WolfTech Active Directory: OU Administration

August 4th, 2011

2-5pm Daniels 201

http://activedirectory.ncsu.edu

What we are going to cover...

- Info for those who are new to AD
- Basic Units of AD: Users, OU's, Groups
- WolfTech Specifics
- Group Policy
- Other AD-related Services

NC STATE UNIVERSITY

New to AD: Tools You'll Need

- Remote Server Administration Tools (RSAT)
  - Windows 7SP1 / 2008r2 version of AdminPak
  - Only way to access Group Policy Preferences
  - Includes all added functionality from 2003 R2+
- GPMC - Included in 2008r2/Windows 7
- SpecOps GPUpdate - Free extension for ADUC
  - Reboot, Shutdown, GPUpdate, Windows Update
- Scripting: VBScript/PowerShell
  - Powershell:
    - Import-Module grouppolicy ; Get-Command *-GP*
    - Import-Module activedirectory; Get-Command *-AD*
  - MS has downloadable 2008 GPO VBScripts
- Custom MMC Consoles

New to AD: Administration Checklist

Prerequisites for being successful:

- DNS needs to be accurate, including DNS domains, use DHCP
  - DNS must be correct for Certificates and SCCM to work
  - You will get a daily email if your PCs don't report this correctly
  - Computers need unique names w/ 15 characters or less
  - IPReport -- easy overview of your unit's IPs; check duplicates
- Network access at boot time needed for many AD features
  - Laptops need to be registered in Nomad (w/unit if users don't)
  - Regular reboots of desktops
- Windows 7/2008r2 - on your machine
  - Newer GPMC features are not available on older OS's
  - Some Powershell cmdlets not available on older OS's
- Firewall access (you must configure this specific to your unit)
  - Printer and File Sharing
  - WMI / Remote Administration
  - Remote Desktop / Remote Assistance
  - Your "administration" computers in contiguous IP range

NC STATE UNIVERSITY

Administration Concepts

1. Design OU/Group Layout Considerations
    - What types of Users do you have to support?
    - What types of computers ?
    - Are there multiple Logical Units? Offices? Departments?
2. Management Policies
    - Who can login where? What level of permissions should they have?
    - Who is allowed to administer the machines?
    - Do you need to deploy Mapped Drives, Scripts, or Printers?
3. Software Deployment Strategy
    - Who can install their own software on what machines?
    - What software packages need to be automated?
4. Migrating Machines
    - Reinstall from scratch or Join them in current state?
    - Pre-Staging Computer Objects
    - Do you include Mac/Linux machines?
    - New Machine/Reinstallation - WDS
5. What other services will you need to provide?

Basic Units of Active Directory

Users, OUs, Groups

NC STATE UNIVERSITY

AD Accounts @ NCSU

Accounts already provisioned for all UnityIDs:

- Centrally managed; very little identity data assoc. w/ each
- Passwords synced via Password Change Page
- Including Workshop Accounts

Units can create their own accounts:

- Avoid local accounts on individual computers. Use domain accounts with local privileges whenever possible.
- Unit accounts must be more than 8 characters
- Administrative: <UNITYID>.admin
- Guests: <DEPT>.<FIRSTNAME>.<LASTNAME>
- Service: <DEPT>.<SERVICENAME>.service
- http://activedirectory.ncsu.edu/ou-admins/naming-conventions/

Coming Soon:

- Cross Realm Trust

NC STATE UNIVERSITY

OU Layout Considerations

OU Structure Concepts

Default OU Layout
Departmental Users
Faculty/Staff
Research/Teaching Labs
Software Packages (*special, do not delete)

Desktops/Laptops OU's:

- Cron Job to maintain group memberships for .Desktops/.Laptops

Favor an overly-hierarchical layout rather than a flat layout

- Allows for easier targeting of GPO's
- Follows a more logical structure for support
- Its harder to move from Flat->Hierarchical than vise-versa

NC STATE UNIVERSITY

OU Layout - Machine Types

- Single User
  - Faculty - Individual login, local admin
  - Staff - Individual or group login, no local admin
  - Grad Students - Group login, no student admin, Faculty admin
- Labs
  - Teaching Labs - college or class login, user rights
  - Public Labs - any account login (or college), user rights
  - Research Labs - Group login, user rights
- Stand Alone
  - Kiosks, Digital Signage - no login, extremely locked down
  - Conference Rooms - any account login
  - Loaner machines
- Servers? Macs? Linux boxes?

Q: Design OU structure based on Function or Organization?
A: Both! First one, then the other.

