WILEY

SYBEX
A Wiley Brand

MCA: Windows Server Hybrid Administrator Study Guide: AZ-800 & AZ-801

Chapter 8: Understanding Group Policies

Introducing Group Policy

- Windows Server 2022 group policies are designed to allow system administrators the ability to customize end-user settings and to place restrictions on the types of actions that users can perform.

- Group policies can be easily created by systems administrators and then later applied to one or more users or computers within the environment.

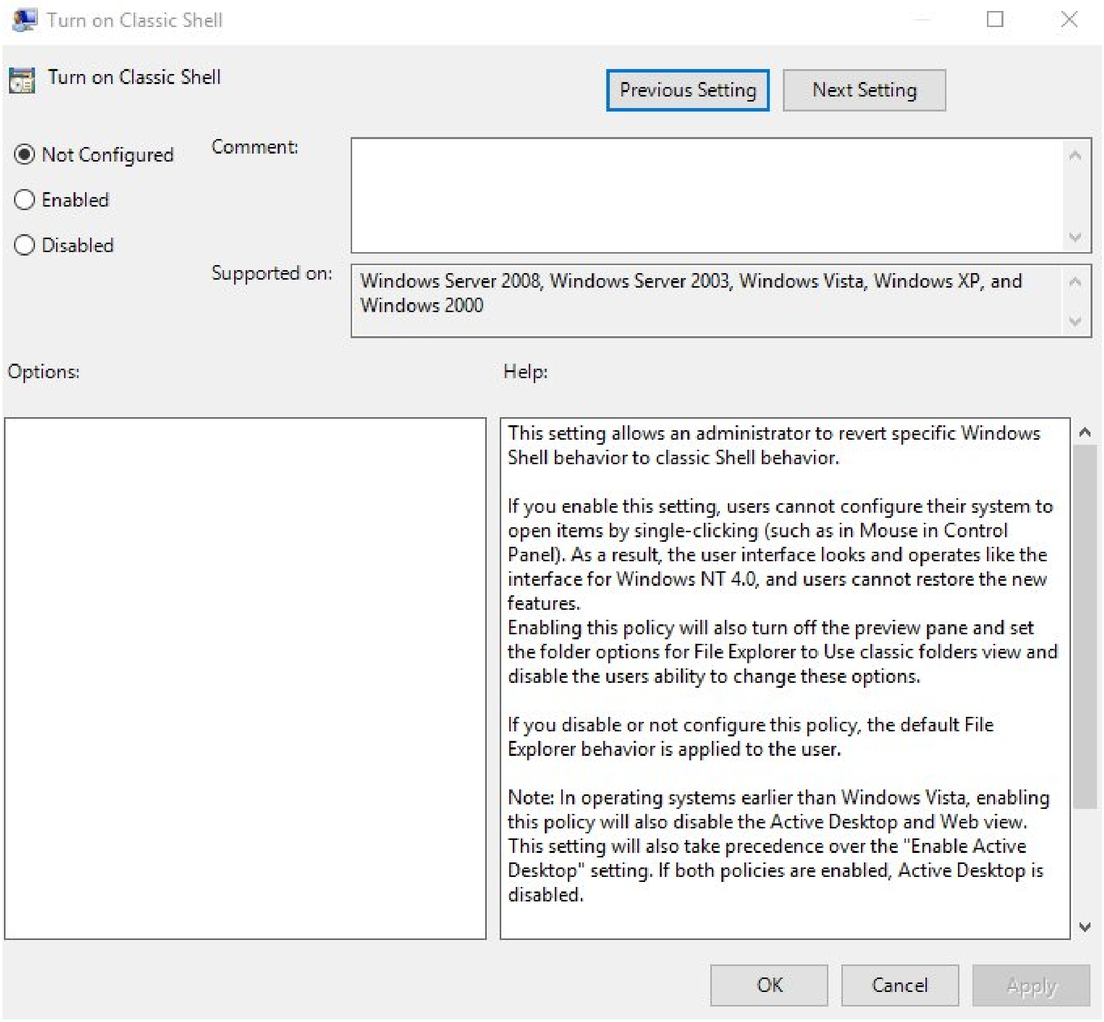
- Although they ultimately do affect Registry settings, it is much easier to configure and apply settings through the use of Group Policy than it is to manually make changes to the Registry.

- For ease of management, Group Policy settings are all managed from within the MMC called Group Policy Management Console (GPMC).

Group Policy Settings

- **Enabled**
  - Specifies that a setting for this Group Policy object has been configured
  - Some settings require values or options to be set
- **Disabled**
  - Specifies that this option is disabled for client computers
- **Not Configured**
  - Specifies that these settings have been neither enabled nor disabled
  - Not Configured is the default option for most settings
  - It simply states that this Group Policy will not specify an option and that other policy settings may take precedence

Group Policy Configuration Settings



● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: Windows Server 2008, Windows Server 2003, Windows Vista, Windows XP, and Windows 2000

This setting allows an administrator to revert specific Windows Shell behavior to classic Shell behavior.

If you enable this setting, users cannot configure their system to open items by single-clicking (such as in Mouse in Control Panel). As a result, the user interface looks and operates like the interface for Windows NT 4.0, and users cannot restore the new features.
Enabling this policy will also turn off the preview pane and set the folder options for File Explorer to Use classic folders view and disable the users ability to change these options.

If you disable or not configure this policy, the default File Explorer behavior is applied to the user.

Note: In operating systems earlier than Windows Vista, enabling this policy will also disable the Active Desktop and Web view. This setting will also take precedence over the "Enable Active Desktop" setting. If both policies are enabled, Active Desktop is disabled.

