Lesson 19: Configuring Group Policy Processing

MOAC 70-411: Administering Windows Server 2012
Overview

• Exam Objective 4.2: Configure Group Policy Processing
• Understanding Group Policy Processing
Understanding Group Policy Processing

Lesson 19: Configuring Group Policy Processing
Group Policies and GPOs

- Group policies are defined using group policy objects (GPOs).
- GPOs are the collection of configuration instructions that the computer processes.
- To assign a group policy, it is linked to an Active Directory container (site, domain, or organizational unit).
Scoping a GPO

Mechanisms for scoping a GPO:

• A GPO link to a site, domain, or organizational unit (OU)
• The GPO link enabled or disabled
• Enforced option of the GPO
• The Block Inheritance option of an OU
• Security group filtering
• WMI filtering
• Loopback policy processing
• Preferences targeting (discussed in Lesson 22)
Configuring Processor Order and Precedence

1. When a computer first starts up, it establishes a secure link between the computer and a domain controller.
2. The computer obtains a list of GPOs that are applied to the computer.
3. Computer configuration settings are applied synchronously (one by one) during computer startup before the Logon dialog box is presented to the user.
4. When the computer configuration settings have been applied and the startup scripts have been applied, users have the Ctrl+Alt+Del option to log on.
5. A user is authenticated and the user profile is loaded.

6. The computer obtains a list of GPOs that are applied to the user. Again, GPO processing is hidden from the user.

7. After the user policies run, any logon scripts defined by GPOs run. Scripts are executed asynchronously.

8. The login script defined for the user in Active Directory user properties is executed.

9. The user’s desktop is displayed.
Understanding Group Policy Inheritance

A computer and user can be affected by multiple GPOs. GPOs are processed in the following order:

1. Local group policy
2. Site
3. Domain
4. OU

A Group Policy uses inheritance in which settings are inherited from the container above.
Understanding Group Policy Inheritance

When Active Directory is installed, two domain GPOs are created by default:

- **Default Domain Policy**: Linked to the domain. It affects all users and computers in the domain including domain controllers. It specifies the password, account lockout, and Kerberos policies.

- **Default Domain Controller Policy**: Linked to the Domain Controllers organization unit, which then affects the domain controllers. It contains the default user rights assignments.
Understanding Group Policy Inheritance

Displaying GPOs for a domain
Change the Precedence of a GPO

Changing the precedence
Managing Group Policy Links

To disable a group policy for a container, you right-click the GPO for the container and click the *Link Enabled* link.
Managing Group Policy Links

Showing a link is enabled for a GPO
Managing Group Policy Links

After a GPO is created, you can:

• View the containers that a GPO is linked to by clicking the GPO in Group Policy Management and viewing the Scope tab.

• Delete a link to a container for a GPO without deleting the GPO by right-clicking the GPO for a container and clicking Delete. When it asks whether to delete the link, click OK.

• Disable the link or delete a link for a container by right-clicking the container in the Scope tab and clicking the Link Enabled option or the Delete Link(s) option.
Managing Group Policy Links

Showing the containers a GPO is linked to
Managing Group Policy Links

Configuring the GPO status
Using Filtering with Group Policies

The exceptions to the processing of group policies can be modified with these options:

• Block inheritance
• Enforced
Configuring Blocking of Inheritance

• By default, group policies flow down to the lower containers and objects.
• To prevent the inheritance of policy settings, block all Group Policy settings from the GPOs linked to parent containers in the Group Policy hierarchy.
• GPOs linked directly to the container and GPOs linked to lower containers are unaffected.
Block the Inheritance of GPOs

Selecting the Block Inheritance option
Block the Inheritance of GPOs

A GPO with the Block Inheritance option enabled
Configuring Enforced Policies

• By enforcing a GPO link, the GPO takes the highest precedence, which will prevail over any conflicting policy settings in other GPOs.

