Introduction to Active Directory

December 10th, 2008

1-3pm Daniels 407

What we are going to cover...

- The basics of Active Directory
- What AD is
- What AD isn't
- Tools
- Management Concepts
- Additional Services
- Q & A

Active Directory is...

A directory service that provides the ability for centralized:

- Authentication
- Authorization
- Management

Active Directory is based on LDAP. LDAP is an industry standard method to access information from a remote database. LDAP does not define what sorts of info are stored or how it should be stored, only how to access it. Any type of data can be stored in a properly constructed LDAP service. In fact, Active Directory Application Mode is just a stand-alone LDAP server. Active directory stores copies of it's data on several Domain Controllers (DC's). If one fails, services are still available.

Tools

Remote Server Administration Toolkit (RSAT) includes:

- Active Directory Users and Computers (ADUC)
- Group Policy Management Console (GPMC)
- Group Policy Editor
- DFS Management Console
- Print Managment Console

Domain-wide Administration:

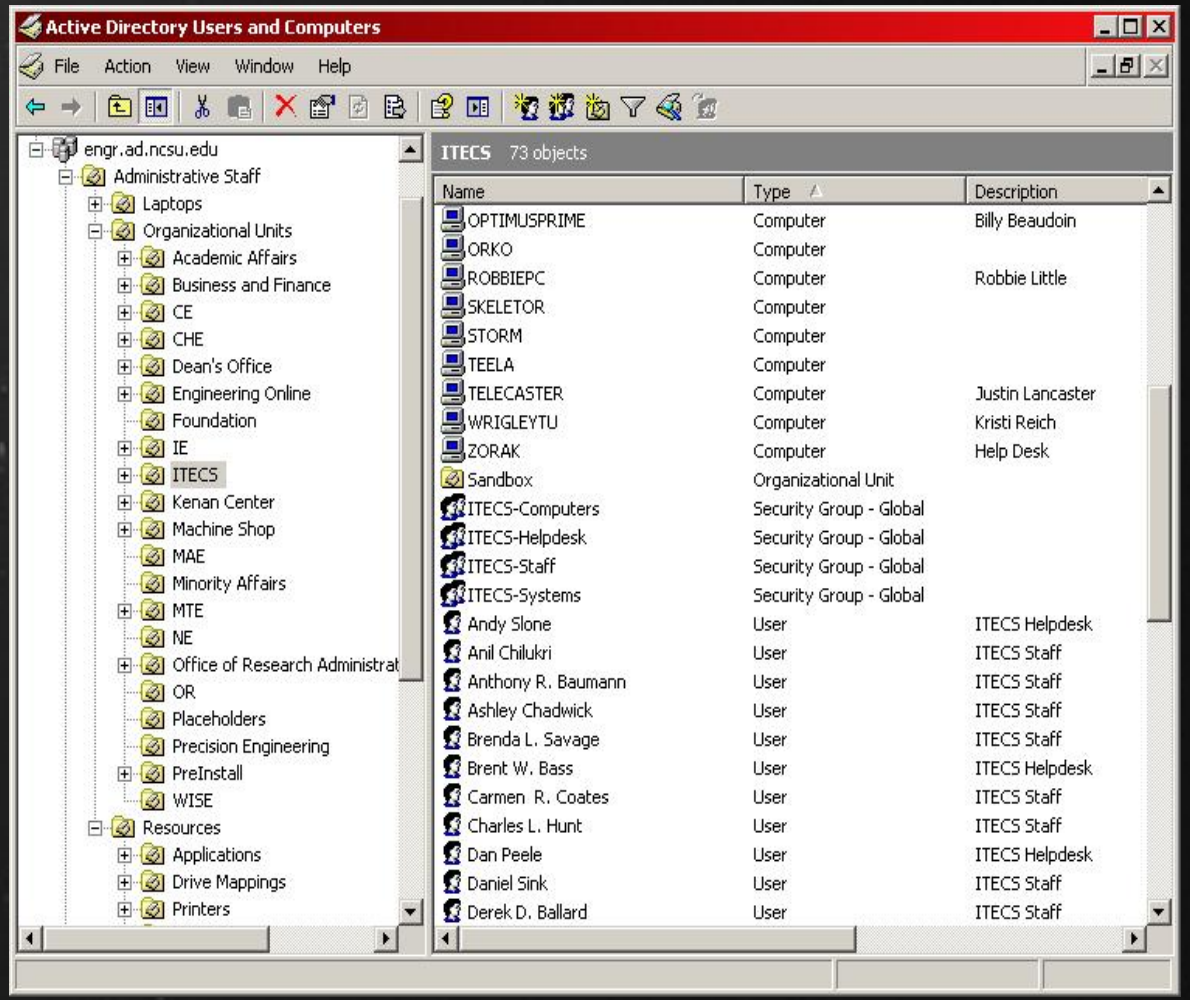
- Active Directory Sites and Services
- Active Directory Domains and Trusts