Group Policy Settings

The main options to configure within user and computer group policies are:

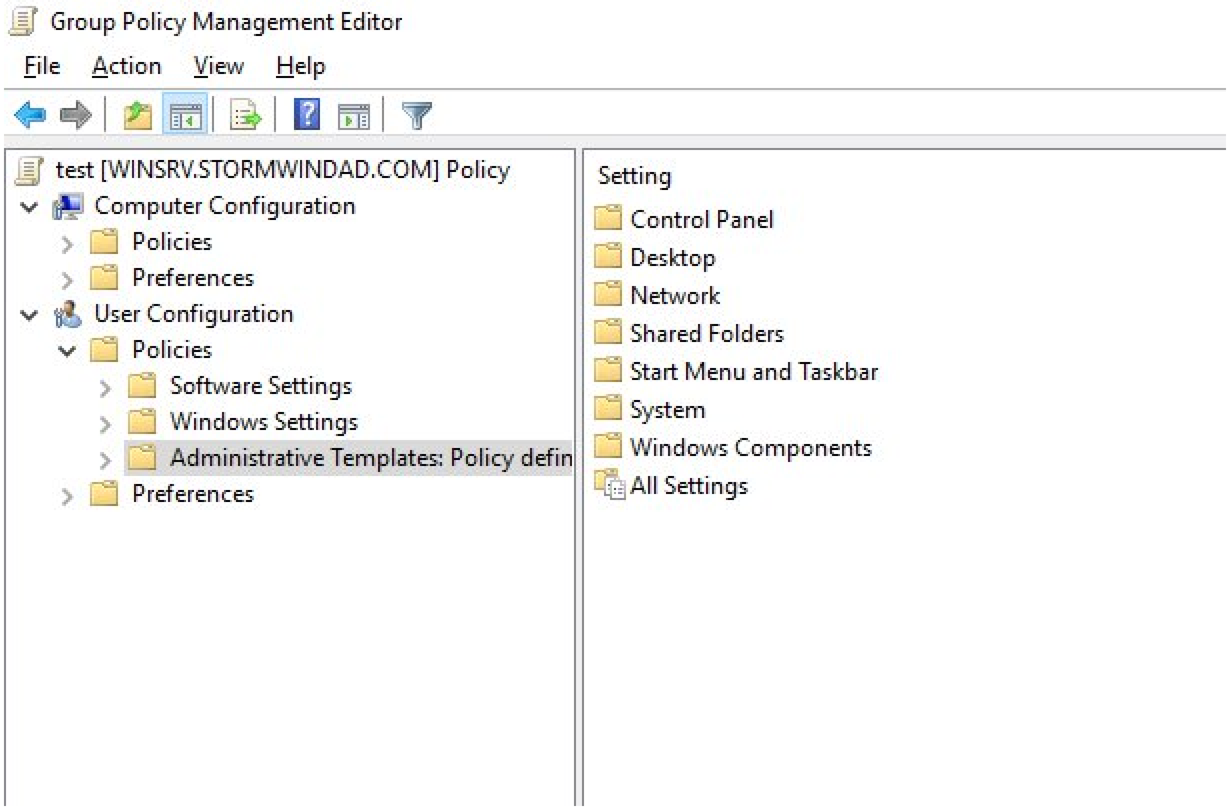
- **Software Settings**
  - Apply to specific applications and software that might be installed on the computer.
  - Systems administrators can use these settings to make new applications available to end users and to control the default configuration for these applications.
- **Windows Settings**
  - Allow systems administrators to customize the behavior of the Windows operating system.
  - The specific options that are available here are divided into two types: users and computers.
  - User-specific settings let you configure Internet Explorer (including the default home page and other settings).
  - Computer settings include security options, such as account policy and event log options.
- **Administrative Templates**
  - Are used to further configure user and computer settings.
  - In addition to the default options available, systems administrators can create their own administrative templates with custom options.

Group Policy Settings - Continued

- **Group Policy Preferences (GPP)**
  - More than 20 additional Group Policy extensions.
  - Give an administrator the ability to deploy settings for client computers without restricting the users from changing the settings.
  - Allows an administrator the flexibility needed to decide which settings to enforce and which settings to not enforce.
- **ADMX Central Store**
  - Optional repository for all administrative templates and it is checked by the Group Policy tools.
  - Be able to edit domain-based GPOs by using the ADMX files that are stored in the ADMX central store.
- **Security Template**
  - Used to configure security settings through a GPO.
  - Setting can be set for account and local policies, event logs, restricted groups, system services, and the registry.
- **Starter GPO**
  - The ability to store a collection of Administrative Template policy settings in a single object.
  - When created from a Starter GPO the new GPO receives the settings and values that were defined from the Administrative Template policy in the Starter GPO.

Group Policy Options

Some of the options you can configure with Group Policy.



Group Policy Management Editor

- test [WINSRV.STORMWINDAD.COM] Policy
  - Computer Configuration
    - Policies
    - Preferences
  - User Configuration
    - Policies
      - Software Settings
      - Windows Settings
      - Administrative Templates: Policy defin
    - Preferences

Setting

- Control Panel
- Desktop
- Network
- Shared Folders
- Start Menu and Taskbar
- System
- Windows Components
- All Settings

Security Settings

- Computer Section Only of the GPO
  - Account Policies
  - Local Policies
  - Event Policies
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wired Network
  - Windows Firewall with Advance Security
  - Network List Manager Policies
  - Wireless Networks
  - Network Access Protection
  - Application Control Policies
  - IP Security Policies
  - Advanced Audit Policy Configuration
- Computer and User Sections of the GPO
  - Public Key Policies
  - Software Restriction Policy

Additional Security Tools

- Restricted Groups
  - allows control of group membership by using a GPO.
- Software Restriction Policy
  - give administrators the ability to identify software and to control its ability to run on the user’s local computer, organizational unit, domain, or site.

Client-Side Extensions

- In Windows Server, group policies are designed using both server-side and client-side extensions (CSEs).

- The server-side elements include a user interface for creating each Group Policy Object (GPO).

- When a Windows client system logs into the Active Directory network, the client-side extensions (normally a series of DLL files) receive their GPOs and the GPOs make changes to the Windows client systems.

Group Policy Objects

- GPOs act as containers for the settings made within Group Policy files, which simplifies the management of settings.
- Group Policy settings are hierarchical.
- These levels determine the GPO processing priority:
  - Local
  - Sites
  - Domains
  - Organizational Units

Group Policy Inheritance

- **Block Policy Inheritance**
  - Specifies that Group Policy settings for an object are not inherited from its parents.
  - This might be used, for example, when a child OU requires completely different settings from a parent OU.
- **Force Policy Inheritance**
  - The Enforced (sometimes referred as the NO Override) option can be placed on a parent object and ensures that all lower-level objects inherit these settings.
  - In some cases, systems administrators want to ensure that Group Policy inheritance is not blocked at other levels.
  - The Enforce option overrides the Block Policy Inheritance option.

