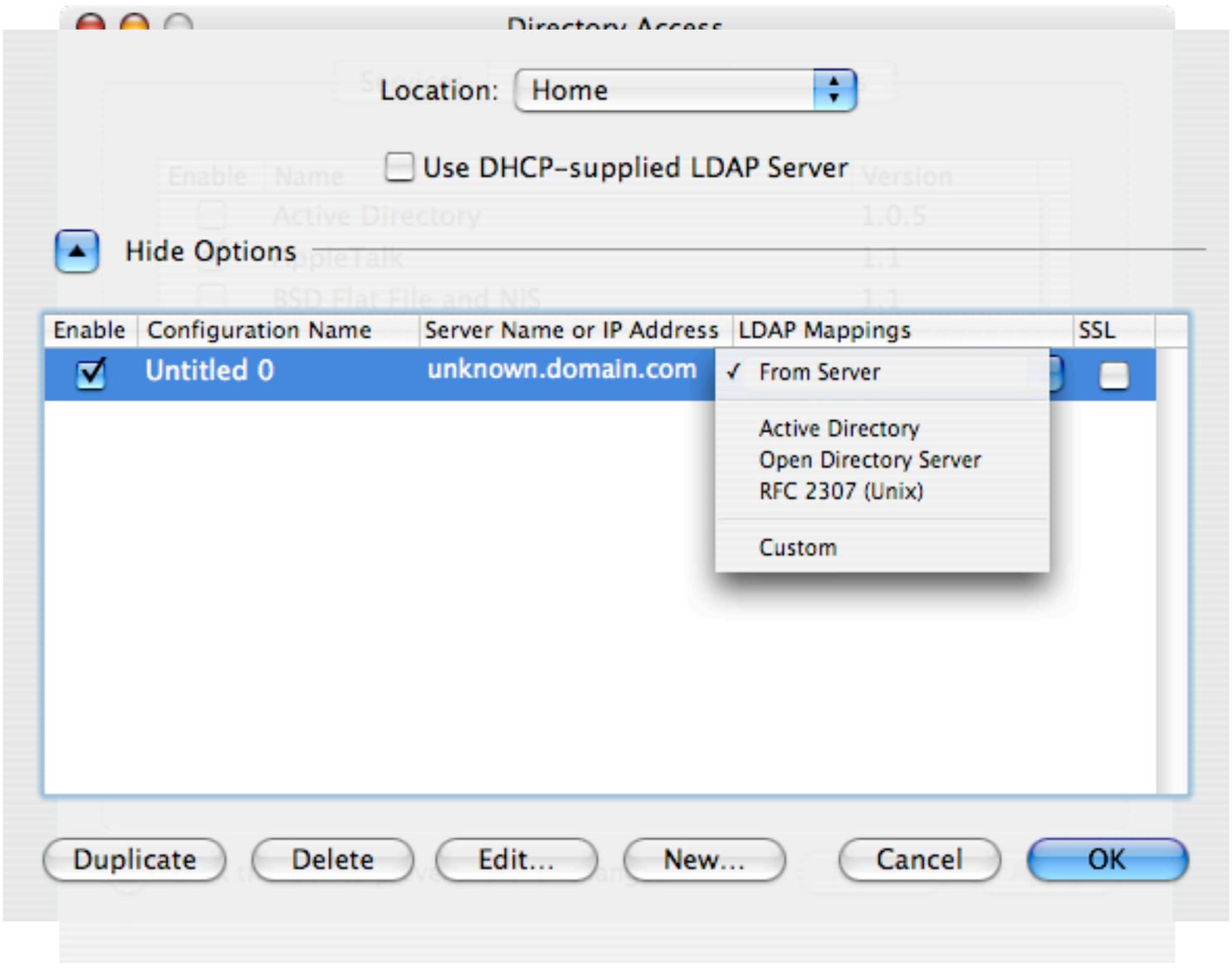


- MacOS X directory services architecture fully supports LDAP (as well as Apple's own Netinfo directory)
- Native plugins provided for:
  - Active Directory (Windows)
  - Open Directory (OSX)
  - RFC 2307 (Unix)
  - Custom schema mappings (but NO native eDirectory plugin)


SunOne
Directory
Server
Open
LDAP
(Linux)
Mac OS X
Open
Directory
Novell
eDirectory
Schema mappings

Early attempts

eDirectory Integration



- No native eDir plug-in
- Must extend eDir schema to accommodate Macs
- Use LDAPv3 and custom mappings on the client