Understanding AD Groups

"Best Practices":

- A-G-DL-P Grouping Strategy
- Creating lots of groups up front will ease administration when change requests are needed later on.
- It is better to have a group and not use it, than need a group and not have one.
- **Always** use groups for delegating permissions.

Types of Groups:

- Group by User Directory Info: Faculty/Staff/Student
- Group by Machine Use: Public Lab/Teaching Lab/Kiosk/Server
- Group by Machine type: Laptop/Desktop
- Group by Administrative Access: Server Admins/Lab Admins
- Groups for Application Deployment
- Groups for Printer Deployment
- Groups for Resource/FileShare Access

WolfTech Default AD Groups

Predefined/Special Groups:

- Users:
  - -OU Admins
  - -Computer Admins
  - -ACS Users
  - -Users
  - -ADToolKit_*
- Computers:
  - Software Groups
  - Enable Remote Desktop/Assistance
- Groups:
  - .Computers
  - .Desktops/.Laptops

NC STATE UNIVERSITY

WolfTech Managed Groups

- Create Groups based on Identity Information:
  - OUC
  - Affiliation (Faculty/Staff/Student, etc)
  - Building
  - Course Rolls
  - Degree
- Membership populated daily (updated early morning)
- Supports expiration dates

- https://www.wolftech.ncsu.edu/adtoolkit/, click WTMG (Demo)

Understanding Group Policy

NC STATE UNIVERSITY

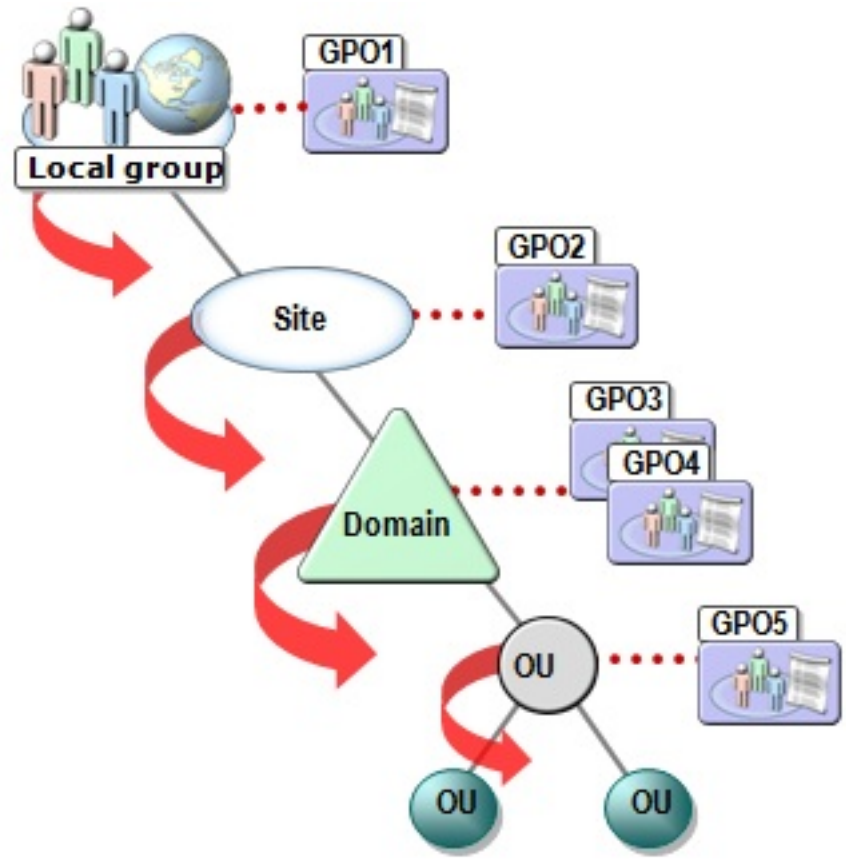
Group Policy Basics

Creating:

- Group Policy Objects Container
- How to copy a GPO

GPO Processing:

- Starts with Local policies
- Site->Domain->OU's
- Each overlays as you get closer to the object
- Link ordering on OU's
- Exceptions:
  - Enforced
  - Blocking Inheritance
- Filter GPO's based on:
  - Group membership
  - WMI
- Deny permission?



NC STATE UNIVERSITY

Group Policy Basics (continued)

Naming Conventions:

- <OU>-
- For software: <OU>-{SW,FW,EX}-
- Use descriptive GPO names, there is no length limit

Some "best practices":

- GPO's that provide access to a resource should be linked at the highest level that is administratively feasible.
- WMI filtering on specific versions of software usually doesn't get updated. Use WMI filters for OS, and Item-Level targeting in GPP for everything else you can.
- If you find yourself creating alot of GPO's to solve a single problem, you are likely doing something wrong.
- Clean up your GPO's, don't just delete the GPO Links.

