

Module 5

Implementing Group Policy

Module Overview

- Introducing Group Policy
- Implementing and administering GPOs
- Group Policy scope and Group Policy processing
- Troubleshooting the application of GPOs

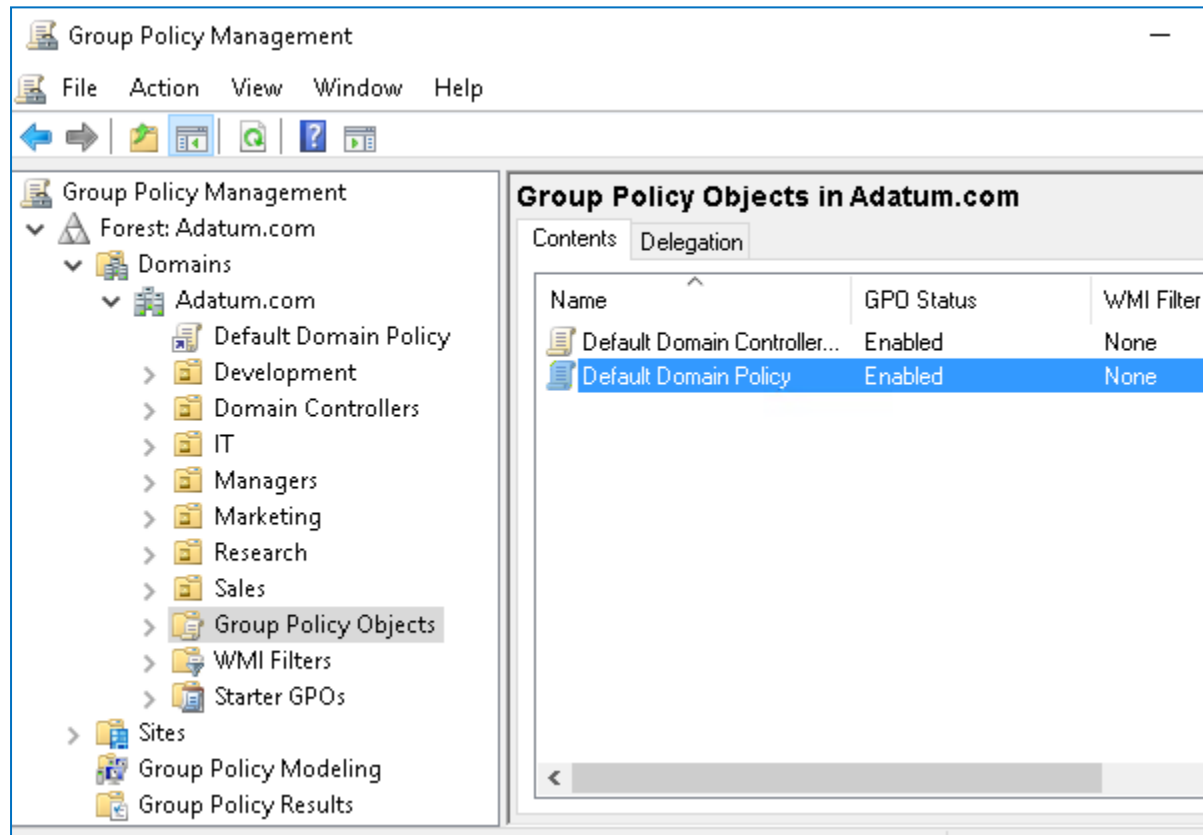
Lesson 1: Introducing Group Policy

- What is configuration management?
- Overview of Group Policy tools and consoles
- Demonstration: Exploring Group Policy tools and consoles
- Benefits of using Group Policy
- Group Policy Objects
- Overview of GPO scope
- Overview of GPO inheritance
- The Group Policy Client service and client-side extensions
- New features in Group Policy in Windows Server 2016