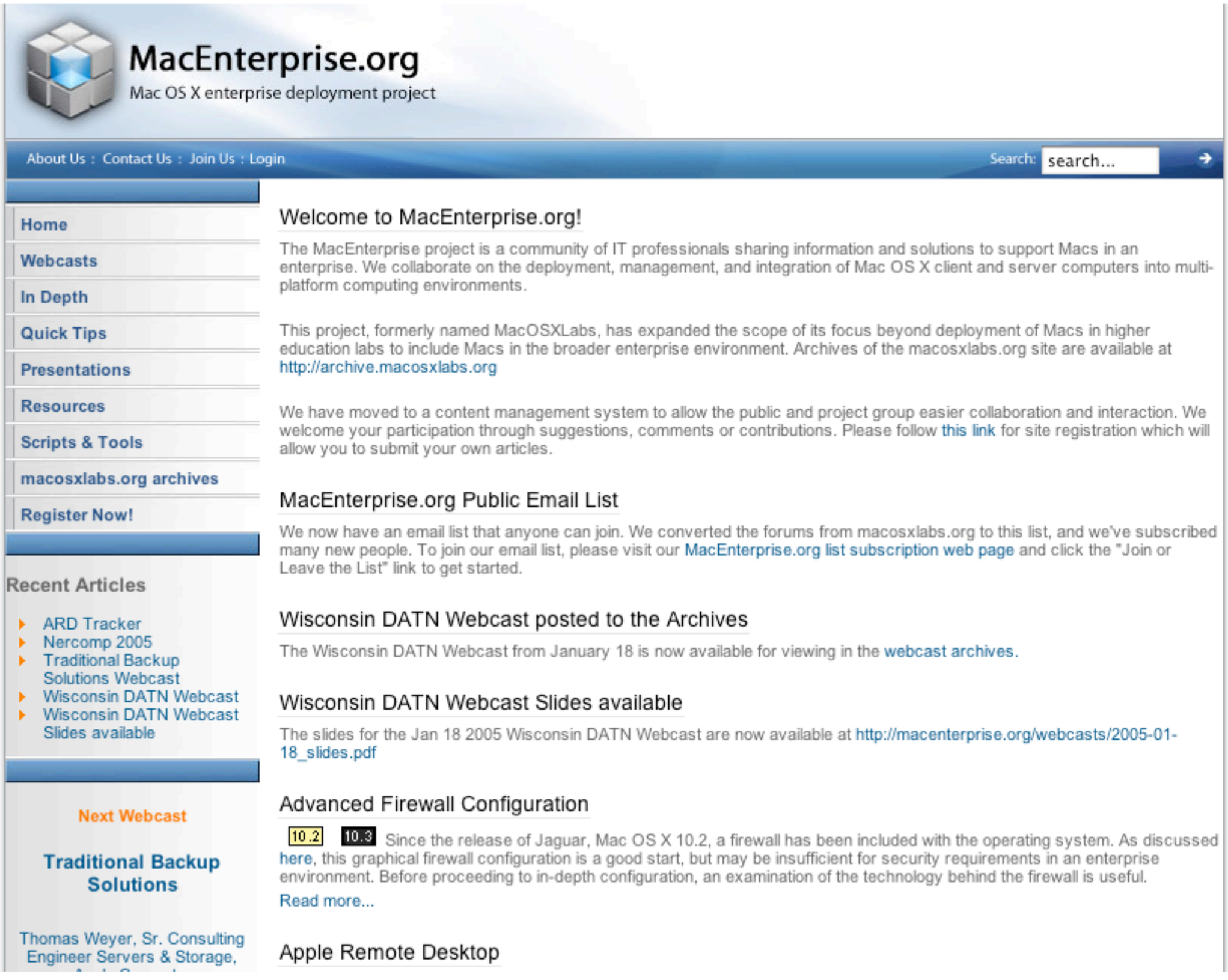
eDir Integration: The Procedure

- Extend schema (LDIF files are available for NW6 and NW6.5)
- Set user attributes
- Create mounts object
- Import server public certificate (for SSL connections) onto client Mac (convert from .der to .pem format)
- Directory Access for LDAP mappings
- Diagnose problems