Creating GPOs (1/2)

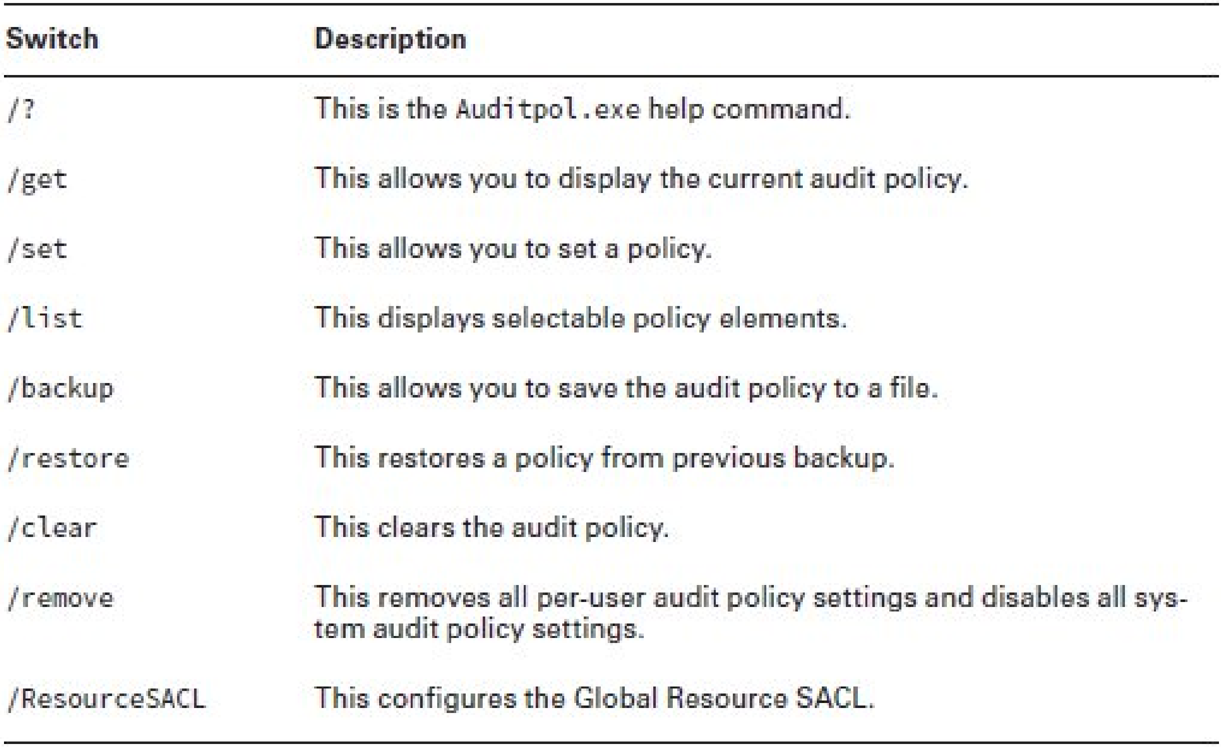
Have your choice of three applications for setting up policies on your Windows Server 2022 computers:

- **Local Computer Policy Tool -** This administrative tool allows you to quickly access the Group Policy settings that are available for the local computer.
- **Group Policy Management Console -** Must use the GPMC to manage Group Policy deployment. The GPMC provides a single solution for managing all Group Policy–related tasks.
- **Auditpol.exe -** a command-line utility to display information about policies and also to perform some functions to manipulate audit policies.

Creating GPOs (2/2)

1. Open the MMC by typing **MMC** in the Run command box.
2. Click File and then click Add/Remove Snap-in.
3. From the available snap-ins list, choose Group Policy Object Editor and click Add.
4. In the Select Group Policy Object dialog box, click the Browse button.
5. Click the Users tab in the Browse For The Group Policy Object dialog box.
6. Click the user or group for which you want to create or edit a local Group Policy and click OK.
7. Click Finish and then click OK.
8. Configure the multiple policy settings.

Auditpol.exe Switches



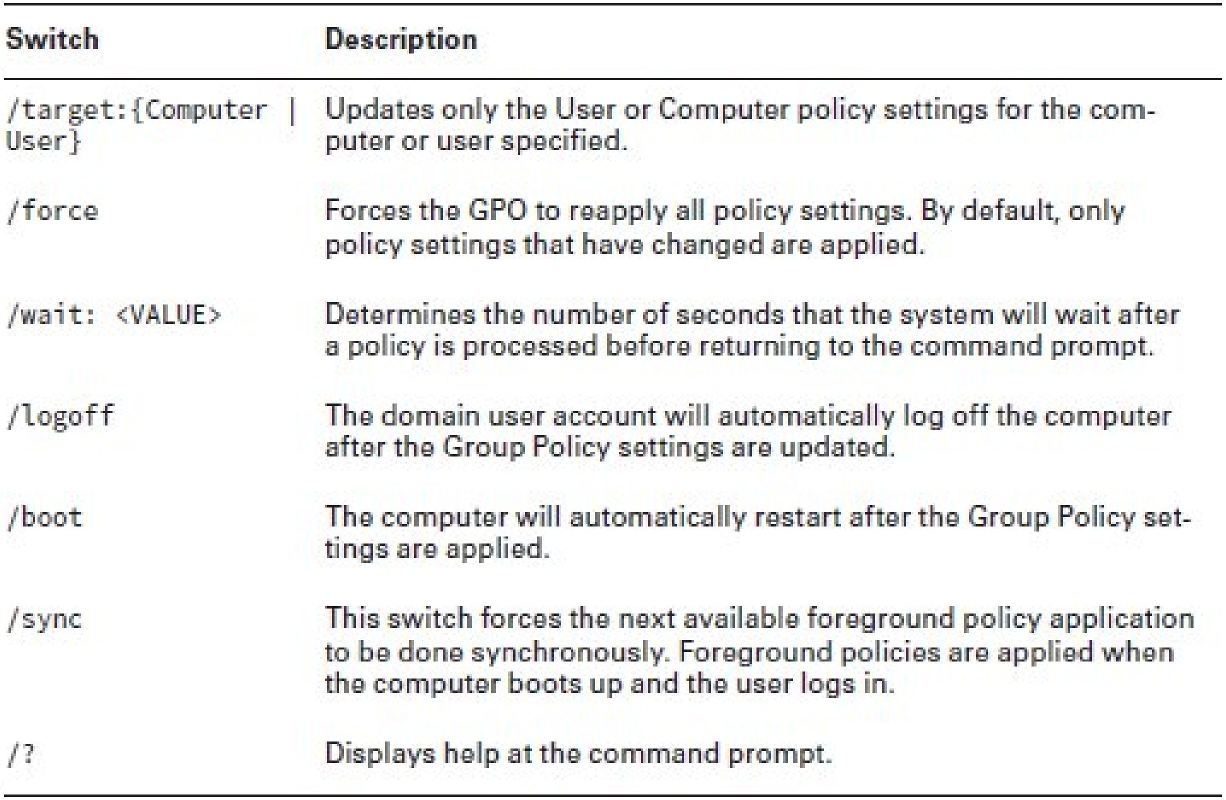
Switch	Description
`/?`	This is the `Auditpol.exe` help command.
`/get`	This allows you to display the current audit policy.
`/set`	This allows you to set a policy.
`/list`	This displays selectable policy elements.
`/backup`	This allows you to save the audit policy to a file.
`/restore`	This restores a policy from previous backup.
`/clear`	This clears the audit policy.
`/remove`	This removes all per-user audit policy settings and disables all system audit policy settings.
`/ResourceSACL`	This configures the Global Resource SACL.