• An enforced link applies to child containers even when those containers are set to Block Inheritance.
Enforce a GPO

Enforcing a GPO
Enforce a GPO

Showing the effect of enforcing a GPO
Configuring Security
Filtering/WMI Filtering

For granular control over who or what receives a group policy, use these filters:

• **Security group filtering**: Uses a security access list (ACL) to determine who can modify or read a policy and who or what a GPO is applied to.

• **WMI filtering**: Uses the WMI Query Language (WQL) to control who or what a GPO is applied to.
Using Security Filtering

Security group filtering specifies which users, computers, or groups based on ACL receive a GPO.
Filtering GPO Scopes

Here are the ways to filter GPO scopes:

• Remove the Allow Apply group policy permission from a group such as Authenticated Users.

• Remove the Authenticated Users group access control entry (ACE), add other groups or users, and assign the Allow Apply group policy permission.

• Add ACE for another group, user, or computer and assign the Deny Apply group policy permission. Like NTFS permissions, the Deny settings always supersede any Allow settings granted to a user through membership in another group or to the user directly.
Configure a Security Group Filtering

Showing current groups and users that have permissions to a GPO
Configure a Security Group Filtering

Showing the ACL for a GPO
Configure a Security Group Filtering

Clicking the Deny Apply group policy permission
WMI Filtering

• **Windows Management Instrumentation (WMI):** A component that extends the Windows Driver Model through an operating system interface that provides information and notification on hardware, software, operating systems, and services.

• **WMI filtering:** Configures a GPO to be applied to certain users or computers based on specific hardware, software, operating systems, and services.
Using WMI Filtering

To use WMI filters:

• You need to have one domain controller running Windows Server 2003 or higher.

• WMI filters will be applied only to computers running Windows XP Professional or newer, or Windows Server 2003 or newer.

• All filter criteria must have an outcome of true for the GPO to be applied.

• Only one WMI filter can be configured per GPO. After a WMI filter has been created, it can be linked to multiple GPOs.
Use WMI with GPOs

Opening the WMI Filters node
Opening the New WMI Filter dialog box
Use WMI with GPOs

Opening the WMI Query dialog box
Use WMI with GPOs

Selecting the name of the WMI filter on the Scope tab
Configuring Loopback Processing

• Group Policy *loopback processing* is used to assign user policies to computer objects.

• No matter who logs on to a computer, the user policies are applied to the computer.
Configuring Loopback Processing

• The loopback policy is enabled using the Group Policy Management Editor, specifically the Computer Configuration\Administrative Templates\System\Group Policy\Configure user Group Policy Loopback processing mode.

• After you enable the setting, you have two modes to choose from that specify the loopback processing mode:
  o Replace mode
  o Merge mode
Configuring Loopback Processing

Configuring the Group Policy loopback processing mode
Configuring Client-Side Extension Behavior

- **Client-side extensions (CSEs)** are processes that interrupt the settings in a GPO and make the changes to the local computer or the currently logged-on user.
- CSEs are triggered when a Group Policy client pulls the GPOs from the domain.
- Each major category of policy setting has CSEs.
Displaying some of the available client-side extensions
You can configure the behavior of CSEs by using Group Policy, specifically \Computer Configuration\Policies\Administrative Template\System\Group Policy\.
Configuring Client-Side Extension Behavior

Configuring scripts policy processing

- Configure scripts policy processing
- Not Configured
- Enabled
- Disabled
- Comment:
- Supported on: At least Windows 2000

Options:
- Allow processing across a slow network connection
- Do not apply during periodic background processing
- Process even if the Group Policy objects have not changed

Help:
- This policy setting determines when policies that assign shared scripts are updated.
- This policy setting affects all policies that use the scripts component of Group Policy, such as those in Windows Settings \& Scripts. It overrides customized settings that the program implementing the scripts policy sets when it was installed.
- If you enable this policy setting, you can use the check boxes provided to change the options. If you disable or do not configure this setting, it has no effect on the system.
- The "Allow processing across a slow network connection" option updates the policies even when the update is being transmitted across a slow network connection, such as a telephone line. Updates across slow connections can cause significant delays.
- The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the system is restarted.
Configuring/Managing Slow-Link Processing

• Group policies executed over slow network links can affect the performance of the client computer, between a site and the corporate office of a site, or the computer being configured via a GPO.