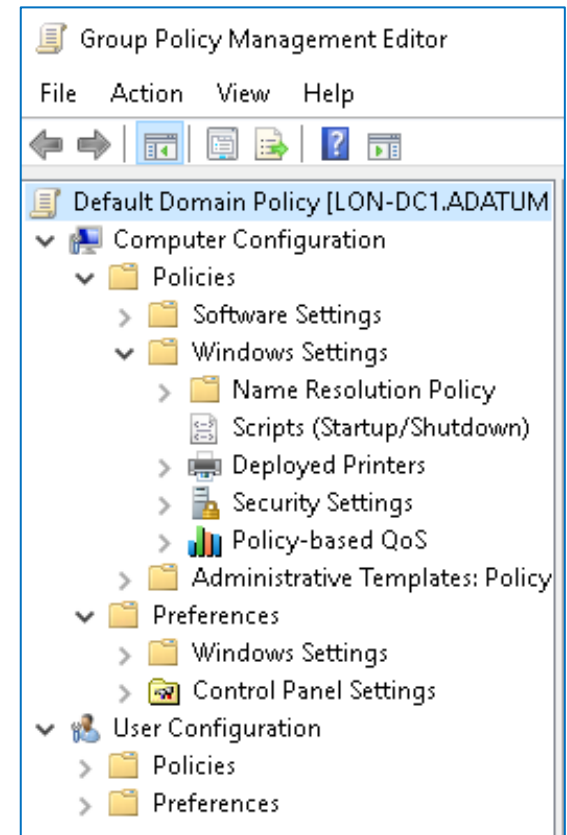
What is configuration management?

- *Configuration management* is a centralized approach to applying one or more changes to more than one user or computer
- The key elements of configuration management are:
 - Setting
 - Scope
 - Application

Overview of Group Policy tools and consoles



Group Policy Management Console



Group Policy Management Editor

Command-line utilities: **GPUpdate** and **GPResult**

Demonstration: Exploring Group Policy tools and consoles

- In this demonstration, you will learn how to:
 - Navigate the GPMC
 - Create a new GPO
 - Configure a setting
 - Perform a Group Policy refresh
 - Examine which GPOs apply to the computer and user

Benefits of using Group Policy

- Group Policy is a very powerful administrative tool
- You can use it to enforce various types of settings to a large number of users and computers
- Typically, you use GPOs to:
 - Apply security settings
 - Manage desktop application settings
 - Deploy application software
 - Manage Folder Redirection
 - Configure network settings

Group Policy Objects

A GPO is:

- A container for one or more policy settings
- Managed with the GPMC
- Stored in the GPOs container
- Edited with Group Policy Management Editor
- Applied to a specific level in the AD DS hierarchy

Overview of GPO scope

- The *scope* of a GPO is the collection of users and computers that will apply the settings in the GPO
- You can use several methods to scope a GPO:
 - Link the GPO to a container, such as an OU
 - Filter by using security settings
 - Filter by using WMI filters
- For Group Policy preferences:
 - You can filter or target the settings that you configure by Group Policy preferences within a GPO based on several criteria

Overview of GPO inheritance

GPOs are processed on a client computer in the following order:

1. Local GPOs
2. Site-level GPOs
3. Domain-level GPOs
4. OU GPOs, including any nested OUs

The Group Policy Client service and client-side extensions

- Group Policy application process:
 1. Group Policy Client retrieves GPOs
 2. Client downloads and caches GPOs
 3. Client-side extensions process the settings
- Policy settings in the **Computer Configuration** node apply at system startup and every 90–120 minutes thereafter
- Policy settings in the **User Configuration** node apply at sign-in and every 90–120 minutes thereafter