Server Public Certificate

- Copy RootCert.der file from SYS:PUBLIC directory on NW server into folder on client Mac
- Open Terminal.app, navigate to folder and type: `openssl x509 -inform DER -outform PEM -in RootCert.der -out RootCert.pem`
- Create directory ‘certs’ in /Library, then sudo `cp [path]/RootCert.pem /Library/certs`
- cd /Library/certs, then: `sudo chown root:wheel RootCert.pem` and `sudo chmod 400 RootCert.pem`
- Add the following line to /etc/openldap/ldap.conf: `TLS_CACERT /Library/certs/RootCert.pem`

MacEnterprise.org



- Dan Sinema (Apple) has produced a package installer that adds a pre-configured eDirectory plugin
- Much easier; still needs a little bit of server-side configuration
  - schema extensions (using a supplied LDIF file)
  - AFP Mount objects
- Documentation has been updated
- See `http://macenterprise.org/content/view/80/77/` for details

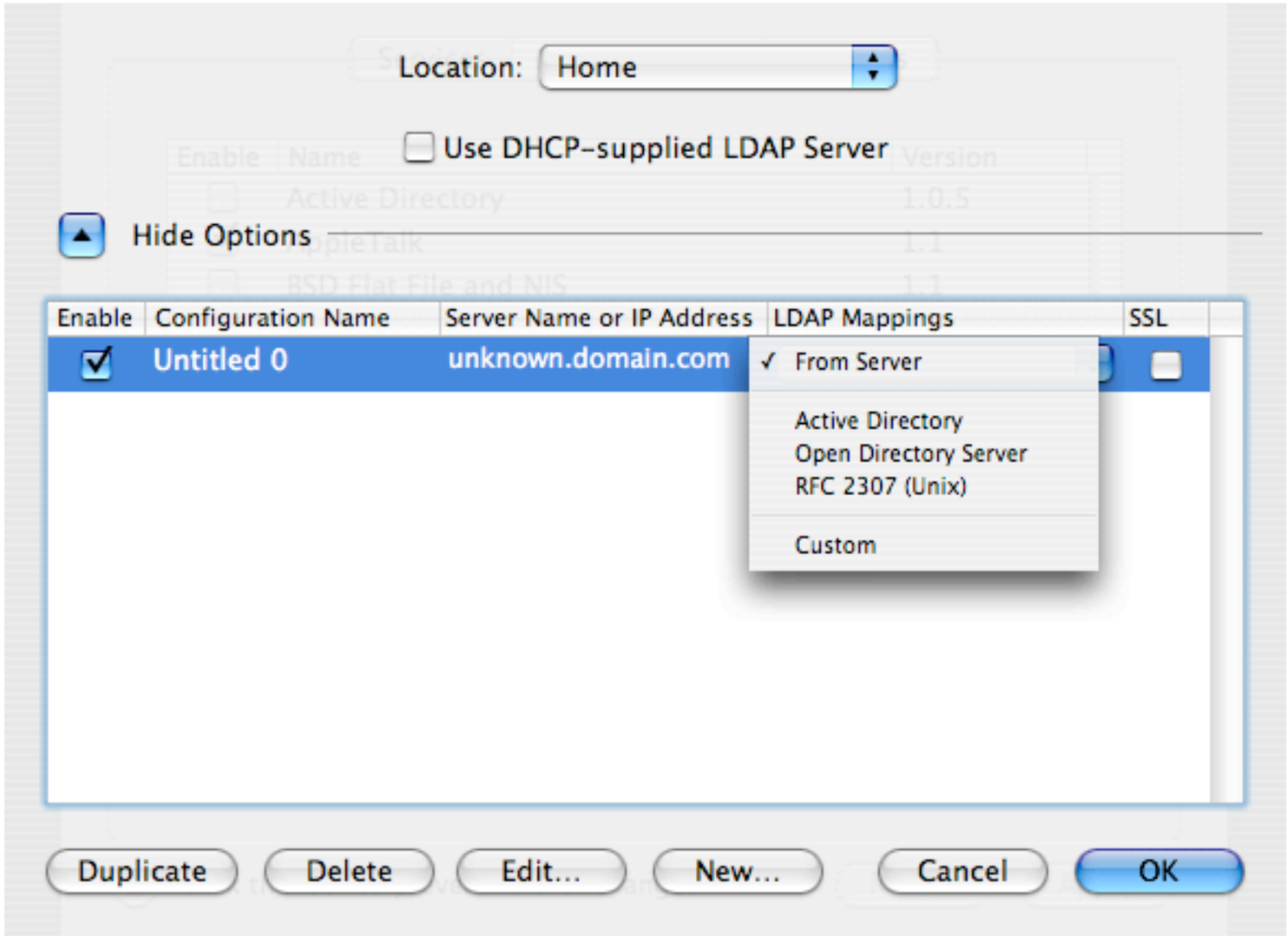
2.3.3 Mapping Listing

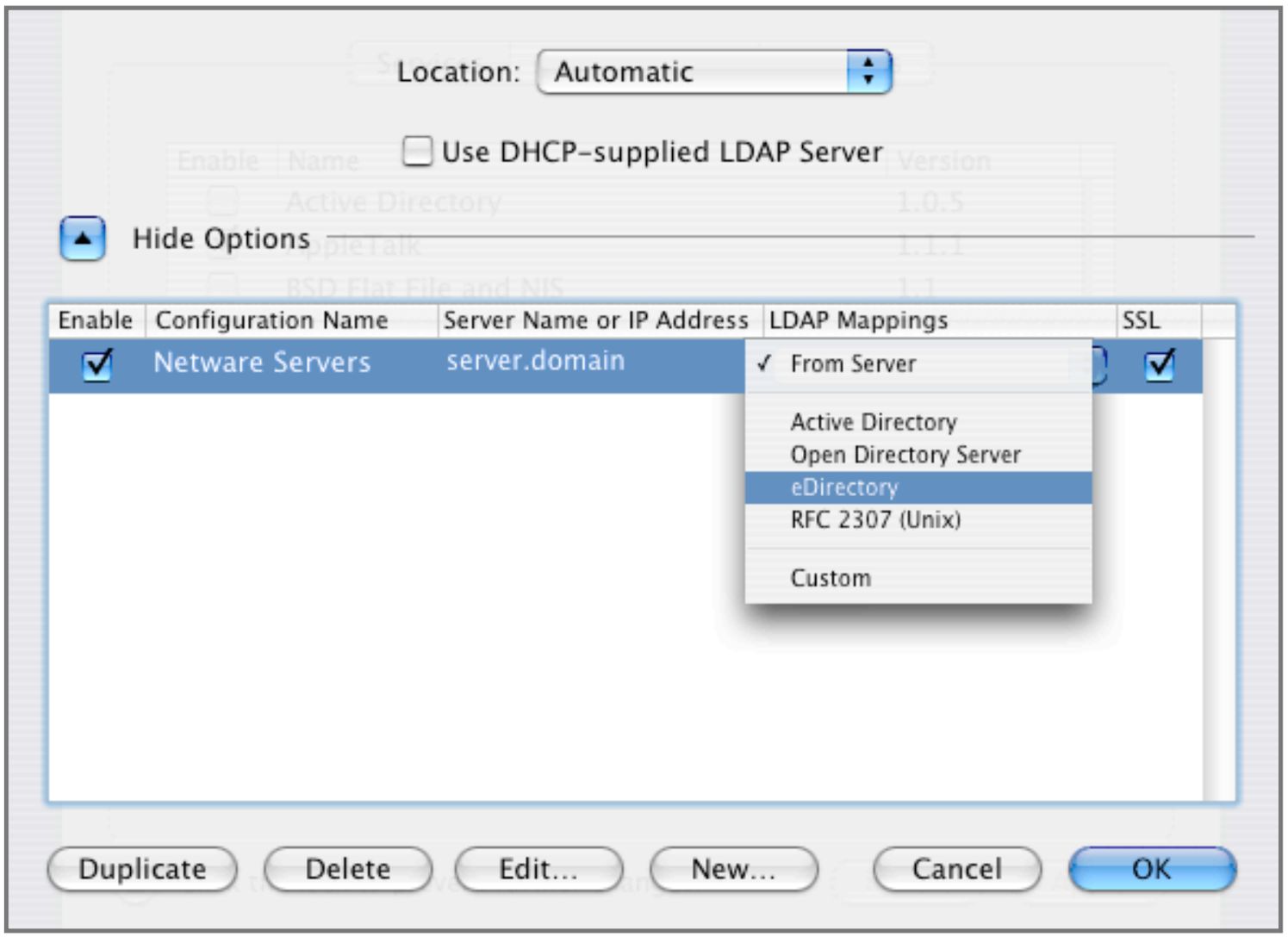
If Tables 1-3 is used for manual mapping discussed in Section 2.3.2 then the table should be read as follows. The “Mac OS X” value should be used to select values for the left hand side of the Mappings screen of the LDAPv3 plug-in in Directory Access. The “eDirectory” value should be used for the values on the right hand side of the Mappings screen of the LDAPv3 plug-in in Directory Access.