AD Objects

Organizational Units
Users
Computers
Groups

Links (publishing):

- Shares
- Print Shares



What AD isn't

- A 100% solution
- A desktop environment
- Microsoft only
- The same as Novell
- 100% Automatable
- A true identity management system
- Perfect

Authentication

Native:

- Kerberos (Version 5)
- NTLMv2
- LDAP
- Smart Cards/Certificates

Extendable to include:

- Biometrics

Client machines authenticate as well, not just user accounts
Supports dual factor authentication
Mac, Linux clients can auth against AD

Trusts

Trusts don't imply any sort of authorization or rights assignment. If Domain "A" trusts Domain "B" all it implies is that accounts from "B" can be used in "A" No rights assignments of any kind are made automatically.

This makes it possible to access resources in multiple domains using a single account.

Trusts:

- Intra-Forest
- Inter-Forest
- Cross Realm

Authorization

Delegation Wizard

Types of Permissions:

- Directory
  - GPO's
  - Manage Groups
- Machine
  - Local/Remote Login
  - User vs. Admin
  - Group Policy allows setting any local permission

Groups are key to any good permissions model

AD supports Nested Groups

Management Concepts

- Domain Structure
  - OU structure
  - User/Computer Locations
  - Grouping Strategy
- Group Policy
  - Linking
  - Filtering
    - Groups
    - WMI Filters
  - Starter GPO's
  - Copying GPO's
  - Group Policy Modelling

Policies vs. Preferences

- Policies:
  - Policies usually cannot be changed by end user
  - Configuring IE
  - Deploying Software
  - Configuring Desktop Experience
- Preferences:
  - End user override optional per setting
  - Pushing Files/Reg Keys/Shortcuts
  - Item-Level Targeting

Both have User and Computer Settings

Loopback - Process User settings using Computer location

Group Policy Examples

- Remote Assistance - Policy
- Remote Administration - Policy
- Configure Wireless - Policy
- Configure Firewall - Policy
- Deploy Printers - Policy or GPP
- Deploy Startup/Shutdown/Logon/Logoff Scripts - Policy or GPP
- Deploy Software (.msi's) - Policy
- Deploy Scheduled Tasks - GPP
- Mapped Drives - GPP
- Power Settings - GPP

Windows Server Update Services (WSUS)

