

# Introduction to WolfTech Active Directory

6 October 2011  
10am-12pm Daniels 201

<http://activedirectory.ncsu.edu>



**NC STATE UNIVERSITY**

# What we are going to cover...

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



# Active Directory is...

A directory service that provides the ability for centralized:

- Authentication
- Authorization
- Management

Active Directory is based on the MIT Athena model. It makes use of SMB, LDAP, and Kerberos.

- SMB (or CIFS) is a network file sharing protocol common to all recent Windows OS's.
- LDAP is an standard method to access information from a remote database, does not define what sorts of info are stored or how it should be stored, only how to access it.
- Kerberos is a network authentication protocol designed by MIT with strong cryptography and a limited attack surface.

Active Directory uses multi-master replication to have all directory data on the Domain Controllers (DC's). If one fails, services are still available.



# Active Directory isn't...

- A 100% solution
- A desktop environment
- Microsoft only
- The same as Novell
- 100% Automatable
- A true identity management system (as implemented at NCSU)
- Perfect



# WolfTech Active Directory Implementation

- Framework
  - Opt-in:
    - Applications
    - Imaging
    - Remote Desktop/Assistance
  - Defaults:
    - OU Structure
    - Enterprise Client Policies
    - Patching
    - Reports - WSUS and DNS
- Delegation
- Governance
- Community Support



# Management Tools

Remote Server Administration Toolkit (RSAT) includes:

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

Domain-wide Administration:

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

ADToolkit

System Center Configuration Manager

WDS/WSUS



# AD Objects

Organizational Units

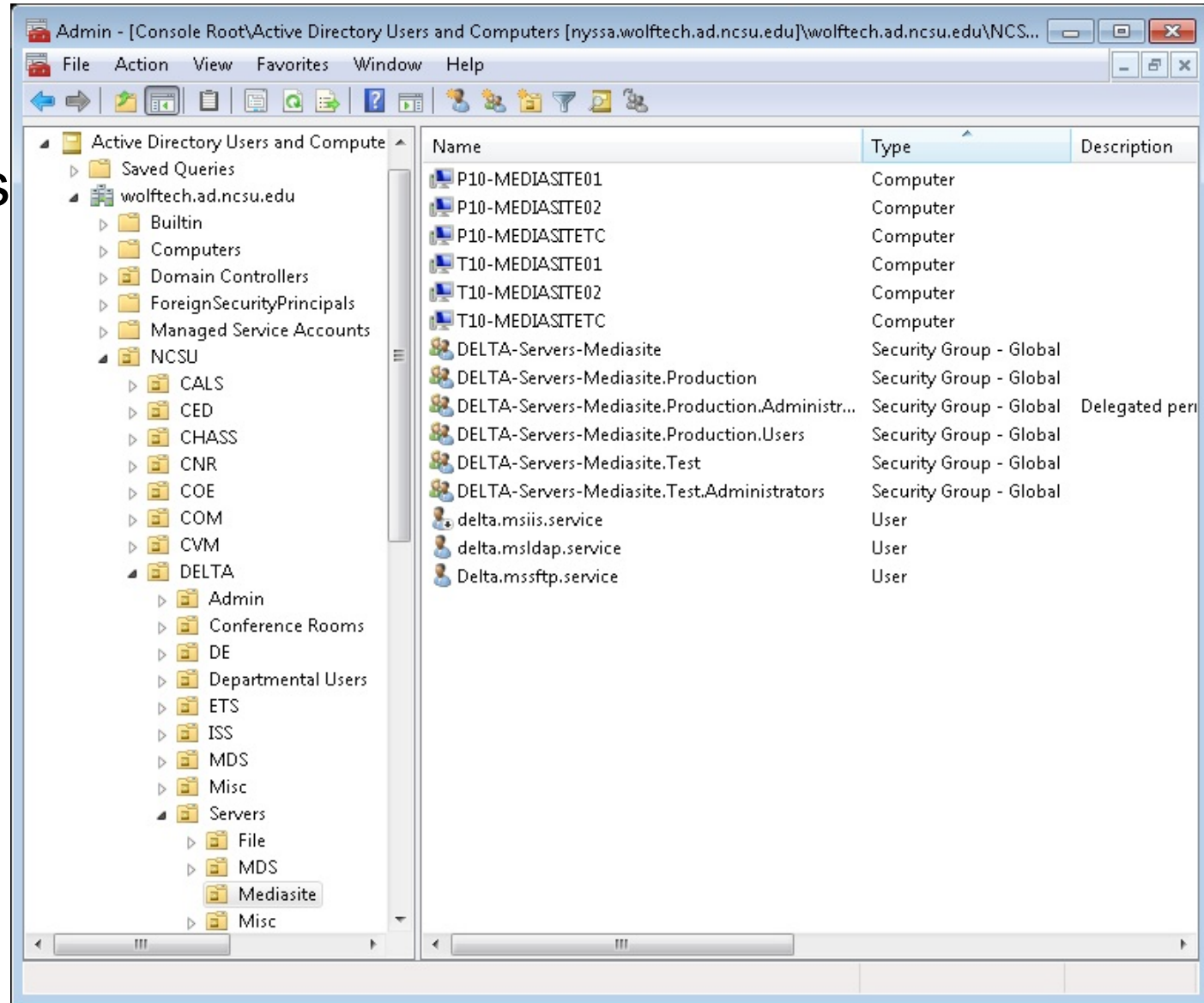
Computers

Users

Groups

Links (publishing):

- File Shares
- Printer Shares



# Authentication

Natively supports:

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

Client machines authenticate as well, not just user accounts

Extendable to include:

- Biometrics

Mac, Linux clients can authenticate against AD

Limitations:

Can't access DFS, Group Policy

Some specific authentication/authorization differences





# AD Objects: Groups

Groups are key to any good permissions model  
Active Directory supports Nested Groups

Concepts:

Identity Groups

Resource Groups

Users -> Identity Group -> Resource Group -> Permissions

Examples of Default Groups (Users vs. Computers):