User Objects			
Record Types / Object Class			
Mac OS X	**EDirectory**	**Required**	**ConsoleOne Screen**
User	**InetOrgPerson, apple-user**	**X**	**N/A**
Attribute Types / Attributes			
Mac OS X	**eDirectory**	**Required**	**ConsoleOne Screen**
RecordName	**uid** **cn**	**X**	**General**
RealName	**fullName** **cn**	**X**	**General**
UniqueID	**uidNumber**	**X**	**UNIX Profile**
PrimaryGroupID	**gidNumber**	**X**	**UNIX Profile**
NFSHomeDirectory	**homeDirectory** **Or** **apple-user-homeDirectory**	**X**	**UNIX Profile** **apple-user-homeDirectory can be found in the Other tab**
HomeDirectory	**apple-user-homeurl**	**X****	

Figure 1

**** If you are mounting home directories with NFS then this value is not required**


Location: Home
Use DHCP-supplied LDAP Server
Hide Options
Enable
Configuration Name
Server Name or IP Address
LDAP Mappings
SSL
Untitled 0
unknown.domain.com
From Server
Active Directory
Open Directory Server
RFC 2307 (Unix)
Custom
Duplicate
Delete
Edit...
New...
Cancel
OK



Directory Access after installing the new eDirectory plugin

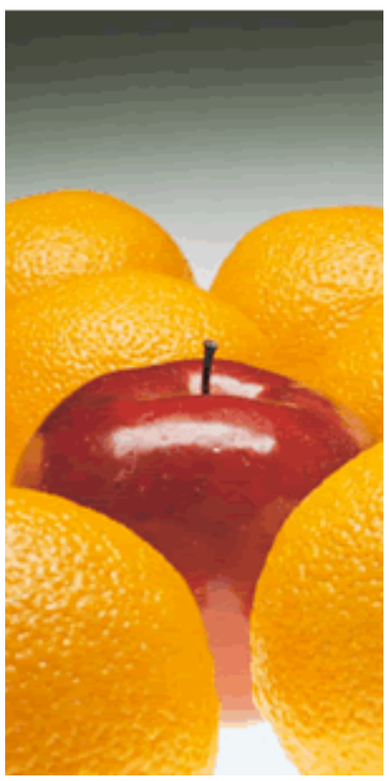
DSCL on MacOS X

```
Computer:~ computer$ dscl localhost
/ > cd LDAPv3/
/LDAPv3 > cd netware.apple.edu/
/LDAPv3/netware.apple.edu > ls
Config
Groups
Mounts
People
Users
/LDAPv3/netware.apple.edu > cd Users/
/LDAPv3/netware.apple.edu/Users > cd ktracy
/LDAPv3/netware.apple.edu/Users/KTracy > read
ACL: 2#subtree#cn=KTracy,ou=SLC,o=DA#[All Attributes
Rights] 6#entry#cn=KTracy,ou=SLC,o=DA#loginScript
2#entry#[Public]#messageServer
2#entry#[Root]#groupMembership
6#entry#cn=KTracy,ou=SLC,o=DA#printJobConfiguration
2#entry#[Root]#networkAddress
7#entry#cn=KTracy,ou=SLC,o=DA#iFolderServerName
cn: KTracy
eMailAddress: 7#KTracy@DA.PO
facsimileTelephoneNumber: 555-1235
fullName: Kimberly Tracy
givenName: Kimberly
groupMembership: cn=Everyone,ou=GW65,ou=Services,o=DA
iFolderServerName: *
l: Salt Lake City
Language: ENGLISH
loginGraceLimit: 6
loginTime: 20040401185428Z
mail: Kimberly.Tracy@digitalairlines.com
messageServer: cn=NW65DA2,ou=Services,o=DA
ndsHomeDirectory:
cn=NW65DA2_SYS,ou=Services,o=DA#4#\users\KTracy
nGWFileID: qub
nGWGroupWiseID: DA.PO.KTracy{106}21BE9990-0528-0000-BFA2-
6D00D100D100
nGWObjectID: KTracy
nGWPostOffice: cn=PO,ou=GW65,ou=Services,o=DA
nGWVisibility: 2
```

http://www.condreyconsulting.com/production/PRODUCTS/Kanaka/Overview.htm

Kanaka (Condrey Consulting)

