

Configuring and Troubleshooting Active Directory Integration

Arek Dreyer, Principal - Dreyer Network Solutions &
Author - 10.6 Directory Services (Peachpit)

Expo: January 27-29 | Conference: January 26-29

Mike Reed, Practice Manager - Apple Solutions,
Forsythe Solutions Group

Agenda

- 10:00 - 10:15 Intro/Overview
- 10:15 - 11:00 Directory Service Architecture (AD/OD)
- 11:00 - 11:45 DNS
- 11:45 - 12:30 Kerberos
- 12:30 - 1:30 Lunch
- 1:30 - 2:15 Authentication/Authorization
- 2:15 - 3:00 Troubleshooting (Replication, Disjointed Namespace, etc.)
- 3:00 - 3:15 Break
- 3:15 - 4:45 Third Party Tools
- 4:45 - 5:00 Questions/Wrap-Up

Intro/Overview

The Basics of AD Integration

On the Windows side

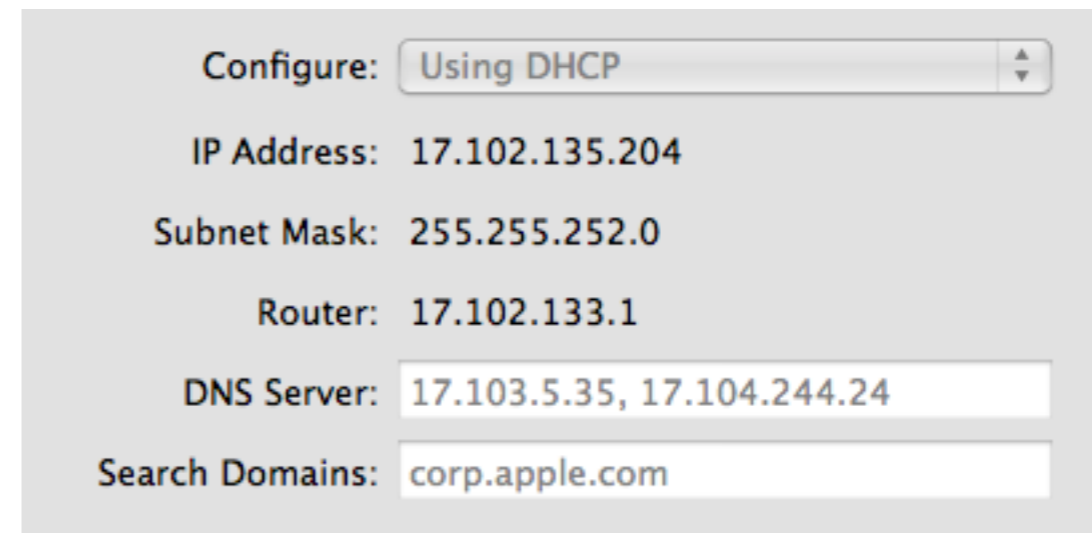
- Use a valid AD Domain Name
 - Underscores are NOT valid characters, but AD will allow them. This WILL BREAK OS X AD integration.

On the OS X side

- Configure Network Preferences
- Configure the AD Plugin
 - The more you customize AD, the more you should expect to configure the AD plugin.

Configuring Network Preferences

- DNS Server must be able to resolve AD service records
- Search Domains should contain, at a minimum, the AD domain name
- Entering .local is NOT required



The screenshot shows a network configuration window with the following settings:

Configure:	Using DHCP
IP Address:	17.102.135.204
Subnet Mask:	255.255.252.0
Router:	17.102.133.1
DNS Server:	17.103.5.35, 17.104.244.24
Search Domains:	corp.apple.com

Configuring the AD Plugin

- 'Prefer this domain server' requires that:
 - DC is listed in DNS
 - DC is in same AD Site
- AD Plugin may not respect choice in all circumstances (AD GC Node)
- 'Allow authentication from any domain...' should be enabled for troubleshooting purposes
 - KERBEROS: domain files