Forcing a GPO to Update

In a Windows Server 2022 domain, when a user logs onto the domain, the latest version of the Group Policy gets downloaded from the domain controller, and it writes that policy to the local store.

- Forcing the GPO from the Server
- Forcing the GPO from the Client

GPUpdate.exe

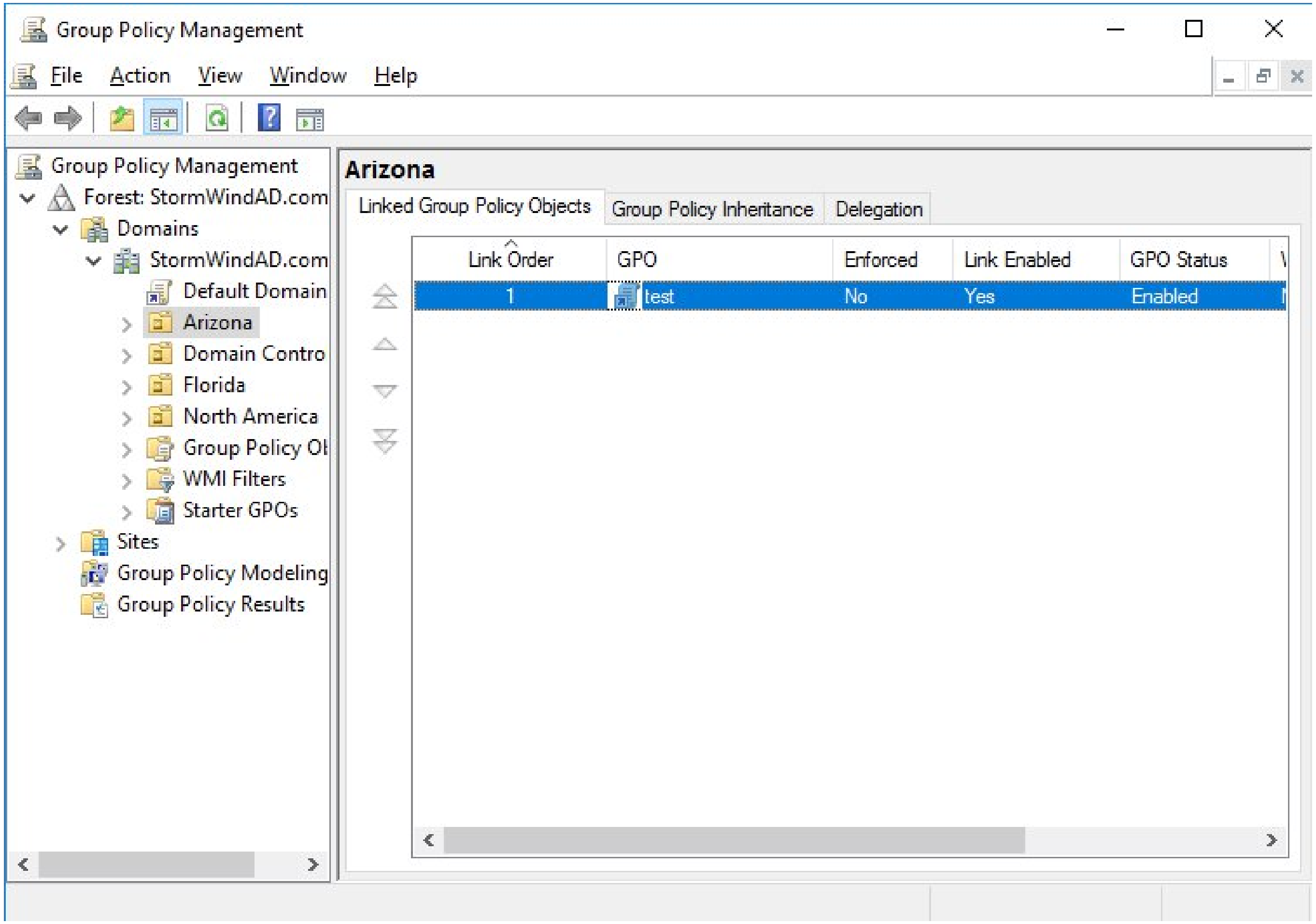


Switch	Description
`/target:{Computer | User}`	Updates only the User or Computer policy settings for the computer or user specified.
`/force`	Forces the GPO to reapply all policy settings. By default, only policy settings that have changed are applied.
`/wait: <VALUE>`	Determines the number of seconds that the system will wait after a policy is processed before returning to the command prompt.
`/logoff`	The domain user account will automatically log off the computer after the Group Policy settings are updated.
`/boot`	The computer will automatically restart after the Group Policy settings are applied.
`/sync`	This switch forces the next available foreground policy application to be done synchronously. Foreground policies are applied when the computer boots up and the user logs in.
`/?`	Displays help at the command prompt.

Managing Group Policy

- GPOs is that they're modular and can apply to many different objects and levels within Active Directory.
- A common administrative function related to using GPOs is finding all of the Active Directory links for each of these objects.
- You can do this when you are viewing the Linked Group Policy Objects tab of the site, domain, or OU in the GPMC.

