

Integrating OS X into Active Directory



James Nairn: jwrn3@cam.ac.uk
University Computing Service

Benefits of Integration

- Allows users to securely log in at a Mac using Active Directory credentials
- Single Sign On reduces admin overheads and simplifies user services
- User's OS X home can either be on local disk, mounted share from Active Directory or from OS X Server

Mac OS X Server
Tiger

Prerequisites for Active Directory Integration

- DNS should be provided by a SRV aware DNS (i.e. Windows)
- NTP server should be used to ensure time is in sync between OS X and Active Directory
- Administrator level accounts needed for OS X & Windows
- OS X 10.4 & Windows Server 2003 highly recommended

Binding OS X to Active Directory

- Simple solution for central user management
- Kerberos provides secure authentication
- Password policies are respected
- Admin rights can be delegated to Mac users
- Home directory can be provided by a variety of means

Binding OS X Server to Active Directory

- Functionality as with OS X client
- OS X Server can join the Active Directory Kerberos domain
- OS X Server services can be made available to all AD users via Kerberos i.e. AFP, SMB (only if AD Kerberos realm joined)

Home Directories

- Four possible options
 - Home on local disk (no roaming)
 - Home on local disk but Windows share automounted
 - Home on automounted Windows share (allows roaming)
 - Home on automounted OS X Server share (also allows roaming)
- 'Mobile Accounts' allow laptop users to authenticate using AD credentials while offline
 - Home on local disk only

NetInfo

- Local authentication database on each Mac
- Always queried first for matching user at login
- Managed through NetInfo Manager
- NextStep legacy

Mac OS X Server
Tiger

Open Directory



- Apple's Directory Services implementation
- Comprises:
 - LDAP server (OpenLDAP, slapd)
 - Password Server (PasswordService)
 - Lookup Service (DirectoryService)
 - Kerberos (kadmin)
 - Legacy lookup Server (lookupd)
 - Netinfo Server (netinfod)

