Windows Group Policy

Type of Systems: Windows Server 2012/2016/2019
Complete Goal: Create, push, and manage policies for the domain.

Overview

Get Started

First, you need to install group policy management tools. There is a GUI version called the Group Policy Management Console (gpmc.msc). There are also Powershell tools. The GUI will not work on Server Core, but you can use it from any domain-connected workstation.

With Powershell
> Get-WindowsCapability -Name Rsat.GroupPolicy* -Online | Add-WindowsCapability -Online

With GUI
Use the Add Roles and Features wizard to install the *Group Policy Management* role.

Server Manager Overview

Steps for creating GPO (Group Policy Overview) in Server Manager:

1. To create a GPO open the Group Policy Management Console (GPMC), go to `Server Manager → Tools → Group Policy Management`
2. Right-click on an `OU` → select the first option *Create a GPO in this domain and Link it here*.
3. Type the Name for this `GPO object → click OK button`.
4. Right-click the GPO object and click Edit.

Powershell Basics

Viewing GPO
> Get-gpo -name <GPO NAME>

The Get-GPO command returns a list of GPO objects. Some properties of an individual GPO object are:
Description
Owner
CreationTime
ID

Finding GPO
Every GPO object must be linked to places in the LDAP DN. View the links on a particular DN:

```
> Get-GPInheritence -Target <OU>
```

Enable or disable a link:

```
> Set-GPLink -Name <GPO Policy object> -Target <OU or group>
      -Enforced Yes -LinkEnabled Yes
```

Specific Tasks

Prevent Windows from Storing LAN Manager Hash

The LM hash is weak and prone to hacking. Therefore, you should prevent Windows from storing an LM hash of your passwords. Perform the following steps to do so:

1. In Group Policy Management Editor window (opened for a custom GPO), go to “Computer Configuration” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Network security: Do not store LAN Manager hash value on next password change” policy.
3. Select “Define this policy setting” checkbox and click “Enabled.
4. Click “Apply” and “OK”.

Steps for blocking an application:

1. Edit the Computer Configuration:
2. You will find the Software Restriction Policies under the path Computer Configuration –> Windows Settings –> Security Settings. Create New Software Restriction Policies:
3. Under the Security Levels you will be able to configure the default software execution permissions for the desired group.

   a. Unrestricted (the default setting) doesn't restrict software execution while Basic User allows only the execution of applications that don't need Administrator rights. Disallowed forbids software execution. With a right-click you can set a new default configuration:
4. The Additional Rules are important to restrict application usage. These rules override the default settings, so you can restrict all the applications and create specific rules to allow the execution of some of them or you can allow the execution of all the applications as default settings and restrict the few ones that bother you. We suggest to use the Path Rule, to restrict or allow the execution of files with a specific path:
5. In this example we are going to allow unrestricted execution for Mozilla Firefox. We can use the %UserProfile% parameter to create dynamic paths and restrict applications installed in the user folders: C:\Program Files\Mozilla **Firefox**\firefox.exe
   a. Another example: Type in to block test.exe in system32-> `%SystemRoot%\system32\test.exe`
6. Your policy is ready. Now drag and drop it in the distribution group:

Steps for changing local admin password through GPO

1. Start the Group Policy snap-in, expand **Computer Configuration**, expand **Preferences**, click **Control Panel**, and then right-click **Local Users and Groups**.
2. From the menu select **New - Local User**.
3. Select **Update** as the action, type **Administrator** into the User name text box, then type the new password into the Password text box, confirming the password in Confirm Password text box. Press **OK**.

Disallow Removable Media Drives, DVDs, CDs, and Floppy Drives

Removable media drives are very prone to infection, and they may also contain a virus or malware. If a user plugs an infected drive to a network computer, it can affect the entire network. Similarly, DVDs, CDs and Floppy Drives are prone to infection.

It is therefore best to disable all these drives entirely. Perform the following steps to do so:

1. In Group Policy Management Editor window (opened for a custom GPO), go to "User Configuration" "Policies" "Administrative Templates" "System" "Removable Storage Access".
2. In the right pane, double-click "All removable storage classes: Deny all accesses" policy

3. Click “Enabled” to enable the policy.
4. Click “Apply” and “OK”.

Disable Guest Account

1. In Group Policy Management Editor (opened for a custom GPO), go to “Computer Configuration” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Accounts: Guest Account Status” policy.
3. Select “Define this policy setting” checkbox and click “Disabled”.
4. Click “Apply” and “OK”.

Disable Anonymous SID Enumeration

1. In Group Policy Management Editor window, go to “Computer Configuration” “Policies” “Windows Settings” “Security Settings” “Local Policies” “Security Options”.
2. In the right pane, double-click “Network Access: Do not allow anonymous enumeration of SAM accounts and shares” policy setting.
3. Select “Define this policy setting” checkbox and click “Disable” to disable it.
4. Click “Apply” and “OK”.

Some specific Windows Group Policy to set

Security Options

● Network security: LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM
● Network security: Do not store LAN Manager hash value on next password change - Enabled
● Network access: Do not allow anonymous enumeration of SAM accounts and shares - Enabled
● Network access: Do not allow anonymous enumeration of SAM accounts - Enabled
● Network access: Allow anonymous SID/name translation - Disabled
● Accounts: Rename administrator account - Rename to something unique (but remember it)
● Interactive logon: Message text for users attempting to log on - sometimes an inject