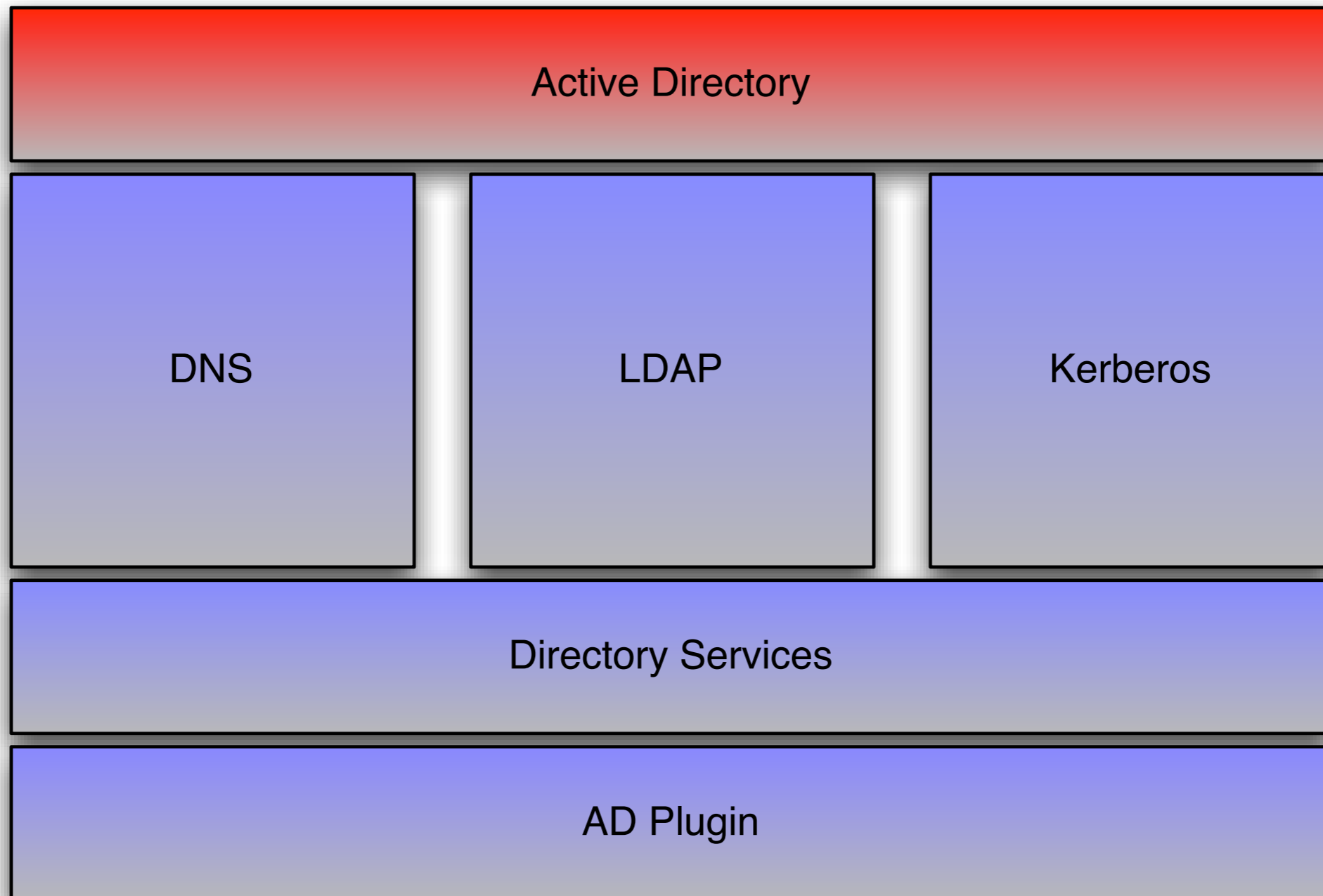
The screenshot shows the configuration dialog for the Active Directory plugin. At the top, there are three input fields: 'Active Directory Forest:', 'Active Directory Domain:', and 'Computer ID: mreed-mbp'. An 'Unbind...' button is located to the right of the 'Computer ID' field. Below these fields is a section titled 'Hide Advanced Options' with a downward-pointing arrow. Underneath, there are three tabs: 'User Experience', 'Mappings', and 'Administrative'. The 'Administrative' tab is selected. In this tab, there are three main options:

- Prefer this domain server: server.domain.forest.example.com. Below this is the text: 'This domain server will be used when available'.
- Allow administration by: A list box containing 'AD\domain admins' and 'AD\enterprise admins'. Below the list box are '+' and '-' buttons and the text: 'All members of these groups will have administrator privileges on this computer.'
- Allow authentication from any domain in the forest

At the bottom right of the dialog are 'Cancel' and 'OK' buttons.