Kanaka

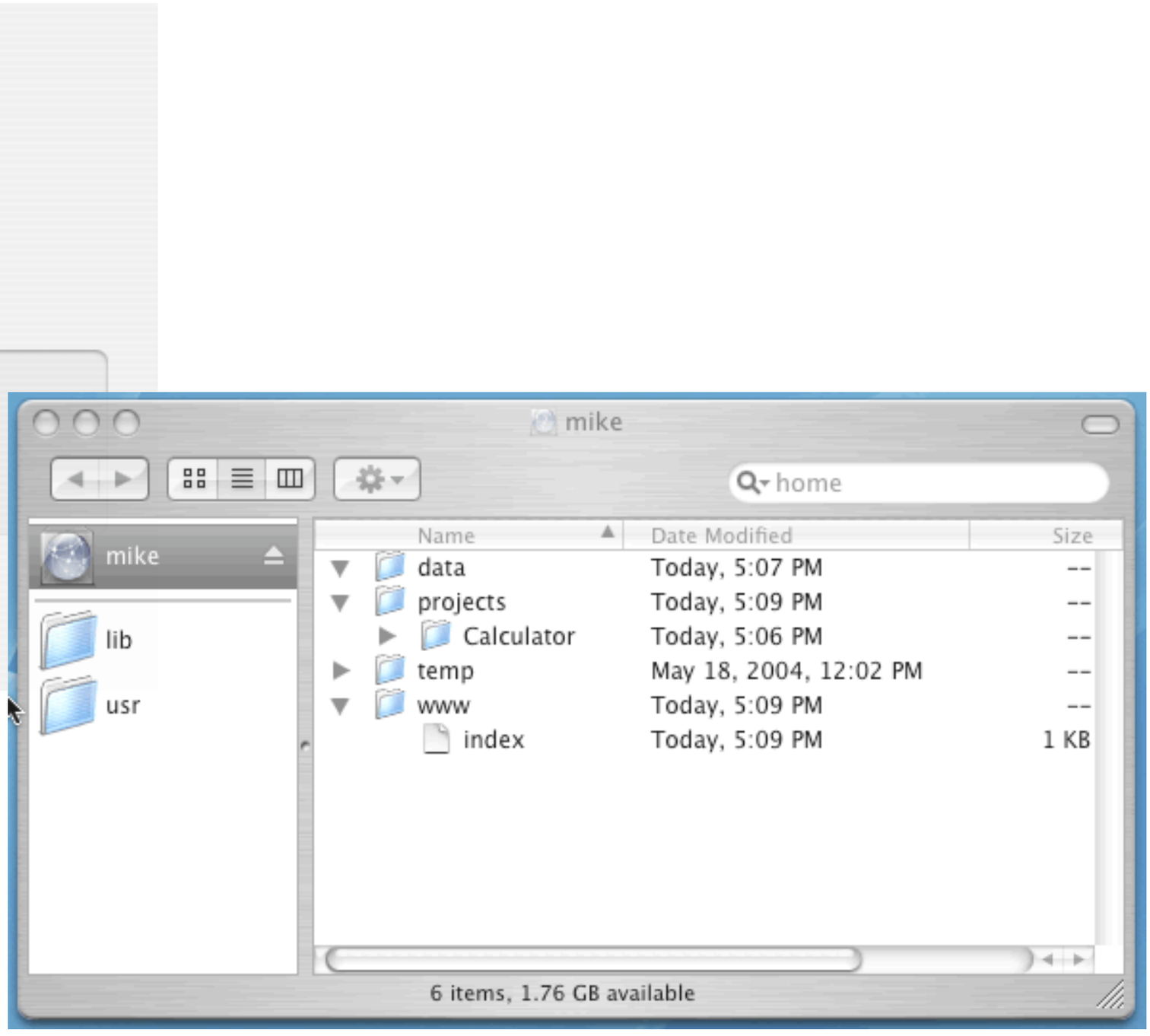


- Integrates with MacOS X log-in subsystem for contextless login on both OSX client and Novell network
- Uses LDAP to authenticate MacOS X clients to eDir
- Replaces manual configuration, schema extension
- Developed by Condrey Consulting in partnership with Apple & Novell