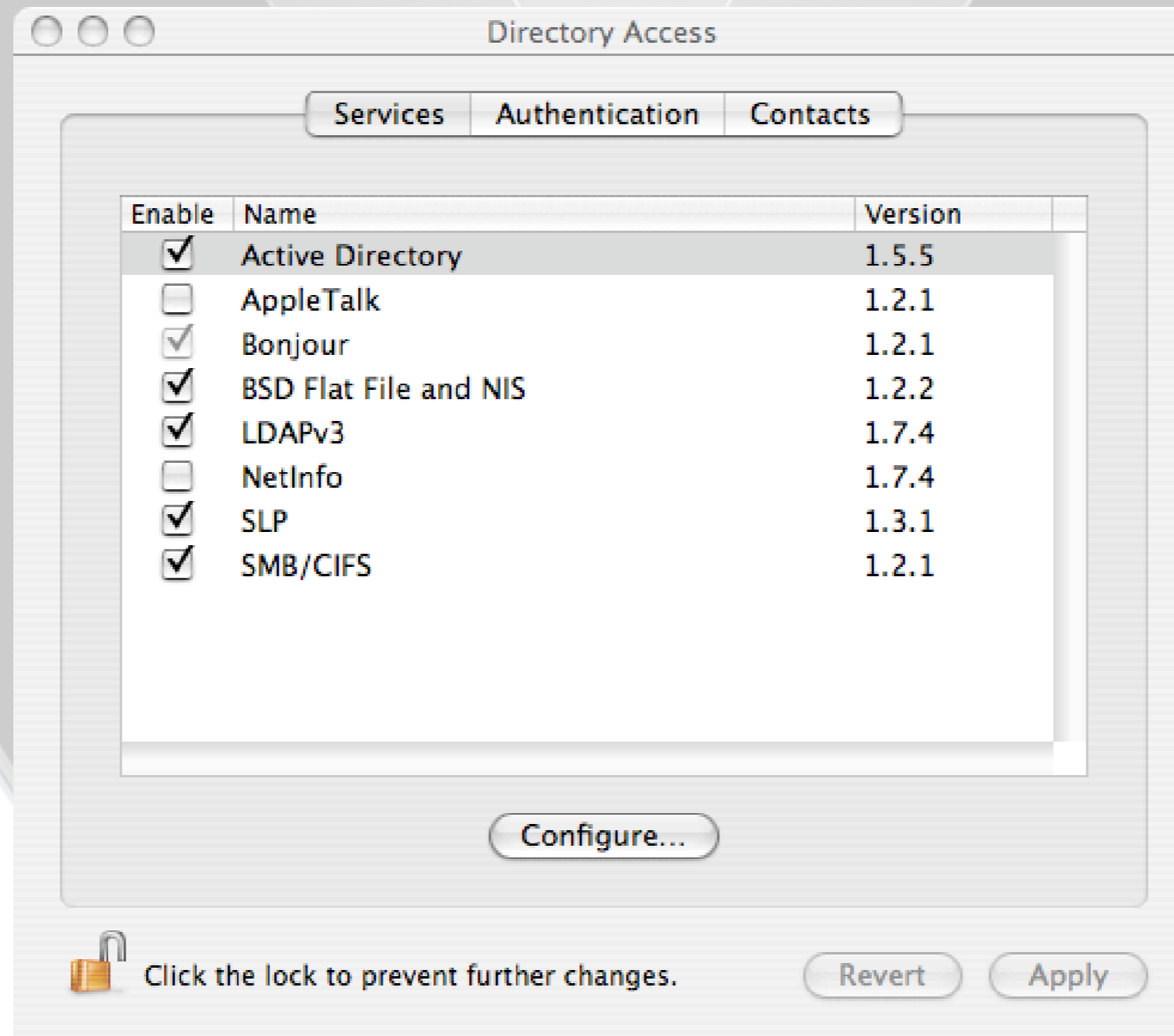
Mac OS X Server
Tiger

Directory Access

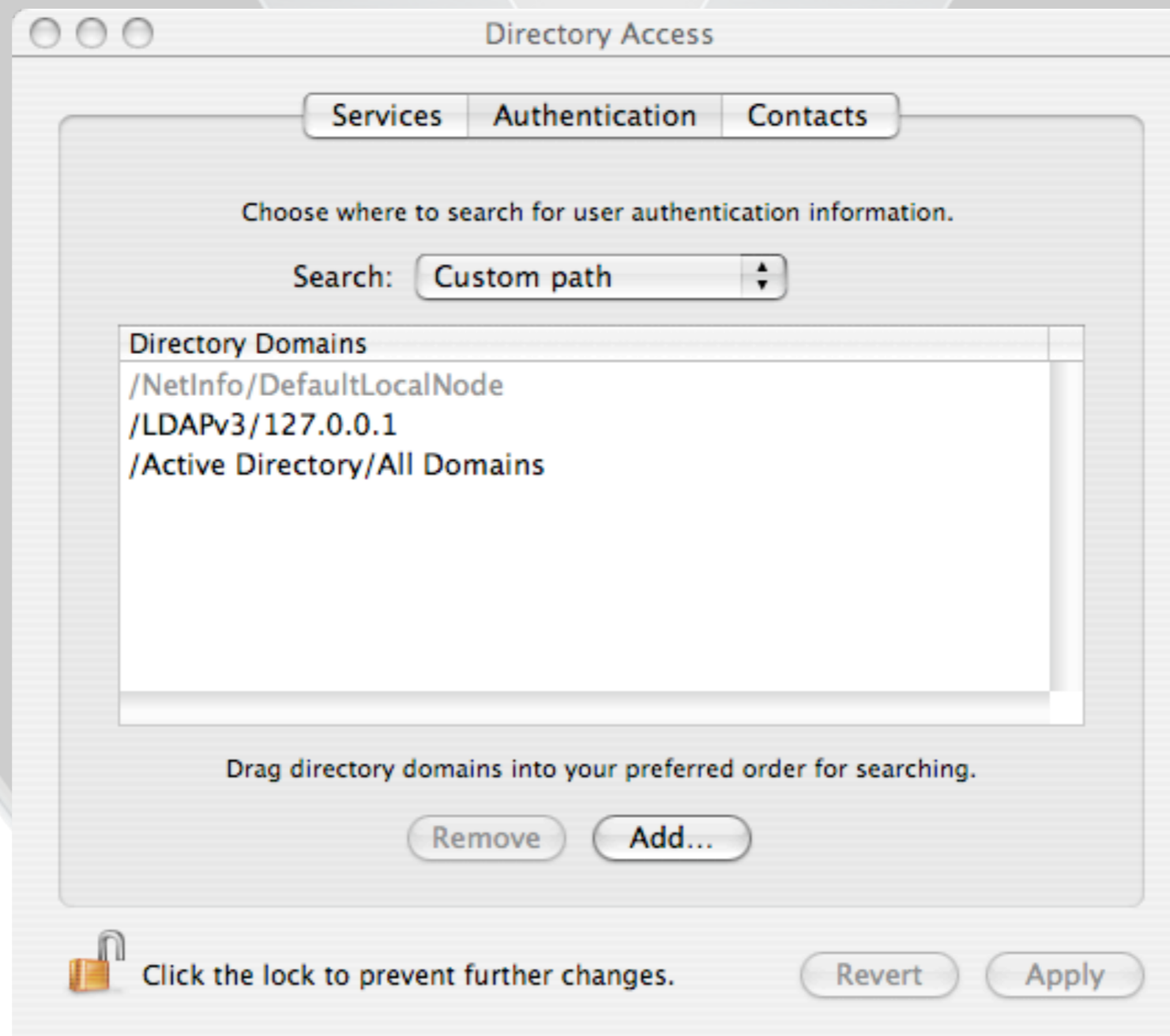
- Defines directories to be searched for resources
- Defines search order for a resource
- Each configuration can be set to search for all resources or specific attributes
- Each attribute can originate from separate directories e.g.
 - Users in Active Directory
 - MCX configuration in OS X Server