Directory Service Architecture

OS X + AD in Snow Leopard



DirectoryService Debug Logging

- Directory Service Debug Logging
 - Has a “Level 7” flag that includes more information than typical DSDebug logging (USR1), but less than API logging (USR2)
 - <http://support.apple.com/kb/HT3186>
- Grepping & Tailing the DS logs:
 - `grep “Active Directory:” /Library/Logs/DirectoryService/DirectoryService.debug.log`
 - `tail -F /Library/Logs/DirectoryService/DirectoryService.debug.log | grep <...>`

DNS

AD & DNS

- Successful AD integration requires a healthy AD DNS implementation
- For those who don't know what is required, Microsoft documents what should show up in AD DNS:
 - <http://technet.microsoft.com/en-us/library/cc759550.aspx>
- What is required:
 - `_ldap` - tells us where the directory is
 - `_kerberos` - tells us where security is
 - `_kpasswd` - tells us where to change passwords
- Format is `_service._protocol.fqdn`
 - Example: `_ldap._tcp.example.com`

Troubleshooting DNS (Pt. I)

```
mreed-mbp:~ mreed$ dig -t SRV _ldap._tcp.example.com
```

```
; <<>> DiG 9.4.2-P2 <<>> -t SRV _ldap._tcp.example.com
```

```
:: global options: printcmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35092
```

```
:: flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2
```

```
:: QUESTION SECTION:
```

```
:_ldap._tcp.example.com.IN SRV
```

```
:: ANSWER SECTION:
```

```
_ldap._tcp.example.com. 600 IN SRV 0 100 389 dc.example.com.
```

```
_ldap._tcp.example.com. 600 IN SRV 0 100 389 dc2.example.com.
```

```
:: ADDITIONAL SECTION:
```

```
dc.example.com. 3600 IN A 192.102.132.85
```

```
dc2.example.com. 3600 IN A 192.102.132.160
```

```
:: MSG SIZE rcvd: 168
```

- Searching for `_ldap`, `_kerberos` and `_kpasswd` should return at least one answer each. If not, the problem is in the customer's AD DNS.
- Searching for `_ldap`, `_kerberos` and `_kpasswd` should return the same number of answers. If not, the problem is in the customer's AD DNS.

Troubleshooting DNS (Pt. 2)

- changeip -checkhostname
 - Validates forward and reverse lookups in DNS. If this has errors, we're likely to have problems in AD (OS X Server)
- Ping the AD domain name: AD typically registers an "A record" for the domain pointing to the first domain controller in the domain for Pre-Windows 2000 clients
- Ping the name and IP address of each AD domain controller
- Ping the OS X workstation/server by name and IP address from an AD domain controller

Kerberos

AD Security - Kerberos

- Requires time ~5m accuracy - USE NTP
- Every AD domain is a different Kerberos realm
- Moving away from edu.mit.Kerberos to /config
 - Can manually configure edu.mit.Kerberos for special situations, but not recommended as troubleshooting
 - If "disjointed", must create [domain_realm] rules for the client in the edu.mit.Kerberos file to map the realms to domains
 - ex: .subdomain.domain.com = REALM.DOMAIN.COM
 - Matching [capath] rules are also needed to enable the client to find the path
 - Alternatively, deslect "All Authentication from All Domains" and manually enter domains, which creates the proper realm files
- Verify principals with 'setspn -l machinename' on Windows (requires Support Tools)
 - Or use 'net ads status' on OS X

AD Security - NTLM

- The fallback when Kerberos can't be used
 - Login REQUIRES Kerberos - no NTLM logins
 - At login, OS X obtains a Kerberos TGT and DOES NOT cache the user's password
 - The next access that requires NTLM and not Kerberos will require the user to input their credentials again
 - Considered as “downlevel” security
 - Often used by Proxy Servers (Safari doesn't do Kerberos)
 - Credentials NOT cached for sharing folders when offline