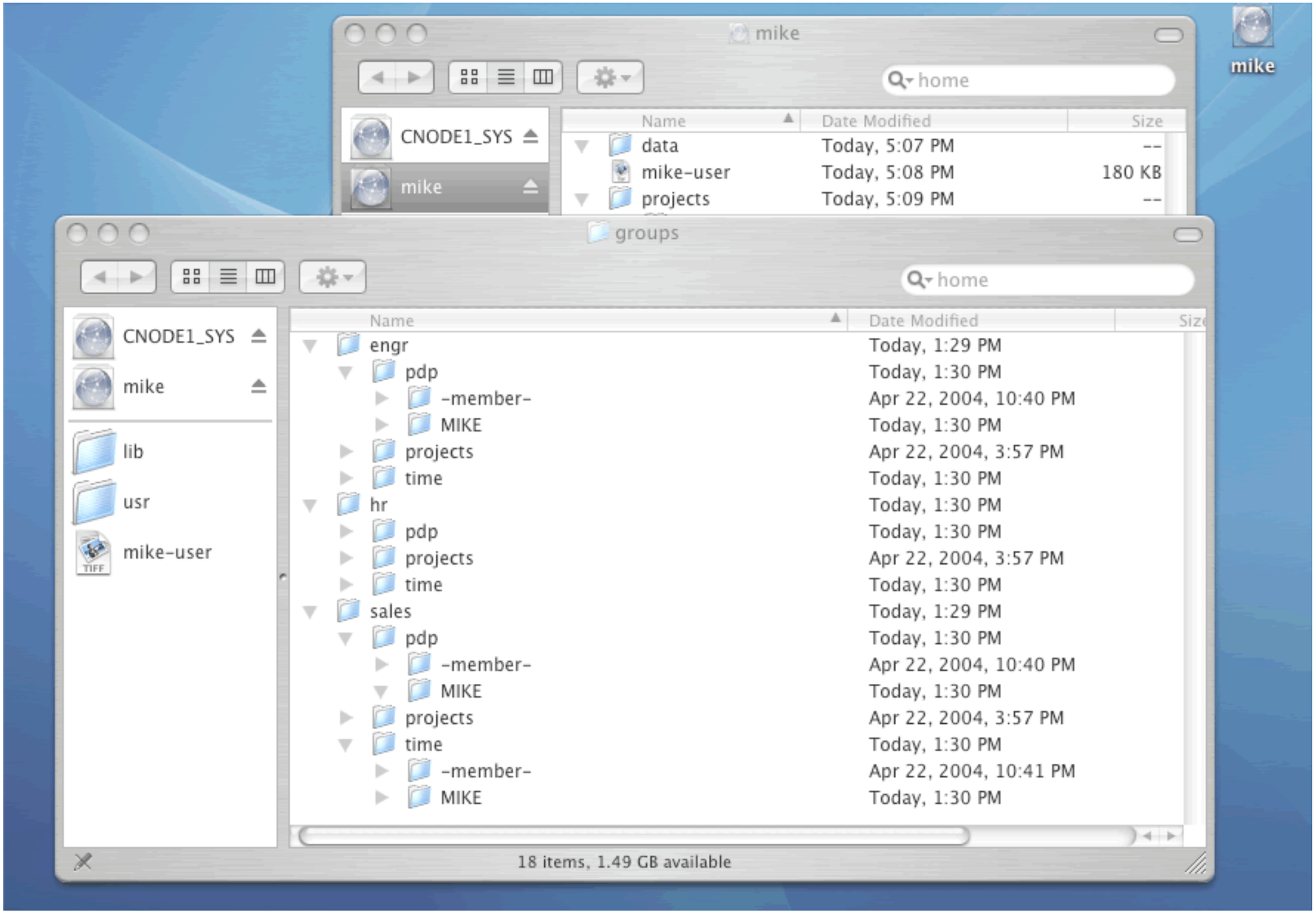
How it works

- After authentication, Kanaka discovers the user's home directory (and any other associated storage) and auto-mounts it
- Home directory location comes from the standard HomeDirectory attribute in eDirectory
  - No separate AFP attributes required
- No need for user to know location of storage
- No manual mapping required
- Users can use any client machine

Volume Mount (simple)



Volume Mount & Group Storage



Kanaka: Futures

- Still in closed beta
- We (OUCS) are one of the beta test sites and are actively working on Kanaka
- Still no indication of when Kanaka will be released, but hopefully later this year
- No indication of cost yet
- All the evidence suggests that Kanaka will be the main route for OSX integration with NetWare for the foreseeable future