Lesson 20: Configuring Group Policy Settings

MOAC 70-411: Administering Windows Server 2012
Overview

• Exam Objective 6.2: Configure Group Policy Settings
• Configuring Group Policy Settings
Configuring Group Policy Settings

Lesson 20: Configuring Group Policy Settings
Group Policy Settings

- The **Computer Configuration** node contains settings that are applied to the computer regardless of who logs on to the computer. By default, computer settings are applied when the computer is started.

- The **User Configuration** node contains settings that are applied when the user logs on.
Group Policy Settings

- Group policy settings are refreshed every 90 minutes with a random delay of 30 minutes (giving a random range between 90 minutes and 120 minutes).
- On domain controllers, group policies get refreshed every 5 minutes.
GPO Node Structure

Viewing the Group Policy Object (GPO) node structure
Computer Configuration
Policies Nodes

- Software Settings
- Windows Settings
- Administrative Templates
Software Configuration
Policies Nodes

Software Settings

Windows Settings

Administrative Templates
Software Installation Using Group Policies

- **Windows Installer**: A software component used for the installation, maintenance, and removal of software on Windows.

- **Microsoft Software Installation (MSI) file**: Contains installation information for software.

- **MSI Transform files**: Used to deploy customized MSI files.

- **MSI Patch files**: Used to apply service packs and hot fixes to installed software.
Assigning or Publishing a Package

To deploy software with group policies, take the following steps:

1. Create a distribution point on the publishing server.
2. Create a GPO to use to distribute the software package.
3. Assign or publish a package to a user or computer.
Assigning or Publishing a Package

When you install to a user or computer, you have the option to assign software or publish software with these options:

• Assign software to a user
• Assign software to a computer
• Publish software to a user
Create a New Software Installation Package

Opening the Software Installation node
Create a New Software Installation Package

Selecting the deployment method
Create a New Software Installation Package

Opening the Properties dialog box for a software package
Create a New Software Installation Package

Changing the deployment type and deployment options

© 2013 John Wiley & Sons, Inc.
Create a New Software Installation Package

Upgrading a software package
Uninstalling a Package

To remove an application:
1. Right-click the package.
2. Click All Tasks.
3. Click Remove.

When the Remove Software dialog box opens, choose one of these options:
• Immediately uninstall the software from users and computers
• Allow users to continue to use the software, but prevent new installations
Uninstalling a Package

Removing software
Using Folder Redirection

Use *Folder Redirection* to:

- Redirect the content of a certain folder to a network location or to another location on the user’s local computer.
- Redirect the Desktop, Start Menu, Documents, Picture, Music, Videos, Favorites, Downloads, and other related folders.

It is found under `\User Configuration\Policies\Windows Settings`. 

© 2013 John Wiley & Sons, Inc.
Using Folder Redirection

Viewing the Folder Redirection folders
Configure Folder Redirection

Configuring the Documents Properties

You can specify the location of the Documents folder.

Setting: Not configured

This Group Policy Object will have no effect on the location of this folder.

Any existing redirection will continue to apply even when this Group Policy object is removed. To ensure that the folder is redirected back to the default location, select the "Redirect to the local user profile location" option.
Configure Folder Redirection

Redirecting to the user’s home directory
Configure Folder Redirection

Specifying the Security Group Membership when using Advanced mode

© 2013 John Wiley & Sons, Inc.
Configure Folder Redirection

Configuring settings when using Advanced mode
Configure Folder Redirection

Using group policies to configure offline files
Using Scripts with Group Policies

- A **script** is a list of commands that can be executed within a single file, which can perform repetitive tasks.
- The **Microsoft Windows Script Hosts (WSH)** is the component that provides scripting capabilities to Windows.
Types of Scripts

Computer Scripts
- Startup
- Shutdown

User Scripts
- Logon
- Logoff
Using Scripts with Group Policies

To use scripts:

1. Create the login script.
2. Execute the script manually to make sure that the script runs and performs as planned.
3. Copy the script to the `c:\Windows\Sysvol\Sysvol\Domain Name\Scripts` folder on a domain controller. The content of SYSVOL volume is automatically replicated to the other domain controllers within the domain.
4. Configure a GPO to execute the script during startup, shutdown, logon, or logoff.
Implement a Login Script Using Group Policies

Opening the Logon Properties dialog box

© 2013 John Wiley & Sons, Inc.
Implement a Login Script Using Group Policies

Adding a script to a GPO
Using Administrative Templates

- **ADM files**: Used to define the settings that an administrator can configure through Group Policy.