LUNCH

Authentication & Replication

How Authentication Works

- How a machine account authenticates
- How a user account authenticates
- Password changes

Why Replication Matters

- GC's, remote DC's, etc.
- Sites, site links, replication time
- Collisions

Troubleshooting

Troubleshooting

- There are three major things we can do to troubleshoot:
 - Verify all settings in Network Preferences and the AD Plugin
 - Examine DNS for consistency
 - Turn up DS Debug Logging and investigate
- If the customer has bound this computer to AD before, even with a different name, have them remove that computer account from AD before re-binding. We search AD by macAddress first, **not** computer name. *If we find an existing computer account, we'll use it.*

KBase Review

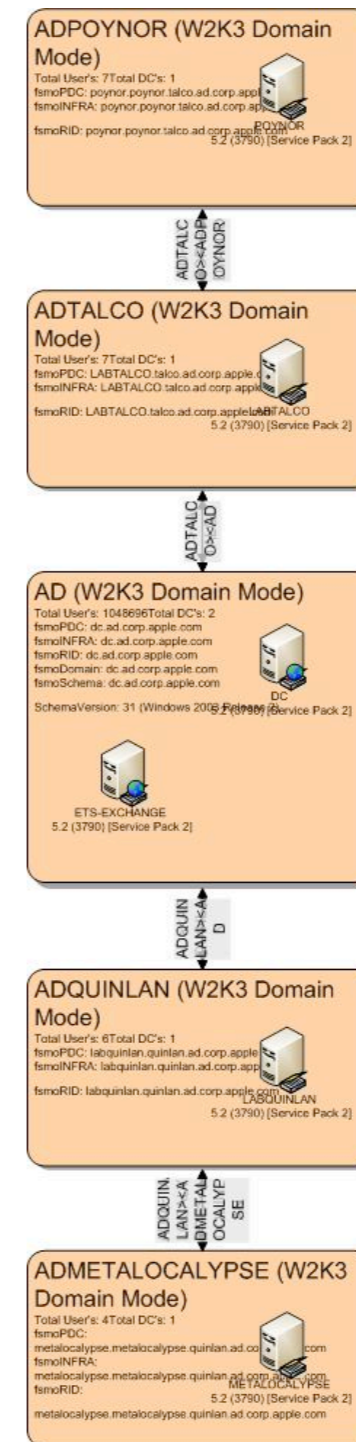
- Enable "Allow cryptography algorithms compatible with Windows NT 4.0" on the Windows Server 2008-based domain controller. More information can be found at: <http://support.microsoft.com/kb/942564> . <http://support.apple.com/kb/TS2967>
- Mac OS X v10.5:Active Directory - Name and password considerations when binding with Directory Utility or dsconfigad <http://support.apple.com/kb/TS1532> and <http://support.microsoft.com/kb/909264>
- Mac OS X v10.6: Successive Active Directory users receive "You are unable to log in to the user account (username) at this time" alert <http://support.apple.com/kb/TS3346>
- Mac OS X v10.6:Active Directory binding lost on network transition (.local domain) (mDNS timeout) <http://support.apple.com/kb/ts3248>
- Mac OS X v10.6: Clients bound to Active Directory may not be able to dismiss screen saver using Active Directory credentials (/etc/authorization) <http://support.apple.com/kb/TS3287>
- Mac OS X 10.5:Active Directory connector uses "macAddress" attribute to locate computer account <http://support.apple.com/kb/TS1534>
- Mac OS X v10.5:Verifying DNS consistency for Active Directory binding <http://support.apple.com/kb/HT3394>
- Mac OS X v10.5:Verifying DNS consistency for Active Directory binding / Ensure that the attribute for the affected home folder (homedirectory) in Active Directory uses a fully qualified host name for the server name. For example: \\server.example.com\homes\user <http://support.apple.com/kb/TS2495>
- Mac OS X 10.5: First 1000 results displayed when querying Active Directory <http://support.apple.com/kb/TS2525> <http://support.microsoft.com/kb/315071>
- Mac OS X Server v10.6: Configuring service principals in Active Directory when using a disjoint namespace <http://support.apple.com/kb/HT3795>
- Mac OS X 10.5 Directory Utility: Configuring "Prefer this domain server" in the Active Directory connector http://support.apple.com/kb/HT3393?viewlocale=en_US

