

# Active Directory: OU Administration

December 17th, 2008

1-4pm Daniels 407

# Workflow

## 1. Get your house in order:

- DNS needs to be accurate
- asset tracking needs to be accurate

## 1. Create or Join a domain?

- How are you going to handle Account creation? Do you need student accounts?
- Do you need to access campus resources? Wolfcopy? ACS Q: drive?

## 2. Design OU Layout

- Types of Users
- Types of computers
- Logical Units

## 3. Implement Management Policies

- Who can login where?
- What level of permissions should they have on each type of machine?
- Do you need to deploy Mapped Drives, Scripts, or Printers?

## 4. Setup Software Deployment Strategy

- Who can install their own software on what machines?
- What software packages need to be automated?

## 5. Migrate Current Machines

- Reinstall or Join?
- Pre-Staging Computer Objects
- Do you include Mac/Linux machines?

## 6. New Machine/Reinstallation strategy

- WDS

## 7. What other services will you need to provide?

# 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
- ShellRunas - Run as different Domain User for Vista
  - Do not do administration with normal unity account
- GPMC - Included in Vista
  - VBScripts in XP version for doing GPO Scripting
- SpecOps GPUUpdate - Extension for ADUC
- Scripting: VBScript/PowerShell

# OU Layout

- 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 (continued)

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

College

  \Department

    \Machine Type

      \Group1

      \Group2

Examples!

# Grouping

Creating lots of groups up front will ease administration when change requests are needed.

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.

- Groups 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

# Group Policy

## Creating:

- How to copy a GPO
- GPO Permissions
- Starter GPO's

## Filtering:

- Linking
- Groups
- WMI
- Deny permission?
- Enforced vs. Blocking Inheritance
- Loopback - Replace vs. Merge

GPO's are applied to an object starting at the root of the domain and overlaid as you get closer to the object.

GPMC: Group Policy Results/Group Policy Modelling

# Group Policy (continued)

Some "best practices":

- Naming Conventions are a must
- Be descriptive
- GPO's that provide access to a resource should be linked at the highest level that is administratively feasible.
- "Deny" permissions on GPO's should be used with care
- 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.
- Always do a "gpupdate" rather than relying on reboots when doing testing of new GPO settings.



# Policies/Preferences

## Policies:

- Software Deployment
- Scripts
- Security Settings
  - Restricted Groups
  - User Rights assignment
  - Machine Permissions (Filesystem, Registry, Services)
  - Software restriction
- Administrative Templates
  - Firewall - no spaces in comma separated lists!
  - Windows Update, IE, desktop environment, etc.

## Preferences:

- Mapped Drives
- Power Settings
- Distributing individual files, registry keys, shortcuts
- Item-Level Targeting

# Print Setup with GPOs

Using group policies, you can deploy, change, and remove printers from computers grouped together into an OU

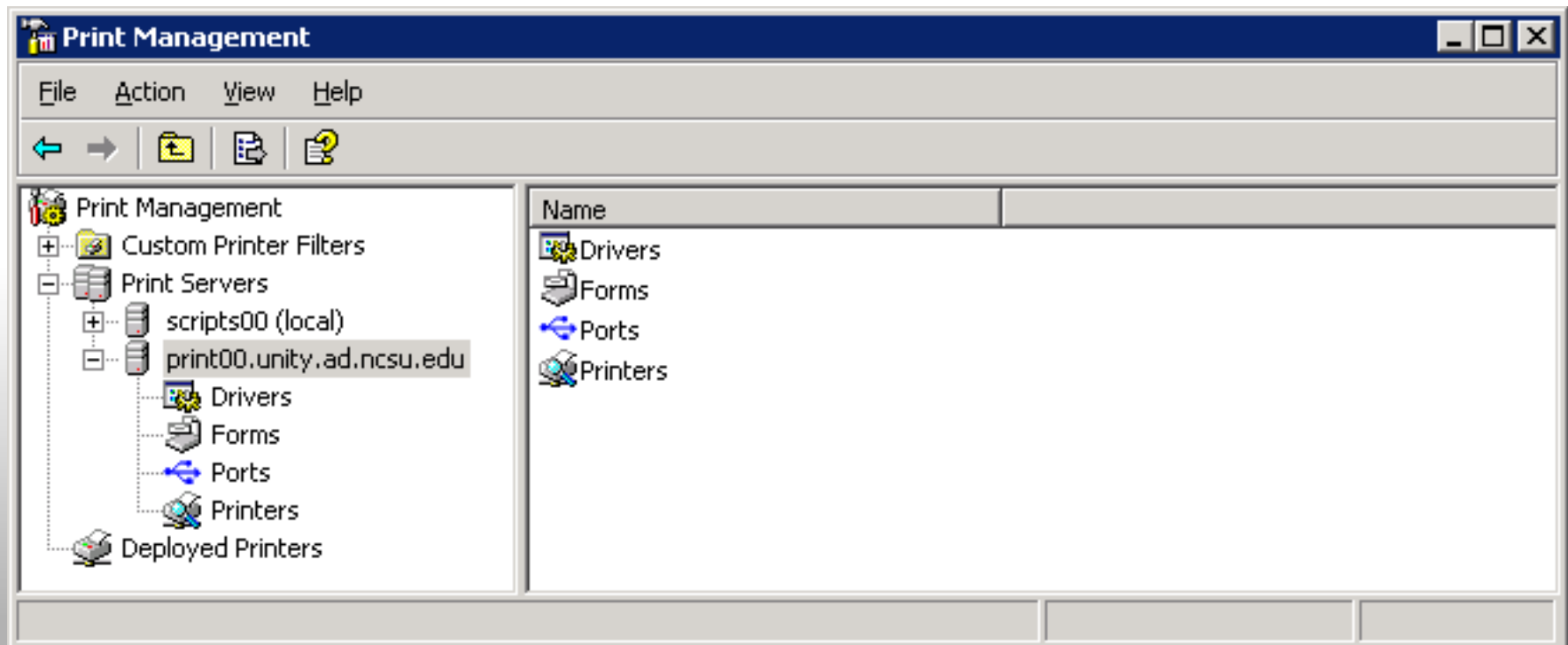
You will need administrative rights over the OU, and a workstation with the GPMC and print management plugins installed.



# Deploying the printers

**DO NOT** use the Group Policy Management Console to deploy printers. Printers can be successfully delivered when set up from GPMC, but they will not be successfully removed from workstations when they are disassociated from the policy.

Instead, you should **FIRST** create and link an empty policy to the OU where you wish the printer deployed, then associate it with the "Printer Management Console"



# Installing printers with scripts

Traditionally (prior to R2) printers are installed with scripts.

Tons of VB and Powershell (and Perl) examples on the web.

The "rundll32.exe" allows you to call functions in a DLL from the command line. All GUI print tasks can be performed with rundll32.

For on-line reference,

**rundll32 printui.dll,PrintUIEntry /?**

# Scenarios

What are some problems that you need to solve?

Q & A