Unified Patch Management for MS Products - FREE

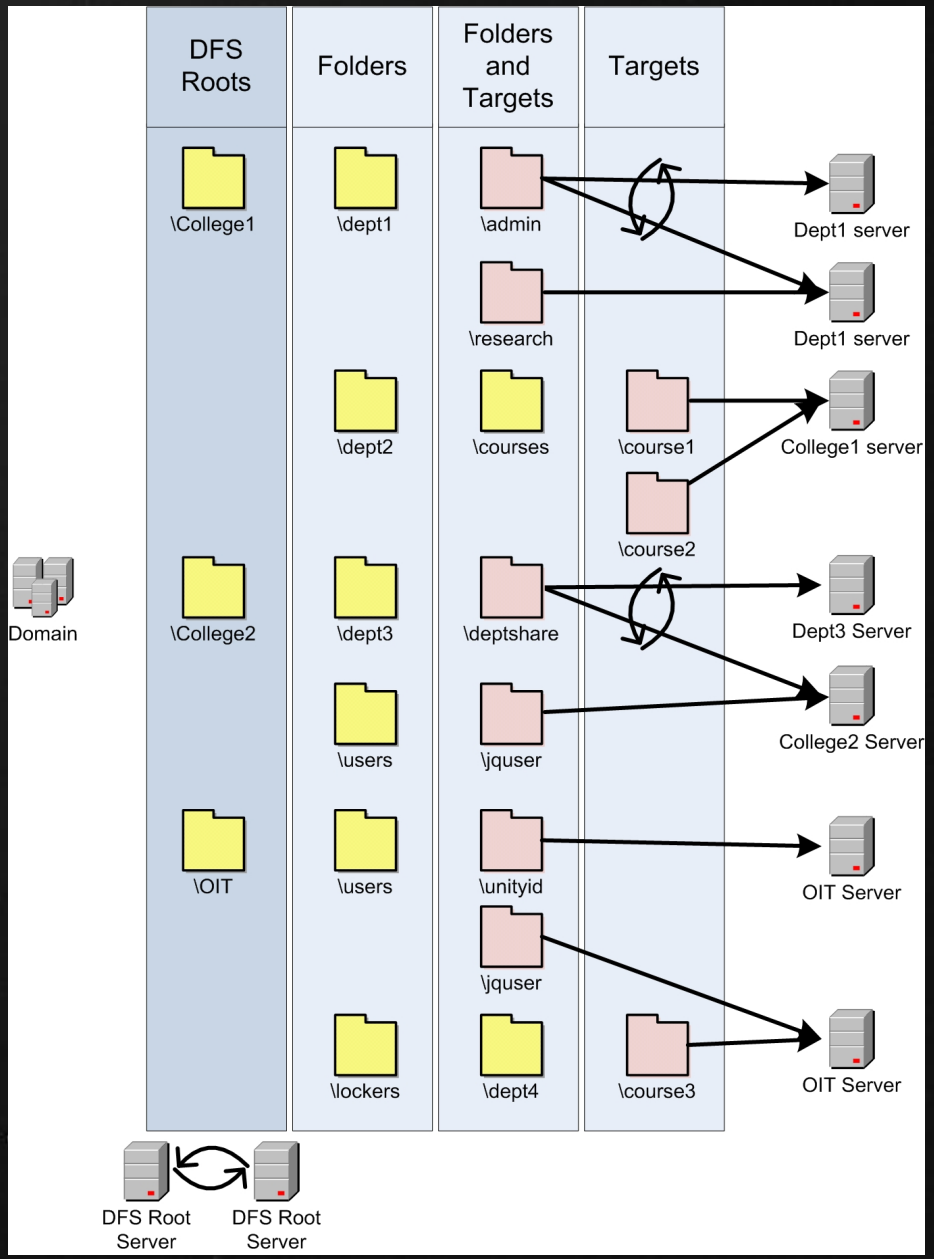
- Apply patches based on grouping
  - Server side groups
  - *Client Side Targeting via Group Policy*
- Types of Patches:
  - Service Packs/Security Patches/Bugfixes
  - Drivers
  - Defender definitions
  - Office Patches/Service Packs
  - Add-ons: Windows Media, Silverlight, GPP, etc.
  - Server Products: SQL, IIS
- Ability to back out patches per group of machines (not always supported by the patches)

Distributed File System (DFS)

DFS is a Network File System

Core CAL Required

- Roots (Namespaces)
  - Delegation
- Folders
  - Create Arbitrary structure
- Targets
  - Where the files are
- Multi-Master Replication



Windows Distribution Services (WDS)

Replaces Remote Installation Services (RIS)
Core CAL Required

- Imaging for XP/Vista/2K3 Server/2K8 Server
- Uses PXE for medialess install
- Uses WinPE (think Vista on a CD) as install environment
- Can have a library of drivers
- GUI tools for setting up:
  - Post-install scripts
  - Joining a domain

Additional Services

Core CAL Required (NCSU has a Site License!):
Certificate Services - PKI
File Services (Clustering, iSCSI)
Print Services
IIS / Webdav
Sharepoint Services 3.0

Additional stuff we don't use: DNS/DHCP

Additional CAL Required:
Terminal Services

Questions?