Computers: Software Groups

Computers: Enable Remote Desktop/Assistance

Users: ACS Users

Users: OU/Computer Admins



# 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

ADUC - Demo



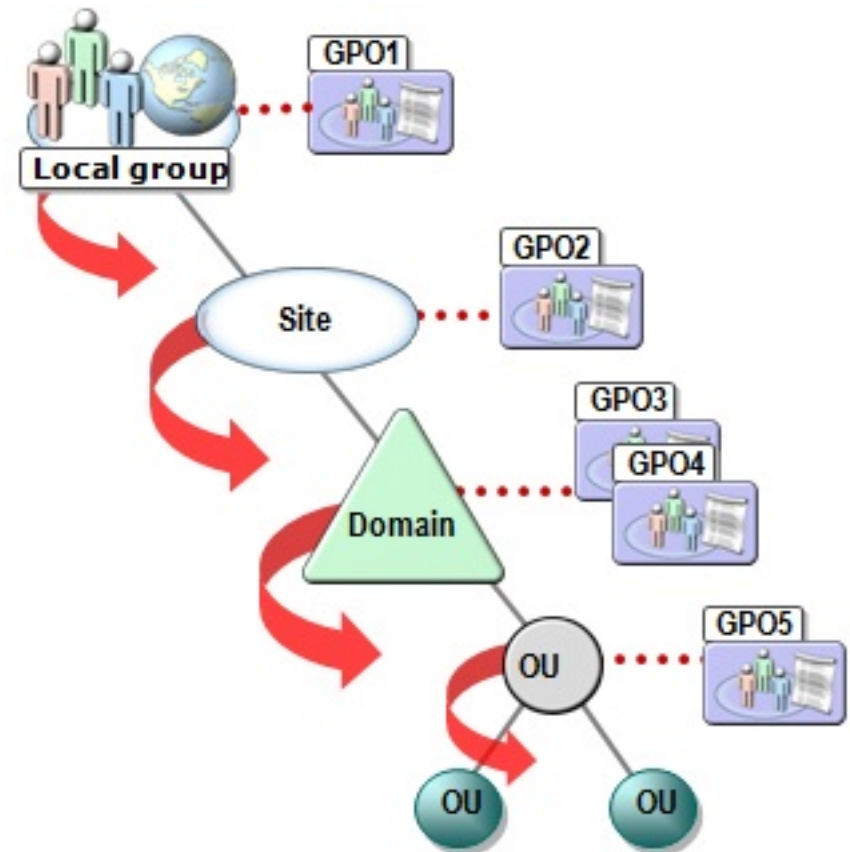
# Management Concepts

## Domain Structure

- OU structure
- User/Computer Locations
- Grouping Strategy

## Group Policy

- Linking
- Filtering
  - Groups
  - WMI Filters
- Copying GPO's
- Group Policy - Resultant Set of Policy



# 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/Drive Mappings
  - Item-Level Targeting
    - Hardware, Software
    - AD Info, Networking

Both have User and Computer Settings

Loopback - Process User settings using Computer location

GPMC - Demo



# Group Policy Examples

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



# Services Provided within WolfTech AD

Domain Controllers - Accounts, Group Policy, DR, etc.

Distributed File System

Certificate Services

Windows Deployment Services

Application Packaging

Windows Software Update Services

ADToolkit: Reporting / WTMG

System Center Configuration Manager



# ADToolkit

<http://www.wolftech.ncsu.edu/adtoolkit/>

Software Provided by WolfTech IT to assist OU Admins:

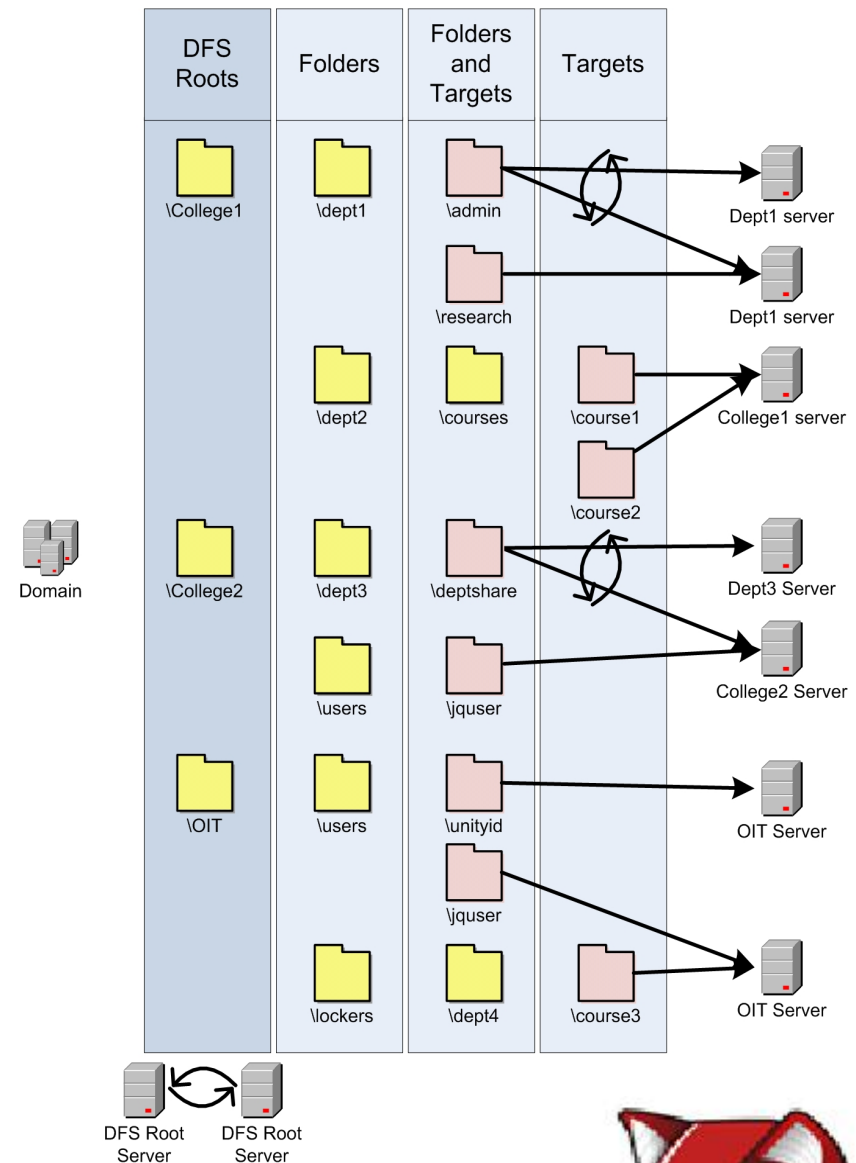
- Reporting
  - DNS Errors, Patch Status, Naming Convention issues, Group Changes, Bitlocker usage, etc...
  - On-Demand and can be Automated for daily/weekly reports to you or your Remedy queue.
- Tools to manage / monitor your software deployments
- User / Group Search
- Management of WT Managed Groups (groups automatically updated from HR + Registration/Records)
- Statistics (and pretty pie charts)
- Unlock Accounts