Viewing GPO Links to an Active Directory OU



Link Order	GPO	Enforced	Link Enabled	GPO Status
1	test	No	Yes	Enabled

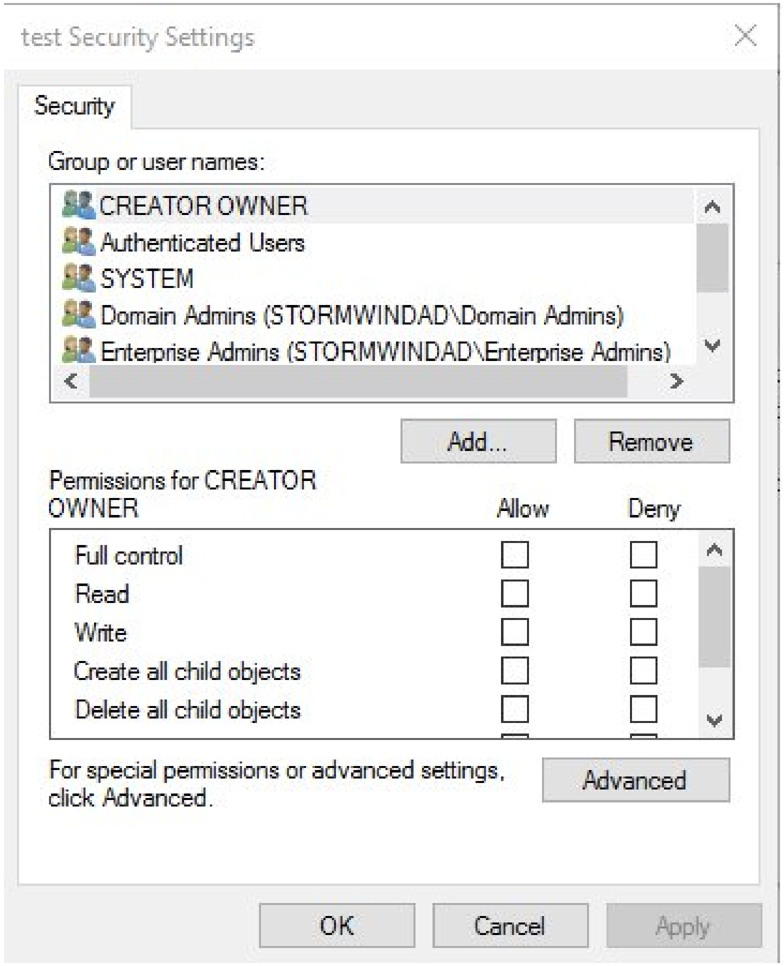
Windows Management Instrumentation (WMI)

- WMI scripts are used to gather information or to help GPOs deploy better.
- Can use WMI scripts to check for computer information such as MAC addresses.
- WMI is a powerful tool because if you know how to write scripts, the possibilities are endless.

Security Filtering of a Group Policy

Another method of securing access to GPOs is to set permissions on the GPOs themselves.

You can do this by opening the GPMC, selecting the GPO, and clicking the Advanced button in the Delegation tab.



test Security Settings

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (STORMWINDAD\Domain Admins)
- Enterprise Admins (STORMWINDAD\Enterprise Admins)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

GPO Permissions

The permissions options include the following:

- Full Control
- Read
- Write
- Create All Child Objects
- Delete All Child Objects
- Apply Group Policy

Delegating Administrative Control of GPOs

It’s important to establish the appropriate security on GPOs themselves for two reasons.

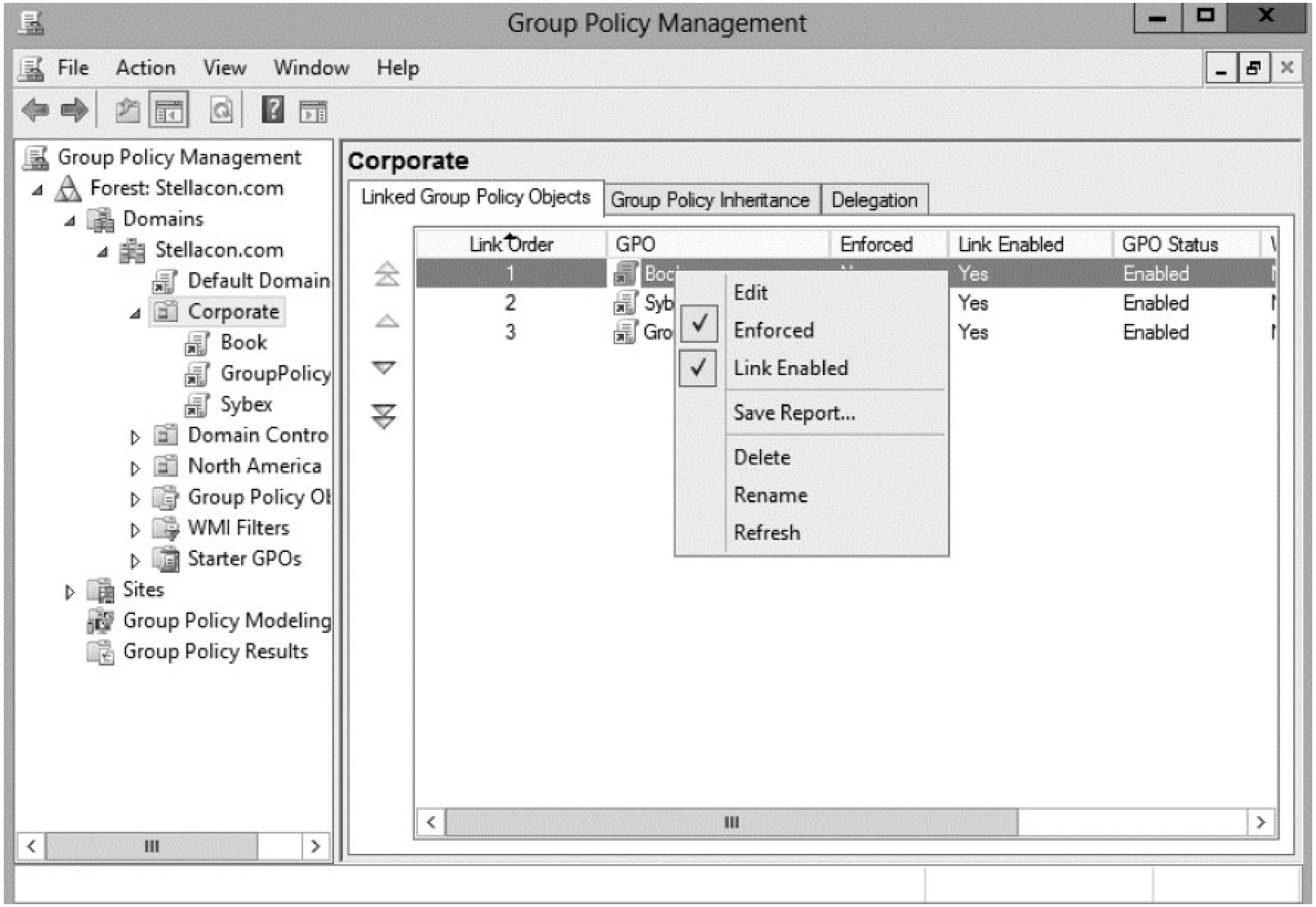
- If the security settings aren’t set properly, users and system administrators can easily override them.
- Having many different system administrators creating and modifying GPOs can become extremely difficult to manage. When problems arise, the hierarchical nature of GPO inheritance can make it difficult to pinpoint the problem.

