Lab #006

Intro to Group Policy: Nitpicking Details

Eric Webb and Jon Martin

Learning Objective: Navigate and learn the Group Policy Management Console (GPMC) and learn the basics of group policy management.

Equipment: No new equipment is required.

Notes: Computer password expired. cmst:315. Will be changed back when we get around to changing it. We can open up group policy management several ways, but we just went into server tools > gpm. Following the book, we set teredo state to enabled. We created a couple of gpos. One changes desktop background, and one restricts all but one ou from accessing the control panel. The main part of the lab was just exploring the management console, and observing that there are user and computer specific controls.

Diagrams: N/A

References: Only the book provided, Mastering Windows Group Policy.

Questions: Active Directory is built with the idea of using Group Policy. Group Policy can nitpick down to the smallest details what a user can and cannot do, better securing a network and enabling the users to find what they need. Local, Site, Domain, and OU is the hierarchy. Authenticated Users are the people affected by the default policy. Not Configured basically is the default, in that it won't seek to make any changes. Disabled might just entirely disable the service. With windows firewall, disabling it means it cannot be enabled, while not configured means the user has the choice to enable it. The default domain policy can only cover so many things. It really restricts you on what you can and can't separate. Creating several gpo's allows you to effectively control every detail, without the risk of conflict. Having many gpo's with minimal settings allows new users and computers to be added easily, just adding what they need. If I create one huge accounting policy, that works great until I need to give access to the hr folks. Or what if I need the head accountant to have more access? What if hr needs access to some functions that accounting has? If we have a "access" gpo, I could just give that to both of them. Gpupdate forces the update of policy, instead of waiting up to 90 minutes to take effect. Gpresult shows what policies have been applied to a workstation, which can be handy to use on remote computers to make sure the policy has been applied. In our lab, we made a gpo that disables use of the control panel, but blocked inheritance on one of our ou's. This allows the one to still have access, but makes sure the potentially hundreds of other ou's cannot. Enforcing gpo's moves the precedence to the top, while ignoring and inheritance blocking. You might block user configuration settings to ensure a user cannot mess with any programs/software you have installed, as well as maintain the settings you want. Testing a gpo on one or two computers allows you to double check that the changes you're making aren't going to cripple your network. It's easier to fix settings on a computer vs being denied access to the whole network. Deny changes are dangerous, as they trump allow access. With a deny in place, there's no real indicator of the deny, especially to users that aren't denied. If something changes and that user has a link removed, they might be denied access to that folder later, causing mass confusion. WMI can tell how much space is available, os version numbers, available ram, desktop/tablet, and so on. This can allow group policy to affect certain devices based on what type of device they are, as well as whatever ou they're in.

Conclusion: The main takeaway of this lab is the experience navigating the gpmc. Good stuff.