• A link is considered slow if the link is less than 500 kilobits per second (kbps).

• The Configure Group Policy slow-link detection is used to define what is considered a slow-link connection.
Configuring/Managing Slow-Link Processing

Defining the maximum speed of a slow link
Troubleshooting GPOs

Windows Server 2012 provides the following tools for performing Result Set of Policy (RSoP) analysis:

• The Group Policy Results Wizard
• The GPResult.exe command
• The Group Policy Modeling Wizard
Troubleshooting GPOs

The **Group Policy Results Wizard** helps you analyze the cumulative effect of GPOs and policy settings on a user or computer.

To run the Group Policy Results Wizard, the following must be true:

- The target computer must be online.
- You must have administrative credentials on the target computer.
- The target computer must run Windows XP or newer.
- WMI must be running on the target computer and ports 135 and 445 must be available to access WMI on the target computer.
Run the Group Policy Results Wizard

Viewing the Computer Selection page
Run the Group Policy Results Wizard

Viewing the User Selection page
Run the Group Policy Results Wizard

Viewing the Details tab for Group Policy Results
Run the Group Policy Results Wizard

Using the Resultant Set of Policy console
Run the Group Policy Modeling Wizard

Selecting the domain controller
Run the Group Policy Modeling Wizard

Selecting the user and computer to model
Run the Group Policy Modeling Wizard

Advanced Simulation Options
You can select additional options for your simulation.

Simulate policy implementation for the following:

- Slow network connection (for example, a dial-up connection)
- Loopback processing
  - Replace
  - Merge

Site:
(None)

- Skip to the final page of this wizard without collecting additional data

Selecting advanced simulation options
Run the Group Policy Modeling Wizard

Changing the user security groups
Run the Group Policy Modeling Wizard

Changing the computer security groups
Run the Group Policy Modeling Wizard

WMI Filters for Users

You can include Windows Management Instrumentation (WMI) filters in your simulation.

WMI filters can be linked to Group Policy objects (GPO). If a filter is linked to a GPO, then that GPO applies only to those users who meet the criteria specified in the filter.

Assume that the selected user meets the criteria for the following filters:

- All linked filters:
- Only these filters:

List Filters  Remove

Skip to the final page of this wizard without collecting additional data

< Back  Next >  Cancel

Changing WMI Filters for Users
Lesson Summary

• Group policies are defined using group policy objects (GPOs), which are the collection of configuration instructions that are processed by the computer.

• To assign a group policy, it is linked to an Active Directory container (site, domain, or organizational unit).

• GPOs are processed in the following order: local group policy, site, domain, and OU.

• By default, a group policy uses inheritance, whereas settings are inherited from the container above.

• When Active Directory is installed, there are two domain GPOs created by default: Default Domain Policy and Default Domain Controller Policy.

• The exceptions to the processing of group policies can be modified with the Block inheritance and Enforced options.
Lesson Summary

• Windows Management Instrumentation (WMI) filtering configures a GPO to be applied to certain users or computers based on specific hardware, software, operating systems, and services.

• Loopback processing allows the Group Policy processing order to circle back and reapply the computer policies after all user policies and logon scripts run.

• Client-side extensions (CSEs) are processes that interrupt the settings in a GPO and make the changes to the local computer or the currently logged-on user.

• Windows Server 2012 provides the following tools for performing RSoP analysis: the Group Policy Results Wizard, the GPRResult.exe command, and the Group Policy Modeling Wizard.
Copyright 2013 John Wiley & Sons, Inc.
All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.