Controlling Inheritance and Filtering Security Group Policy

- By default, GPO settings flow from higher-level Active Directory objects to lower-level ones.

- System administrators can also force inheritance. By setting the Enforced option, they can prevent other system administrators from making changes to default policies.

Setting the Enforced GPO Option



Corporate

Link Order	GPO	Enforced	Link Enabled	GPO Status
1	Boo		Yes	Enabled
2	Syb		Yes	Enabled
3	Gro		Yes	Enabled

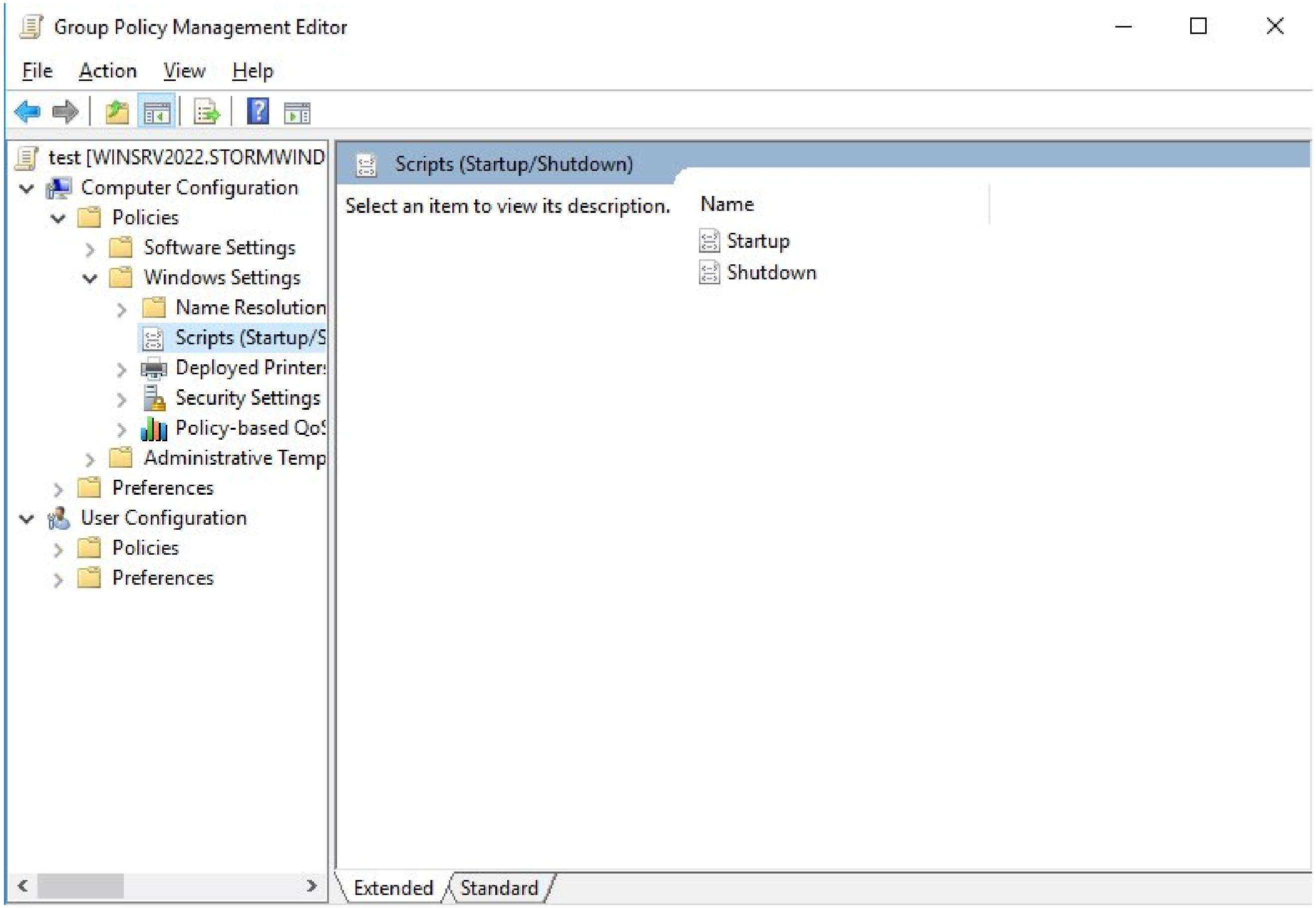
✓ Enforced

✓ Link Enabled

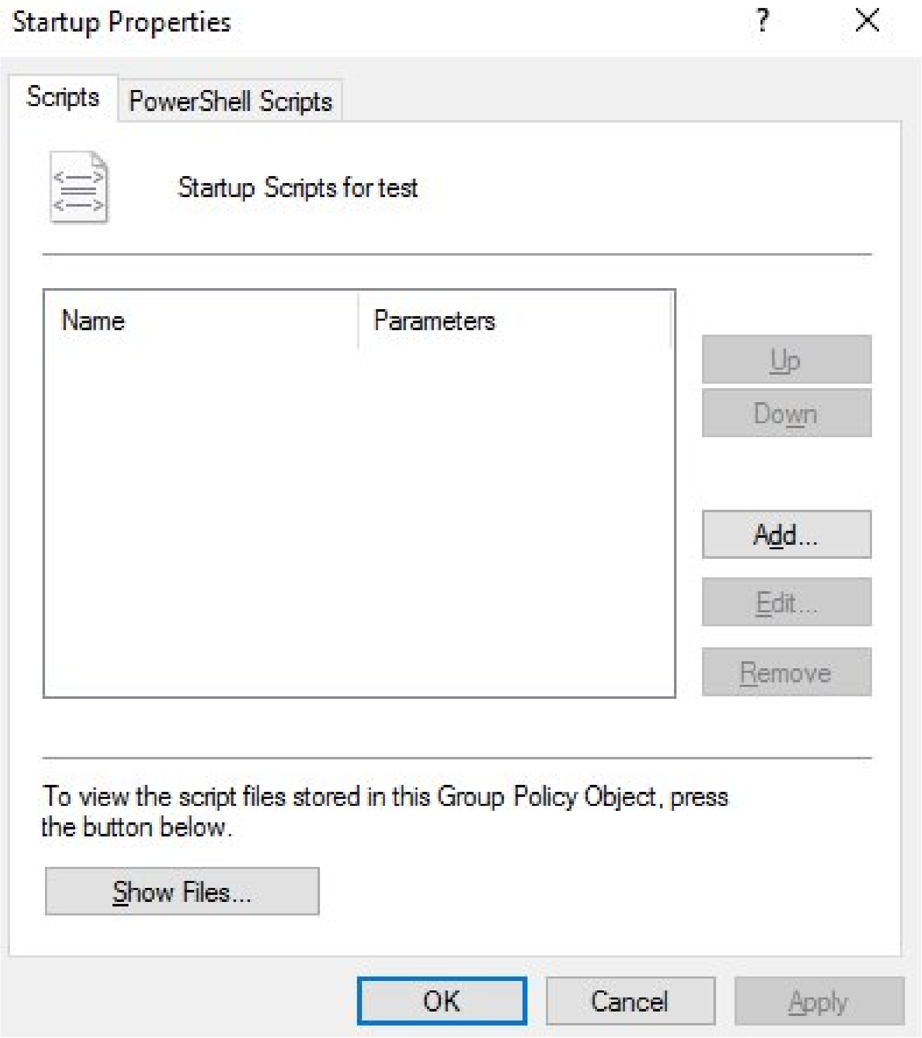
Assigning Script Policies

- Script policies are specific options that are part of Group Policy settings for users and computers.
- To set script policy options, simply edit the Group Policy settings.
- There are two main areas for setting script policy settings:
  - **Startup/Shutdown Scripts -** These settings are located within the Computer Configuration ➢ Windows Settings ➢ Scripts (Startup/Shutdown) object.