- **ADMX files**: Like ADM files but based on eXtensible Markup Language (XML). Can be stored in a single location called the Central Store in the SYSVOL directory.

- **ADML files**: Language-specific files used to store descriptions of settings.
Managing Administrative Templates

Requirements for an Administrative Template setting are displayed:

• On the Extended tab, when you click to select an Administrative Template setting
• When you double-click an Administrative Template setting
Managing Administrative Templates

Selecting an Administrative Template
Managing Administrative Templates

Viewing the Settings dialog box
Managing Administrative Templates

When configuring Administrative Templates, there are three states:

- **Not Configured**: The registry key is not modified or overwritten.
- **Enabled**: The registry key is modified by this setting.
- **Disabled**: The Disabled settings undo a change made by a prior Enabled setting.
The Central Store:

- Is a folder structure created in the SYSVOL directory on the domain controllers in each domain in your organization.
- Is created only on a single domain controller for each domain.

The content of the SYSVOL will be replicated to the other domain controllers.
Creating a Central Store

1. Create a PolicyDefinitions folder in the %systemroot%\sysvol\domain\policies\ folder.

2. The PolicyDefinitions folder stores all language-neutral ADMX files. Therefore, copy all files from the %systemroot%\PolicyDefinitions\* folder to the %systemroot%\sysvol\domain\policies\ folder.

3. Copy all the language folders and files to %systemroot%\sysvol\domain\policies\ PolicyDefinitions.
A **security template** is a collection of configuration settings stored in a text file with the .inf extension. They can be used to:

- Save the security configuration to a file.
- Deploy the security settings to a computer or group policy.
- Analyze compliance of a computer’s current configuration against the desired configuration.
Policies Configured with Security Templates

Account

Restricted Groups

Local

System Services

Event Log

Registry Permissions
To create a new security template, right-click the node where you want to store the security template, and click New Template.
Open the Security Templates Snap-In

Naming the security template
Open the Security Templates Snap-In

Viewing a security template
Compare Settings with a Security Template

Viewing the Security Configuration and Analysis console
Compare Settings with a Security Template

Comparing a security template with actual settings
Custom Administrative Template Files

• To make settings in ADMX files available to a GPO, add the Administrative Templates file to the GPO.

• If you have older ADM files, either add them to the GPO or convert the ADM file to an ADMX file.
Add Custom ADM Administrative Template Files

Opening the Add/Remove Templates dialog box
Add Custom ADM Administrative Template Files

Navigating to and opening an ADM file
Using ADMX Migrator

ADMX Migrator:

• Is a snap-in for the MMC that simplifies the process of converting existing Group Policy ADM templates to the new ADMX format.

• Provides a graphical user interface for creating and editing Administrative Templates.
Use ADMX Editor to Migrate ADM Templates

Opening the ADMX Migrator
Property Filters for Administrative Templates

- By default, all policy settings are displayed.
- To narrow down the displayed list of settings, use *Administrative Templates Property Filters*.
Property Filters for Administrative Templates

- To filter the settings displayed, select or deselect the following filter options:
  - Managed or Unmanaged
  - Configured or Not Configured
  - Keyword Filters
  - Requirements Filters
Lesson Summary

• Group Policies provides centralized management and configuration of operating systems, applications, and user settings.
• Windows Installer installs, maintains, and removes software on Windows.
• Installation information for software is stored in a Microsoft Software Installation (MSI) file.
• To deploy software with group policies, create a distribution point on the publishing server, create a GPO to use to distribute the software package, and assign or publish a package to a user or computer.
• Folder redirection allows you to redirect the content of a certain folder to a network location or to another location on the user’s local computer.
Lesson Summary

- Starting with Windows Vista and Windows Server 2008, ADMX files define the settings that an administrator can configure through Group Policy.
- The Central Store is a folder structure created in the SYSVOL directory on the domain controllers in each domain in your organization.
- Security templates help you implement security settings quickly and efficiently.
- ADMX Migrator is a snap-in for the Microsoft Management Console (MMC) that simplifies the process of converting your existing Group Policy ADM templates to the new ADMX format and provides a graphical user interface for creating and editing Administrative Templates.
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.