BREAK

Third Party Tools

Microsoft Tools

- MPS Reports
 - Generates text-based report of AD configuration
- AD Topology Diagrammer
 - Provides graphical view of AD topology - sites,



Apache Directory Studio

The screenshot displays the Apache Directory Studio interface with three main panes:

- LDAP Browser:** Shows a tree view of the directory structure. The selected entry is `CN=beans3` under `CN=Computers`.
- Entry Editor:** Displays the details for the selected entry. The DN is `CN=beans3,CN=Computers,DC=ad,DC=corp,DC=apple,DC=com`. The attributes and their values are as follows:

Attribute	Description	Value
<i>objectClass</i>		<i>computer (structural)</i>
<i>objectClass</i>		<i>organizationalPerson (structural)</i>
<i>objectClass</i>		<i>person (structural)</i>
<i>objectClass</i>		<i>top (abstract)</i>
<i>objectClass</i>		<i>user (structural)</i>
<i>cn</i>		beans3
<i>instanceType</i>		4
<i>objectCategory</i>		CN=Computer,CN=Schema,CN=Configuration,DC=ad,DC=corp,DC=apple,DC=com
<i>accountExpires</i>		9223372036854775807
<i>badPasswordTime</i>		128679799355468750
<i>badPwdCount</i>		0
<i>codePage</i>		0
<i>countryCode</i>		0
<i>distinguishedName</i>		CN=beans3,CN=Computers,DC=ad,DC=corp,DC=apple,DC=com
<i>dNSHostName</i>		beans3.ad.corp.apple.com
<i>dSCorePropagationData</i>		Dec 31, 1600 4:00:01 PM PST (16010101000001.0Z)
<i>dSCorePropagationData</i>		Aug 1, 2008 8:04:11 AM PDT (20080801150411.0Z)
<i>isCriticalSystemObject</i>		FALSE
<i>lastLogoff</i>		0
<i>lastLogon</i>		128711962803281250
<i>lastLogonTimestamp</i>		128708122491562500
<i>localPolicyFlags</i>		0
<i>logonCount</i>		231
<i>name</i>		beans3
<i>networkAddress</i>		17.102.132.135
<i>networkAddress</i>		fe80::1%lo0
<i>networkAddress</i>		fe80::20a:95ff:fe95:a4ae%en0
<i>objectGUID</i>		Invalid Data
<i>objectSid</i>		Invalid Data
<i>operatingSystem</i>		Mac OS X
<i>operatingSystemVersion</i>		10.5.4 (Build 9E17)
<i>primaryGroupID</i>		515
<i>pwdLastSet</i>		128710896113437500
<i>sAMAccountName</i>		beans35
<i>sAMAccountType</i>		805306369

- Outline:** Shows a hierarchical view of the selected entry's attributes, including `objectClass`, `cn`, `instanceType`, `objectCategory`, `accountExpires`, `badPasswordTime`, `badPwdCount`, `codePage`, `countryCode`, `distinguishedName`, `dNSHostName`, `dSCorePropagationData`, `isCriticalSystemObject`, `lastLogoff`, `lastLogon`, `lastLogonTimestamp`, `localPolicyFlags`, `logonCount`, `name`, `networkAddress`, `objectGUID`, `objectSid`, `operatingSystem`, `operatingSystemVersion`, `primaryGroupID`, `pwdLastSet`, `sAMAccountName`, `sAMAccountType`, `servicePrincipalName`, `userAccountControl`, `uSNChanged`, `uSNCreated`, `whenChanged`, and `whenCreated`.
- Progress:** Shows "No operations to display at this time."

Wireshark

- Packet captures are often overkill (good logging comes first), but can be helpful for troubleshooting:
 - Kerberos
 - SMB
 - LDAP
- tcpdump will create the capture, Wireshark is a great tool for reading them
- On Leopard, please include the -K flag to disable TCP checksum validation

Wrap Up / Questions



NEW for 2011 - Online Session Evaluations

To complete the online evaluation forms for sessions you attend, go to:

<https://www.cteusa.com/idg1/>

Login: First Initial and Last Name (all one word; no spaces/characters)

For example John Smith = JSMITH

Password: Your Registration ID (Found on your Badge and in your registration confirmation)