  - **Logon/Logoff Scripts** These settings are located within the User Configuration ➢Windows Settings ➢ Scripts (Logon/Logoff) object.

Viewing Startup/Shutdown Script Policy Settings



Setting Scripting Options



Startup Properties

Scripts | PowerShell Scripts

Startup Scripts for test

Name	Parameters

To view the script files stored in this Group Policy Object, press the button below.

Loopback Policy

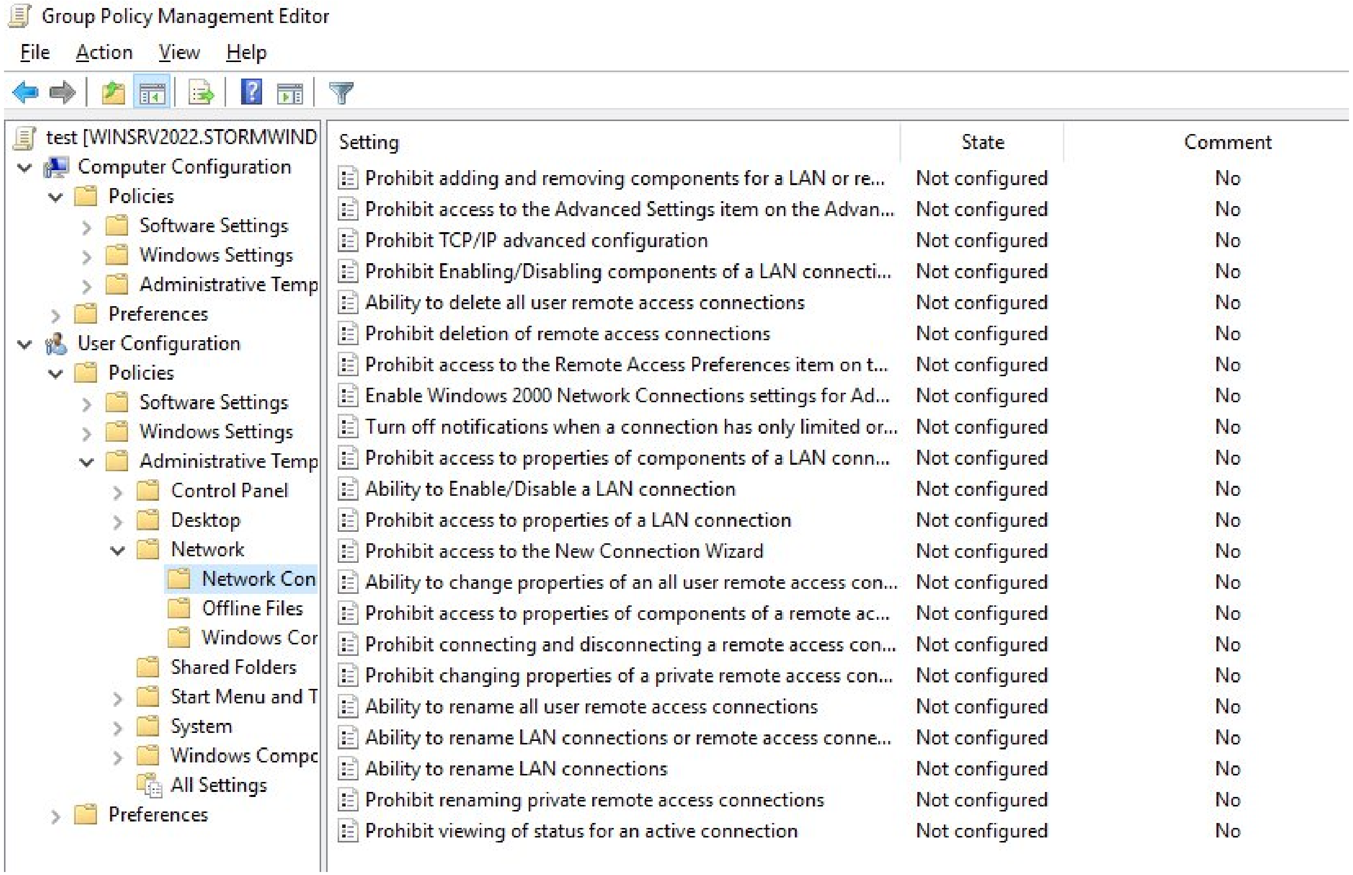
- Used when user settings of a Group Policy Object should be applied to a computer, based on its location, instead of the user object.
- Two ways to retrieve the list of GPOs for any user when using a specific computer in an OU
  - **Merge Mode** - The GPOs for the computer are added to the end of the GPOs for the user. Because of this, the computer's GPOs have higher precedence than the user's GPOs.
  - **Replace Mode** - In the Replace mode, the user's GPOs are not used. Only the GPOs of the computer object are used.