New features in Group Policy in Windows Server 2016

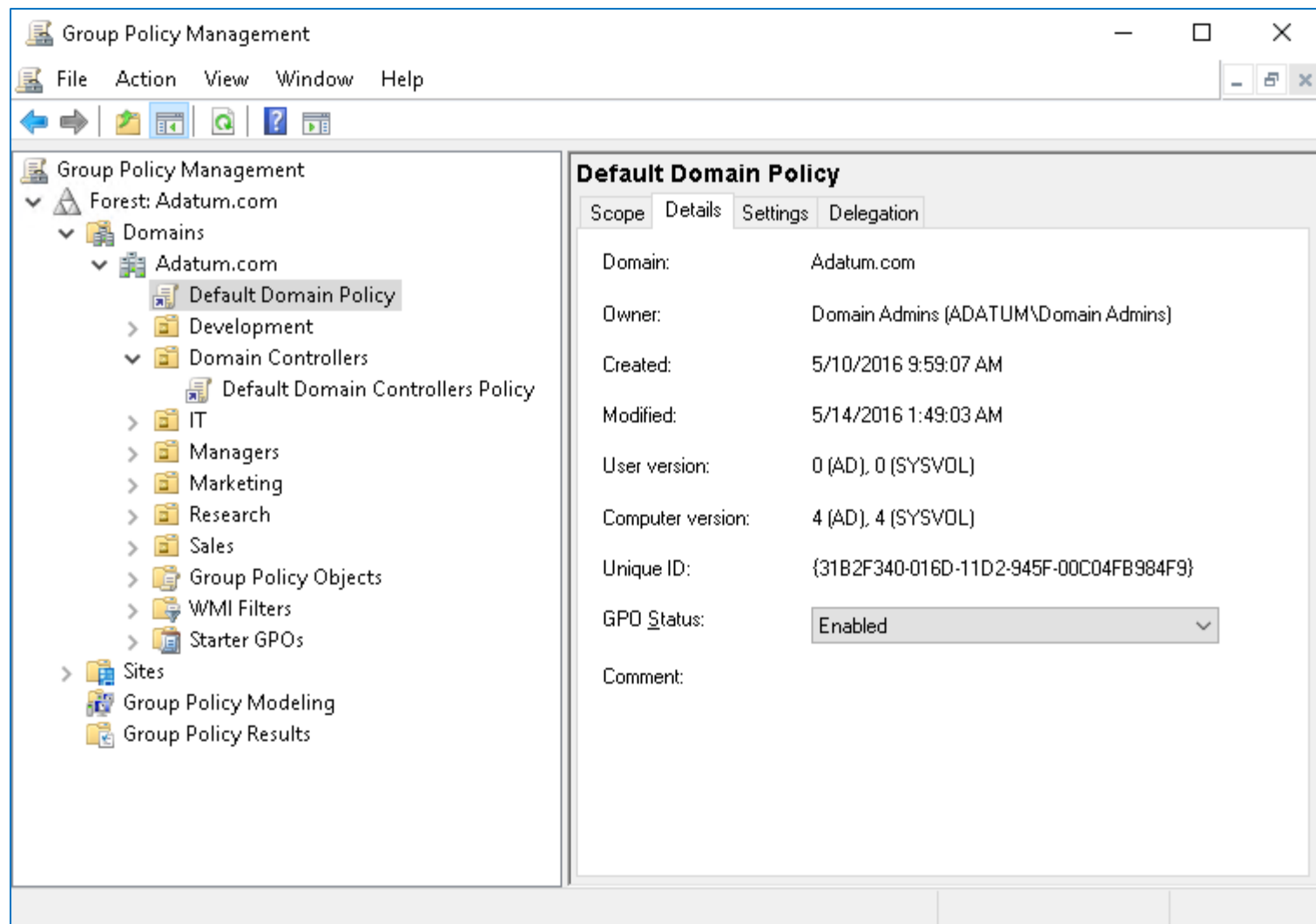
Windows Server 2016 introduces a few changes and improvements to Group Policy, including:

- Importing the following types of policy settings on Nano Server:
 - Registry settings
 - Security settings
 - Audit settings
- Including Windows 10 administrative templates

Lesson 2: Implementing and administering GPOs

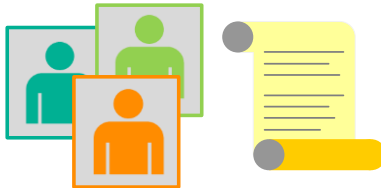
- What are domain-based GPOs?
- GPO storage
- What are starter GPOs?
- Common GPO management tasks
- Delegating administration of Group Policy
- Demonstration: Delegating administration of Group Policy

What are domain-based GPOs?



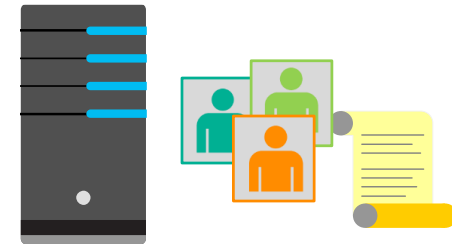
GPO storage

GPO



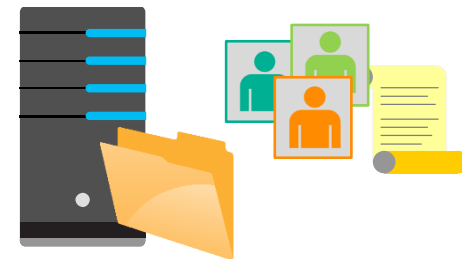
- Contains Group Policy settings
- Stores content in two locations

Group Policy container



- Stored in AD DS
- Provides version information

Group Policy template



- Stored in shared SYSVOL folder
- Provides Group Policy settings

What are starter GPOs?

