

Field Notes on Active Directory Best Practices

August 2005

Domain Controllers

- Understand what the FSMO does and how services should be placed.
- Understand there is one “Domain Naming Master” and “Schema Master” per Forest.
- Understand there is one “RID Master”, “Infrastructure Master”, and “PDC Emulator” per Domain.
- Understand that the “Infrastructure Master” will not function properly if placed on a Global Catalog server. However, if the Active Directory consists of a single forest and a single domain you can make the same DC the “Infrastructure Master” and a Global Catalog (GC) without experiencing any problems.
- Have at least two DC’s/GC’s in each domain (unless running SBS). Users can not logon without a Global Catalog available on the network.

DNS Services

- Do not use the same DNS name for Active Directory which is used on the Internet.
- Use a non-Internet resolvable DNS name for Active Directory, such as “corp.domain.com” or “domain.local”.
- If at all possible use Active Directory integrated DNS; avoid using third-party services such as BIND. This may complicate the DNS update and location process, and add to troubleshooting complexity.
- Create Reverse DNS zones for all subnets on your network and assign these subnets to Active Directory Sites using the “Active Directory Sites and Services” MMC.
- Let Active Directory manage the zone names. Do not manually create child DNS zone’s for physical site locations. For example “chicago.corp.domain.com” or “denver.corp.domain.com”. The DNS zones are logical and based upon the Forest and Domain design, not on physical sites.

Organization Unit Structure

- Base the OU structure on administrative needs, or policy needs.
 - The structure does not have to mirror the company organizational chart.
 - If it does help simplify administration, the structure may reflect the organization.
- Use a basic OU design. This will reduce administrative overhead and directory query responses.
- Limit the number of OUs created and the number of levels. No more than 3 levels deep off of the root if possible.
- Have a process to “justify” any new OU that is under consideration.

Group Policy Object Basics

- Keep it Simple. The fewer number of Group Policies implemented is better for reducing the administration burden.
- Use the “Default Domain Policy” to only apply domain wide security settings, such as password and auditing policies, nothing more.
- Use the default “Authenticated Users” group to apply only site, domain, or OU wide settings.

- Use Security Group filtering to apply department, role based, or managed software policies.
- Use the Group Policy modeling and logging tools, found in the GPMC in designing new group policies and resolving potential conflicts.
- Understand the order of policy application. 1-Local, 2-Site, 3-Domain, 4-parent OU, 5-child OU, and so on.
- Understand any conflicting settings in the last policy to apply - which is closest to the user/machine object - will override previous settings. Unless a previous policy uses the “No Override” function.
- Do not use “Block Policy Inheritance” or “No Override” settings unless you fully understand how they work and the repercussions of using them. Using these options changes the generally understood rules (see above) of group policy processing.

Group Policy Object's for Software Installation

- Use only one installation package (including transform) per product version.
 - One installation package per physical site may be used.
- Only use a Group Policy to deploy software if multiple people will be using the software.
- Make use of Security Groups to “Assign” software to a machine (preferred) or a user object.
 - You can create a security group per package, for example “Install IE 6” or “Install Office 2003 Pro”, in order allow the installation package to assign the particular software.
- Use a minimum number of GPOs to deploy software packages. One Policy can contain instructions for many installation packages. This is where security groups play a large role.

Group Policy Object's for Login Scripts

- Design standard drive mappings for the entire organization, or site. For example, if you use a company wide file share, assign the same drive letter for this share across all departments in the organization.
- In order to reduce future drive mapping conflicts, make sure you “reserve” any standard drive mappings, so they are not used to assign a different share to this common drive letter for individual users.
- If you choose to assign login scripts using GPO's, create a script based upon per department or per site needs.
- If users across the organization or in a department require custom mappings, this can be accomplished by assigning a personal login script using their user object profile. This can in addition to, or instead of, using a company, department, or site login script via GPO as long as you follow the rule to reserve common drive letters – which will prevent mapping conflicts.

Group Policy Object's for Folder Redirects

- Use a minimum number Group Policies for Folder Redirection settings. Use only one Policy per site or department if possible.
- Consider implementing Dfs if user data is located across multiple file servers.

Group Policy Object's for Server and Workstation Lockdowns

- Use Group Policies to control user access for Terminal/Citrix Servers.
- Use Group Policies to lockdown "Role based" users or workstations.
- Use Group Policies to restrict control panel icons, Internet Explorer settings, proxy settings, Windows Update settings, and command prompt access for all users.

Online Resources:

- Windows 2003 Server Resource Kit, Deployment Guide, Designing and Deploying Directory and Security Services.
<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/DepKit/d2ff1315-1712-48e4-acdc-8cae1b593eb1.msp>
- White Paper "Designing OU and Group Structure in W2003"
<http://www.informit.com/articles/printerfriendly.asp?p=98126>

Copyright © 2005 by Jason Hartley. All rights reserved.

Use the information in this document at your own risk. The above best practices are based upon personal experience and considered personal field notes. No guarantee or warranty is made or implied in the accuracy of the content in this guide. Visiting Microsoft.com to obtain current design guidelines and recommendations is always advised.

Find more info at <http://www.itedge.net>