Managing Network Configuration

- **Computer Network Options -** These settings are located within the Computer Configuration ➢ Administrative Templates ➢ Network ➢ Network Connections folder.
- **User Network Options -** User Configuration ➢Administrative Templates ➢ Network.

- Some examples of the types of settings available:
  - The ability to allow or disallow the modification of network settings.
  - The ability to allow or disallow the creation of Remote Access Service (RAS) connections.
  - The ability to set offline files and folders options.

Viewing Group Policy User Network Configuration Options



Setting	State	Comment
Prohibit adding and removing components for a LAN or re...	Not configured	No
Prohibit access to the Advanced Settings item on the Advan...	Not configured	No
Prohibit TCP/IP advanced configuration	Not configured	No
Prohibit Enabling/Disabling components of a LAN connecti...	Not configured	No
Ability to delete all user remote access connections	Not configured	No
Prohibit deletion of remote access connections	Not configured	No
Prohibit access to the Remote Access Preferences item on t...	Not configured	No
Enable Windows 2000 Network Connections settings for Ad...	Not configured	No
Turn off notifications when a connection has only limited or...	Not configured	No
Prohibit access to properties of components of a LAN conn...	Not configured	No
Ability to Enable/Disable a LAN connection	Not configured	No
Prohibit access to properties of a LAN connection	Not configured	No
Prohibit access to the New Connection Wizard	Not configured	No
Ability to change properties of an all user remote access con...	Not configured	No
Prohibit access to properties of components of a remote ac...	Not configured	No
Prohibit connecting and disconnecting a remote access con...	Not configured	No
Prohibit changing properties of a private remote access con...	Not configured	No
Ability to rename all user remote access connections	Not configured	No
Ability to rename LAN connections or remote access conne...	Not configured	No
Ability to rename LAN connections	Not configured	No
Prohibit renaming private remote access connections	Not configured	No
Prohibit viewing of status for an active connection	Not configured	No

Configuring Network Settings

- In Windows Server 2022, you can set a lot of user and network settings by using GPOs.

- To configure any of these settings, open the Group Policy Management Console and choose the GPO you want to edit.

Computer Certificates in Group Policy

- Certificates are one part of what security experts call a *public-key infrastructure (PKI)*.

- A PKI has several different components that you can mix and match to achieve the desired results. Microsoft's PKI implementation offers the following functions:
  - Certificate Authorities
  - Certificate Publishers
  - PKI-Savvy Applications
  - Certificate Templates

Redirecting Folders

- Documents are always available no matter where the user logs on.
- Data in the shared location can be backed up during the normal backup cycle without user intervention.
- Data can be redirected to a more robust server-side-administered disk that is less prone to physical and user errors.
- When you decide to redirect folders, you have two options: basic and advanced.
  - **Basic** redirection redirects everyone’s folders to the same location (but each user gets their own folder within that location).
  - **Advanced** redirection redirects folders to different locations based on group membership. For instance, you could configure the Engineers group to redirect their folders to `\\Engineering1\My_Documents` and the Marketing group to `\\Marketing1\My_Documents`.

Managing GPOs with Windows PowerShell

Windows PowerShell can help automate many of the same tasks that you perform using the Group Policy Management Console.

- The Windows PowerShell Group Policy cmdlets can help you perform some of the following:
  - Maintain, create, remove, back up, and import GPOs
  - Create, update, and remove GPO links to Active Directory containers
  - Set Active Directory OUs and domain permissions and inheritance flags
  - Configure Group Policy registry settings
  - Create and edit Starter GPOs

Item-Level Targeting

- Battery Present Targeting
- Computer Name Targeting
- CPU Speed Targeting
- Date Match Targeting
- Disk Space Targeting
- Domain Targeting
- Environment Variable Targeting
- File Match Targeting
- IP Address Range Targeting
- Language Targeting
- LDAP Query Targeting
- MAC Address Range Targeting
- MSI Query Targeting
- Network Connection Targeting
- Operating System Targeting

Item-Level Targeting - Continued

- Organizational Unit Targeting
- PCMCIA Present Targeting
- Portable Computer Targeting
- Processing Mode Targeting
- RAM Targeting
- Registry Match Targeting
- Security Group Targeting
- Site Targeting
- Terminal Session Targeting
- Time Range Targeting
- User Targeting
- WMI Query Targeting

Restoring a GPO

There are normally two reasons why you have to restore a GPO—you accidently deleted the GPO, or you need to restore the GPO to a previous state.

Restoring a GPO:

1.Open the Group Policy Management Console.
2.In the console tree, right-click Group Policy Objects and choose Manage Backups.
3.Choose the backup you want to restore and click the Restore button.

Importing or Copying GPOs

There may be times when you need to import or copy a GPO from one domain to another domain.

An administrator can use the import or copy-to-transfer settings from one GPO to another GPO within the same domain, to a GPO in another domain in the same forest, or to a GPO in a domain in a different forest.

Importing or copying a GPO:

1.Open the Group Policy Management Console.

2.In the console tree, right-click Group Policy Objects and choose either Import Settings or Copy.

Migration Tables

- Migration tables tell you how domain specific settings should be treated when the GPO is moved from the domain in which it was created to another domain.
- Three settings that can be used:
  - Do Not Use A Migration Table
  - Use A Migration Table
  - Use A Migration Table Exclusively

Resetting the Default GPO

- To reset the default GPO to its original settings:

```
DCGPOFix [/ignoreschema]
[/target: {Domain | DC |
Both}] [/?]
```