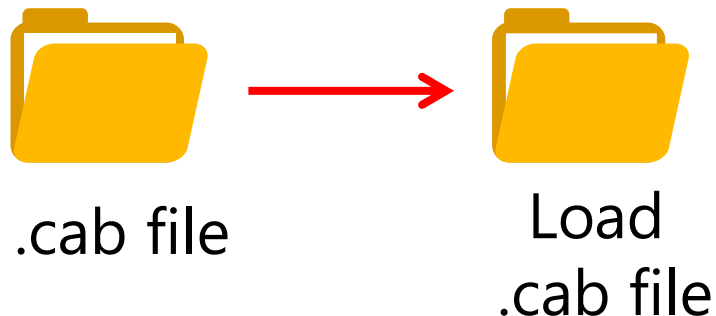
A starter GPO:

- Stores administrative template settings on which new GPOs will be based
- Can be exported to .cab files
- Can be imported into other areas of an organization

Exported to .cab file



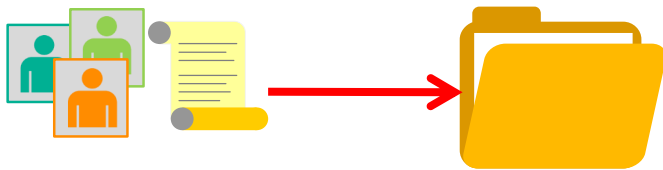
Imported to the GPMC



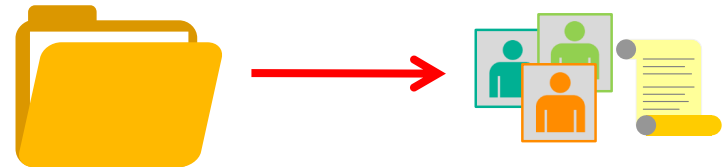
Common GPO management tasks

You can manage GPOs by using GPMC or Windows PowerShell. These are some of the options for managing the state of GPOs:

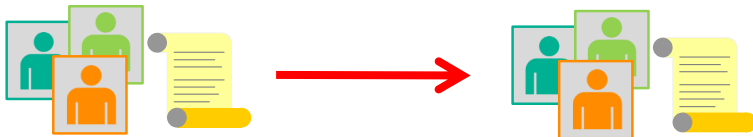
Back up GPOs



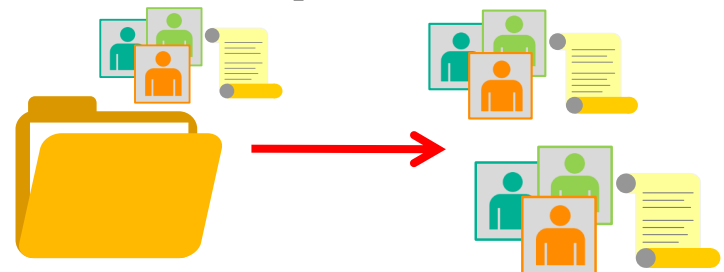
Restore GPOs



Copy GPOs



Import GPOs



Delegating administration of Group Policy

- Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise
- You can delegate the following Group Policy tasks independently:
 - Creating GPOs
 - Editing GPOs
 - Managing Group Policy links for a site, domain, or OU
 - Performing Group Policy modeling analysis in a domain or OU
 - Reading Group Policy results data in a domain or OU
 - Creating WMI filters in a domain