Mac OS X Server
Tiger

Directory Access - Services



Directory Access - Authentication



Basic AD Plugin Functionality

- Allows Macs to bind to Active Directory
- Available in OS X 10.3 & 10.4
- Functionality consistent between OS X client & Server

Mac OS X Server
Tiger

Additional AD Plugin Functionality

- Caching of login details to allow mobile users to authenticate offline
- Translation of UNC path of homedirectory attribute to Mac compatible form
- Creation of local home directory in /Users if homedirectory attribute is not set
- Map UID to Active Directory attribute
- Delegation of admin rights on local Mac through groups

Active Directory Plugin

Active Directory Forest:

Active Directory Domain:

Computer ID:

Hide Advanced Options

Create mobile account at login

Require confirmation before creating a mobile account

Force local home directory on startup disk

Use UNC path from Active Directory to derive network home location

Network protocol to be used: ▾

Default user shell:

erver

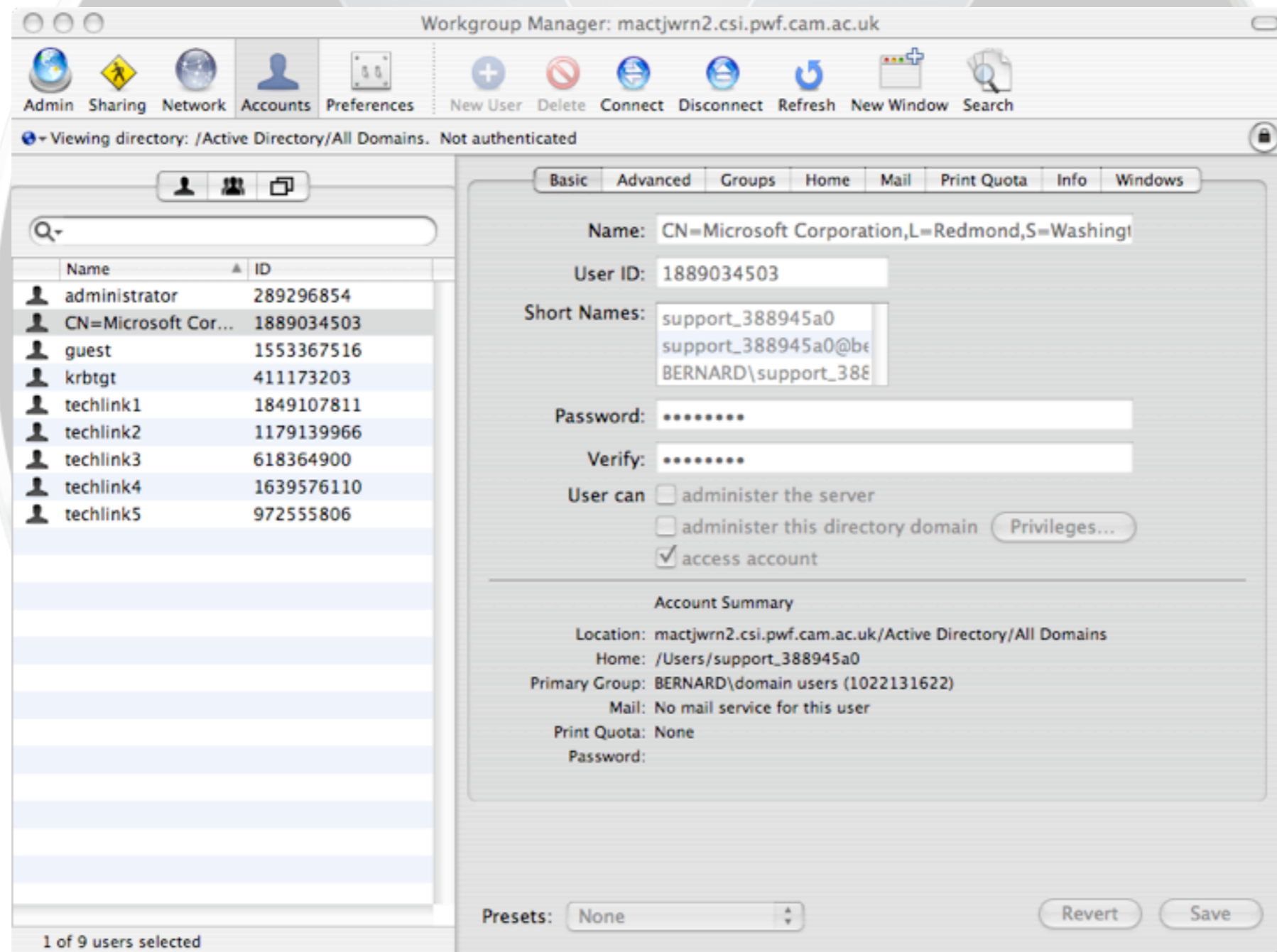
Binding OS X Server

- Use Active Directory for DNS
- Bind into Active Directory using Directory Access plugin
- Change role of server to 'Connected to a Directory System'
- Use Server Admin to join the Kerberos realm hosted by Active Directory

Managing Active Directory Users

- Users can be hosted in AD with their Mac environment managed by Workgroup Manager (OS X Server)
- Users not duplicated in OD but groups etc are populated by references to the original user object
- Group membership checked at login and environment configured accordingly

Active Directory Users in WGM



Managing Kerberos Tickets

- Kerberos.app - Apple provided application to manage tickets
- Located in `/System/Library/CoreServices/`
- Provides a method to:
 - Create, renew and destroy tickets
 - Change password
 - View ticket details

Mac OS X Server
Tiger

Integration Caveats

- SMB signing must not be enforced for 10.4 and older clients to connect. See: http://www-tus.csx.cam.ac.uk/pc_support/WinNT/OSXAuth/OSXauthentication.html
- OS X 10.4 is recommended. Integration possible with 10.3 but far more problematic with complicated setups

Mac OS X Server
Tiger

Scaling

- Image Macs where possible
 - NetInstall
 - NetRestore
 - Casper
 - Disk Utility
- Bind using a script
 - Part of an image
 - Deployed to unmanaged Macs

Mac OS X Server
Tiger

Scripting

- **dsconfigad** to configure AD plugin:
 - Bind to Active Directory
 - Configure binding options
- **dscl** to manage Directory Services:
 - Create and delete users and groups
 - Manage object attributes
 - Configure Authentication and Contacts panes of Directory Access

Scripting - 2

- Some functionality can only be accessed through the command line
- Privileged AD user and password must be specified when binding
- **dsconfigldap** is equivalent of dsconfigad for LDAP binds

Mac OS X Server
Tiger

Configuration Files for OS X

- `/Library/Preferences/DirectoryService/`
 - Contains Directory Access config files
- `/etc/krb5.keytab`
 - Kerberos keytab file containing details of realms and kerberised services

Troubleshooting



- Use **dscl** on OS X to browse Directory Services in Terminal
- Use Kerberos application to check granting of tickets
- Check 'Users and Computers' in Windows to see if there is a computer record and remove if necessary
- Check networking and ntp etc
- Check log files

Mac OS X Server
Tiger

Log Files

- /Library/Logs/DirectoryService/
 - DirectoryService.error.log
 - DirectoryService.server.log
- /var/log/
 - system.log
 - kdc.log
- Use Console or Server Admin to browse logs
- Check Security log in Event Viewer

Mac OS X Server
Tiger



AD Integration Products

- ExtremeZ-IP
- ADmitMac
- DAVE

Mac OS X Server
Tiger

ExtremeZ-IP



- No client software required - Windows server install
- Full AFP v3.1 compatibility
- File and Print services supported
- Supports Bonjour, Kerberos
- www.grouplogic.com/products/extreme/overview.cfm

ADmitMac

- OS X based install
- Supports AD & domain authentication
- Supports SMB signing
- Allows centralised account management
- Many more features
- www.thursby.com/products/admitmac.html

DAVE

- OS X based install
- Supports MacOS 8.6 - OS X 10.4
- Supports Windows/Mac file sharing
- Domain login only, not Active Directory
- www.thursby.com/products/dave.html

Integration with other Directory Services

- Novell eDirectory
 - Use LDAP as interface to eDir
 - Schema needs extending for full Mac support
 - Kanaka is 3rd party plugin
- LDAP server (OpenLDAP etc)
 - RFC 2307 supported
- NIS
 - Supported by OS X

Mac OS X Server
Tiger

Web Resources



- www.afp548.com
- www.shukwit.com/
- www.bombich.com/mactips/activedir.html
- www.macwindows.com

Mac OS X Server
Tiger

Binding Demonstration

- Binding OS X to Windows Server 2003
- Logging in an Active Directory user
- Mounting a share at login

Mac OS X Server
Tiger