Group Policy Diagnostics

gpupdate - initiate a Group Policy refresh (optional: /force)

Group Policy Results - What is applying now (Demo)

- Extremely useful for figuring out why a machine isn't behaving as you expect -- list every policy it sees and from which GPO its getting it. Use to identify inheritance issues.

Group Policy Modeling - Planning out changes before making them (currently limited to domain admins)

Group Policy Logging:

- http://technet.microsoft.com/en-us/library/cc775423(WS.10).aspx

GPP debug logging:

- Computer Configuration\Policies\Administrative Templates\System\Group Policy

http://technet.microsoft.com/en-us/library/cc787386(WS.10).aspx

NC STATE UNIVERSITY

Group Policy - WolfTech Specifics

WolfTech uses Loopback Processing (merge mode)

- User Settings still have to Apply to the User Account
- Why do we do this? What does that mean? (Demo)

"Enterprise Client" Policies

- Microsoft Baselines for each OS set as domain defaults
- http://activedirectory.ncsu.edu/services/base-infrastructure/default-security-policies/

Permissions:

- All OU Admins get Read to all GPO's (via script)
- Delegate permissions to <OU>-OU Admins group for GPO's following naming conventions mentioned earlier (via script)
- "Deny" permissions on GPO's should be used with care
  - Primary use case is in Software Distribution

Policies

Types of Policies:

- Software Deployment
- Scripts
- Security Settings
  - Restricted Groups (append or overwrite modes; Demo)
  - User Rights assignment
  - Machine Permissions (Filesystem, Registry, Services)
  - Software restriction
  - Configure Wireless
  - Role-based Windows Security Baselines already in WolfTech
    - WS08R2-Hyper-V, WS03 EC Print Servers Policy
- Administrative Templates
  - Firewall - no spaces in comma separated lists!
  - Windows Update, IE, Office, desktop environment, etc.
  - DNS Domain, DNS Search order
  - WSUS Groups (client-side targetting)

Preferences

Types of Preferences:

- Mapped Drives (Demo)
- Power Settings
- Printers (Demo)
- Distributing individual files, registry keys, shortcuts

Features of Preferences

- Collections (Registry only)
- You can copy/paste between GPO's for GPP!
- Item-Level Targeting lets you filter based off of:
  - IP Address/MAC Address/Battery State
  - Security Group/OU/User
  - Registry/File Match
  - Date/Time
  - and much, much, more! (**but don't go crazy)

http://activedirectory.ncsu.edu/ou-admins/tools/gmpc/group-policy-preferences/

Other Services

Software Distribution,WSUS,
WDS, SCCM

NC STATE UNIVERSITY

Software Distribution

- Naming: OU-{EX/FW/SW/DN}-Vendor-App-Version[-r#]
  - NCSU-SW-SAS-JMP-8.0.2
  - SW - Licensed Software
  - FW - Freeware
  - EX - Experimental (In testing, Use at own rise, etc.)
  - DN - Deny
- Installation Methods
  - GPO
  - SCCM
- Group Hierarchy
  - Groups Created in an "<OU> Software" OU replicates down to all child colleges/departments
- DEMO: ADToolkit Software Tools

Windows Server Update Services (WSUS)

Unified Patch Management for MS Products

- Apply patches based on grouping
  - Client Side Targeting via Group Policy (Demo)
  - Early, Normal and Late patch schedules
- Types of Patches:
  - Service Packs/Security Patches/Bugfixes/MS Defender defs
  - 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://www.wolftech.ncsu.edu/support/support/Active_Directory/Documentation/WSUS_Management_Console

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

NC STATE UNIVERSITY

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
- Groups: <OU>-Allow Imaging, <OU>-Computer Migrators
- NetBootGUID: Prestaging using 20 zeroes + MAC Address
- GUI tools for setting up:
  - Post-install scripts
  - Joining the domain

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

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
- activedirectory-patches@lists.ncsu.edu
- wds@lists.ncsu.edu

Jabber

- "activedirectory" on conference.jabber.eos.ncsu.edu

Remedy

- wolftech_ad_technical@remedy.ncsu.edu

Governance Committees

- http://activedirectory.ncsu.edu/governance/

NC STATE UNIVERSITY

Q & A

NC STATE UNIVERSITY