Demonstration: Delegating administration of Group Policy

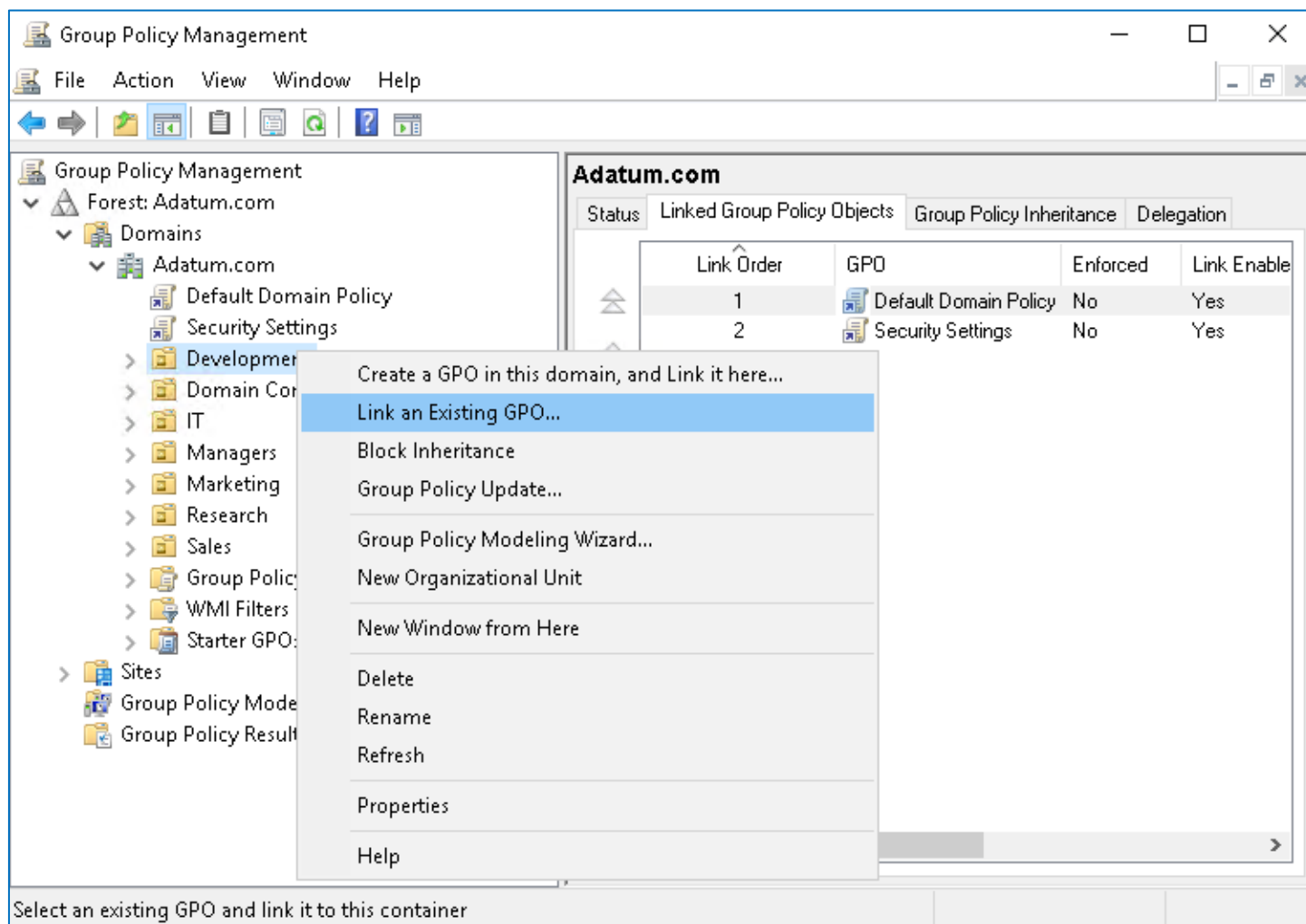
- In this demonstration, you will learn how to:
 - Delegate permissions to create GPOs
 - Delegate permissions to link GPOs
 - Delegate permissions to view Group Policy results

Lesson 3: Group Policy scope and Group Policy processing

- What are GPO links?
- Demonstration: Linking GPOs
- Group Policy processing order
- Configuring GPO inheritance and precedence
- Using security filtering to modify Group Policy scope
- What are WMI filters?
- Demonstration: Filtering Group Policy application
- How to enable or disable GPOs and GPO nodes
- Loopback policy processing
- Considerations for slow links and disconnected systems
- Identifying when settings become effective

What are GPO links?

After you have linked a GPO, the users or computers in that container are within the scope of the GPO, including computers and users in child OUs