# Distributed File System (DFS)

## DFS is a Network File System

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





# Windows Distribution Services (WDS)

- Imaging service for Windows 7, 2008 R2 Server, or custom images
- Uses PXE (F12) for medialess install
  - Must use one of the following DHCP templates in QIP:
    - WDS-Main, WDS-Centennial, PXE-all
- Uses WinPE (think Win7 on a CD) as install environment
- Library of drivers available to all images
  - Additional/New drivers added by OU Admin request
- GUI tools for setting up:
  - Post-install scripts
  - Joining the domain

<http://activedirectory.ncsu.edu/services/imaging/windows-deployment-services/>



# Windows Server Update Services (WSUS)

## Unified Patch Management for MS Products

- Apply patches based on grouping
  - Client Side Targeting via Group Policy
  - Early, Normal and Late patch schedules
- Types of Patches:
  - Service Packs/Security Patches/Bugfixes
  - MS Defender definitions
  - MS Office Patches/Service Packs
  - Add-ons: Windows Media, Silverlight, GPP, etc.
  - Server Products: SQL, IIS, Sharepoint
- Ability to back out patches per group of machines (not always supported by the patches and rarely utilized)
- Reporting: ADToolkit Report - Demo

<http://activedirectory.ncsu.edu/services/patching/>



# System Center Configuration Manager

Inventory

Application Deployment

- Mandatory

- Self Service

Patch Management

- Microsoft

- Custom and Third-Party

Imaging

Power Management

Mobile Device Management



# Where Can I Go for Help?

## AD Site

- <http://activedirectory.ncsu.edu>

## Mailing Lists

- [activedirectory@lists.ncsu.edu](mailto:activedirectory@lists.ncsu.edu)
- [activedirectory-patches@lists.ncsu.edu](mailto:activedirectory-patches@lists.ncsu.edu)
- [wds@lists.ncsu.edu](mailto:wds@lists.ncsu.edu)

## Jabber

- "activedirectory" on [conference.jabber.eos.ncsu.edu](http://conference.jabber.eos.ncsu.edu)

## Remedy

- [wolftech\\_ad\\_technical@remedy.ncsu.edu](mailto:wolftech_ad_technical@remedy.ncsu.edu)



# Questions?

