WolfTech Active Directory: OU Administration

June 30th, 2009

2-5pm Daniels 407

http://www.wolftech.ncsu.edu/activedirectory

Tools

- Remote Server Administration Tools (RSAT)
  - Vista SP1+ / 2008 version of AdminPak
  - Only way to access Group Policy Preferences
  - Includes all added functionality from 2003 R2
- GPMC - Included in Vista
  - VBScripts for doing GPO Scripting
- SpecOps GPUpdate - Extension for ADUC
- Scripting: VBScript/PowerShell
- ShellRunas - Run as different Domain User for Vista
  - Do not do administration with normal unity account
- Custom MMC Consoles
- DEMO!

NC STATE UNIVERSITY

Migration Checklist

1. Get your house in order:
    - DNS needs to be accurate, including DNS domains, use DHCP
    - Asset tracking needs to be accurate
    - Laptops - register in NOMAD
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?

Accounts

- Accounts already provisioned for all Unity
- Centrally managed
- Passwords synced via Password Change Page
- Units can create their own accounts:
  - more than 8 characters
  - Administrative: <UNITYID>.admin
  - Guests: <DEPT>.<FIRSTNAME>.<LASTNAME>
  - Service: <DEPT>.<SERVICENAME>.service

http://www.wolftech.ncsu.edu/support/support/Active_Directory/Naming_Standards

- Coming Soon:
  - Workshop Accounts
  - Cross Realm Trust

Grouping

"Best Practices":

- 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 Access

WolfTech Managed Groups

- Create Groups based on:
  - OUC
  - Affiliation
  - Building
  - Course Rolls
- Membership populated daily!
- Set expiration dates!

- http://www.wolftech.ncsu.edu/wtmg/

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 - no login, extremely locked down
  - Conference Rooms - any account login
  - Loaner machines
- Servers
- Macs? Linux boxes?

OU Layout Considerations

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

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

Desktops/Laptops OU's:

- Cron Job to help maintain group memberships

Group Policy Basics

Creating:

- Group Policy Objects Container
- How to copy a GPO
- Starter GPO's

GPO Processing:

- GPO processing starts at the root of the domain and overlays as you get closer to the object
- Link GPO's to OU's
- Link ordering on OU's
- Filter GPO's based on Group membership
- Filter GPO's based on WMI
- Enforced vs. Blocking Inheritance
- Deny permission?

NC STATE UNIVERSITY

Group Policy Basics (continued)

Naming Conventions:

- <OU>-
- For software: {SW,FW,EX}-<OU>-
- Be descriptive in your 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 doing something wrong.

Group Policy Diagnostics

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

Group Policy Results - What is applying now
Group Policy Modeling - Planning out changes before making them (currently doesn't work)

Group Policy Logging:

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

Group Policy - WolfTech Specifics

WolfTech uses Loopback Processing (merge mode)

Permissions:

- Cron:
  - All OU Admins get Read to all GPO's
  - Delegate permissions to <OU>-OU Admins group for GPO's following naming conventions mentioned earlier
- "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
  - User Rights assignment
  - Machine Permissions (Filesystem, Registry, Services)
  - Software restriction
  - Configure Wireless
  - Windows Security Guide Templates are already in WolfTech
    - {VSG, XP, WS03, WS08} EC
- Administrative Templates
  - Firewall - no spaces in comma separated lists!
  - Windows Update, IE, desktop environment, etc.
  - DNS Domain, DNS Search order
  - WSUS Groups (client-side targetting)

Software Distribution

- Naming: SW-OU-Vendor-App-Version-Build date
  - SW-NCSU-Mathworks-Matlab-7.6-20090605
- Assigned via GPO
  - "Remove when out of scope"
  - SW - Licensed Software
  - FW - Freeware
  - EX - Experimental (In testing, Use at own rise, etc.)
- Group Hierarchy
  - A Group Created at <OU> Software level will replicate down to all child colleges/departments

Preferences

Types of Preferences:

- Mapped Drives
- Power Settings
- Printers*
- Distributing individual files, registry keys, shortcuts
- Collections
- 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!

http://www.wolftech.ncsu.edu/support/support/Active_Directory/Documentation#Group_Policy_Preferences

Windows Software Update Services

WSUS is the freepatch distribution product provided by MS.

- All patches except drivers
- Approval Timelines:
  - Early, Normal, Late
  - Use GPO to set the Client Group: <DEPT>-Early
- Reports
  - http://www.wolftech.ncsu.edu/support/support/Active_Directory/Documentation/WSUS_Management_Console

http://www.wolftech.ncsu.edu/support/support/Active_Directory/Service_Groups#WSUS_Service_Group

Windows Distribution Services

WDS is the free image creation and deployment product provided by MS

- PXE - DHCP Templates (WDS-Main, WDS-Centennial, PXE-All)
- Base OS's + drivers
- Vista/Windows 7 are easy, XP works

http://www.wolftech.ncsu.edu/support/support/Active_Directory/Documentation/WDS

Scenarios

What are some problems that you need to solve?

Q & A

NC STATE UNIVERSITY