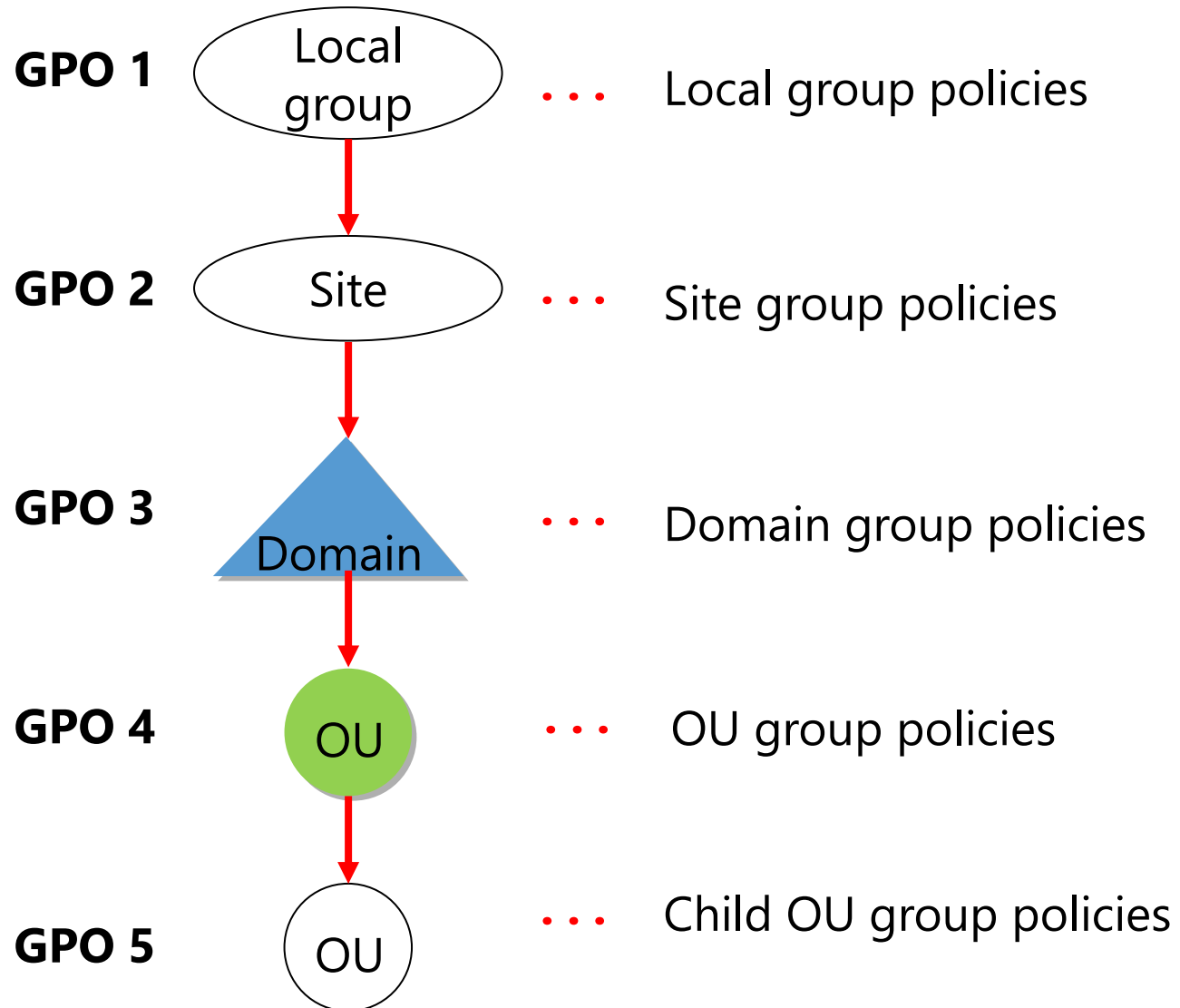


Demonstration: Linking GPOs

In this demonstration, you will learn how to:

- Create and edit two GPOs
- Link the GPOs to different locations
- Disable a GPO link
- Delete a GPO link

Group Policy processing order



Configuring GPO inheritance and precedence

- The application of GPOs linked to each container results in a cumulative effect called *policy inheritance*:
 - Default precedence: Local → Site → Domain → OU → Child OU... (LSDOU)
 - Visible on the **Group Policy Inheritance** tab
- Link order (attribute of GPO link):
 - Lower number → Higher on list → Precedence
- Block Inheritance (attribute of OU):
 - Blocks the processing of GPOs from a higher level
- Enforced (attribute of GPO link):
 - Enforced GPOs override Block Inheritance
 - Enforced GPO settings win over conflicting settings in lower GPOs

Using security filtering to modify Group Policy scope

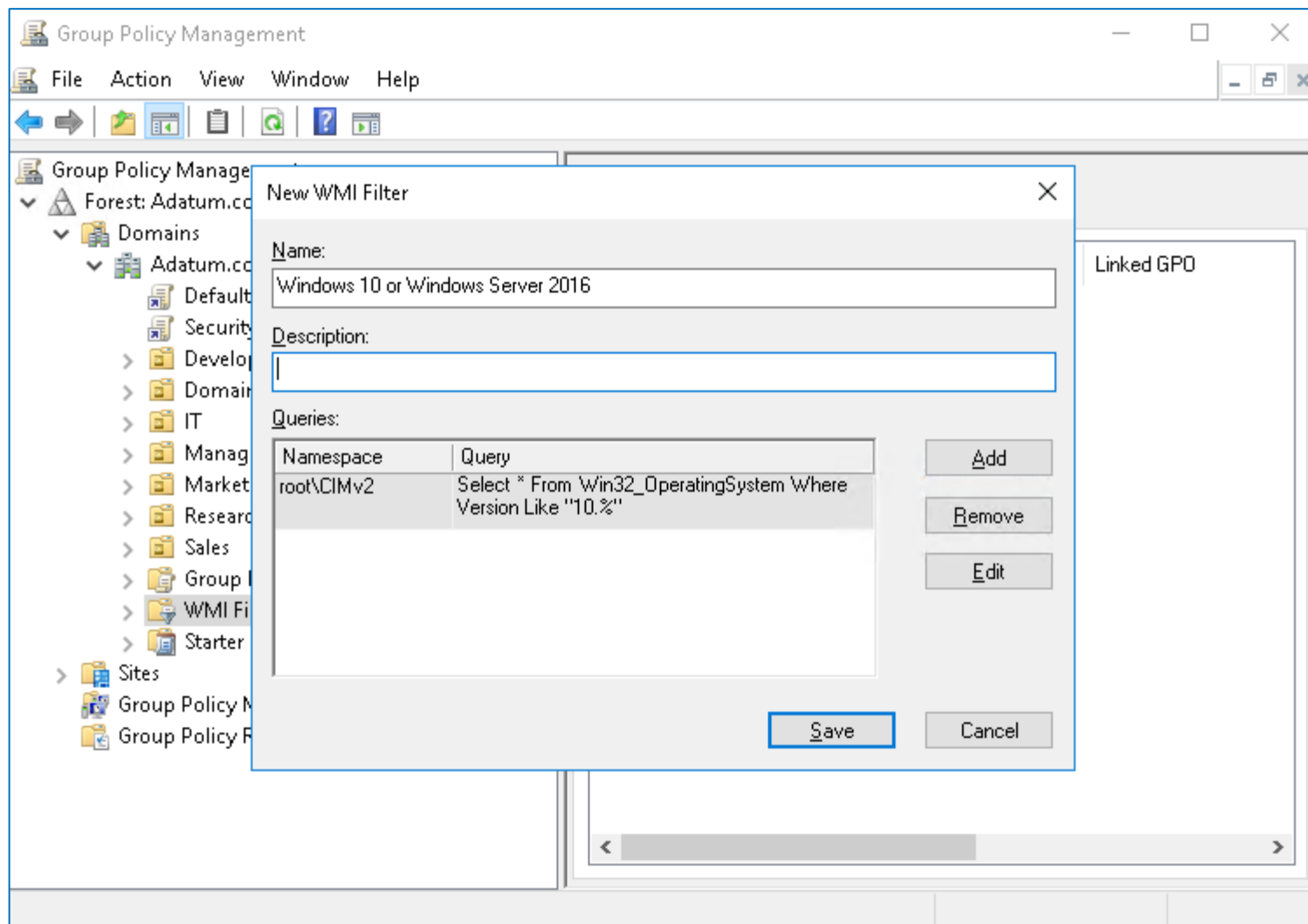
- Apply Group Policy permission:
 - GPO has an ACL (**Delegation** tab → **Advanced**)
 - Members of the Authenticated Users group have Allow Apply Group Policy permissions by default
- To scope only to users in selected global groups:
 - Remove the Authenticated Users group
 - Add appropriate global groups: Must be global groups (GPOs do not scope to domain local)
- To scope to users except for those in selected groups:
 - On the **Delegation** tab, click **Advanced**
 - Add appropriate global groups
 - Deny the Apply Group Policy permission

What are WMI filters?

- WMI queries can filter GPOs based on system characteristics, including:
 - RAM
 - Processor speed
 - Disk capacity
 - IP address
 - Operating system version
- WMI queries are written by using WQL, for example
`select * from Win32_OperatingSystem where Version like "10.%"`
- WMI filters can be expensive in terms of Group Policy processing performance



What are WMI filters?

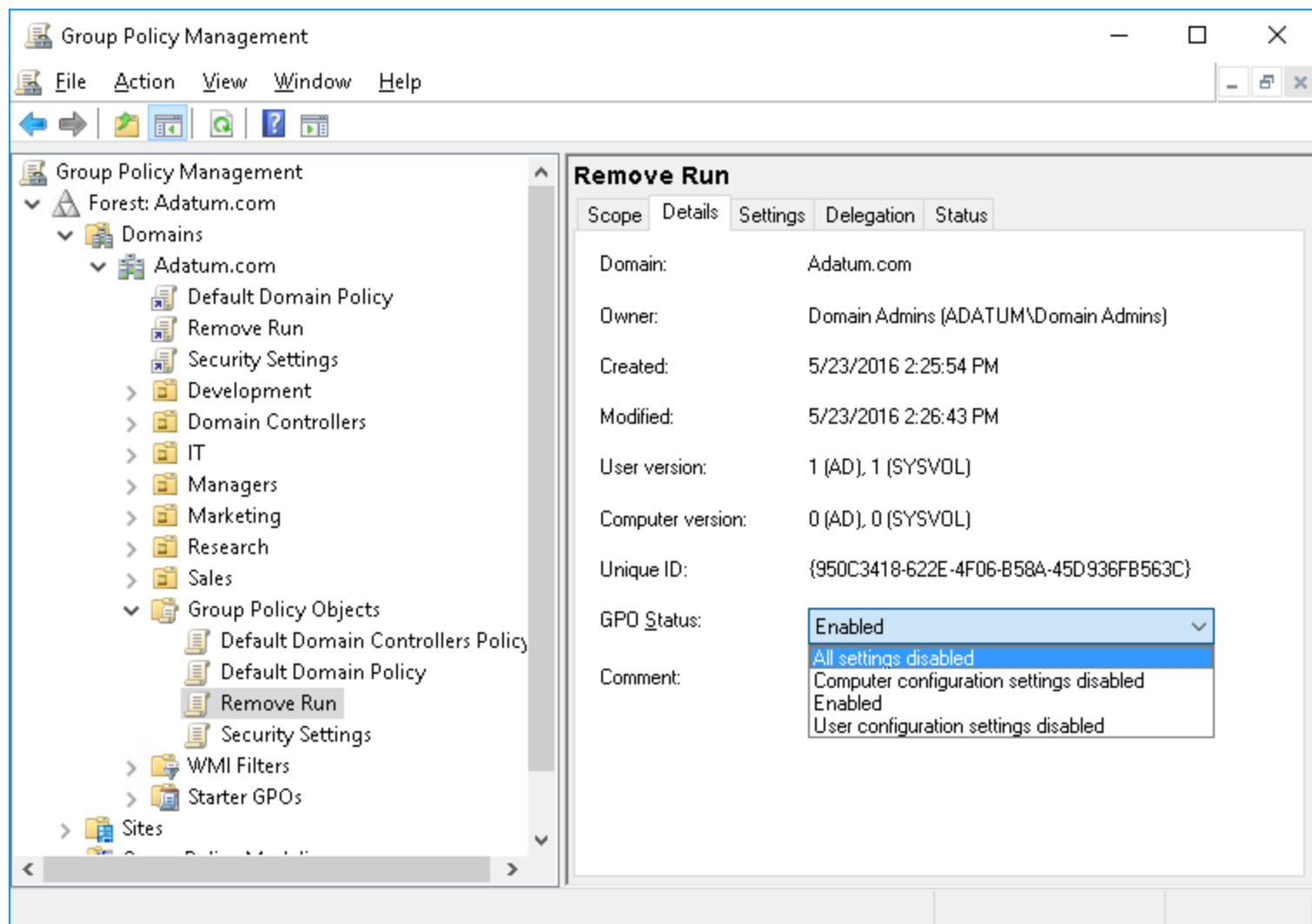


Demonstration: Filtering Group Policy application

In this demonstration, you will learn how to:

- Create a new GPO, and link it to the **IT** OU
- Filter Group Policy application by using security group filtering
- Filter Group Policy application by using WMI filtering

How to enable or disable GPOs and GPO nodes

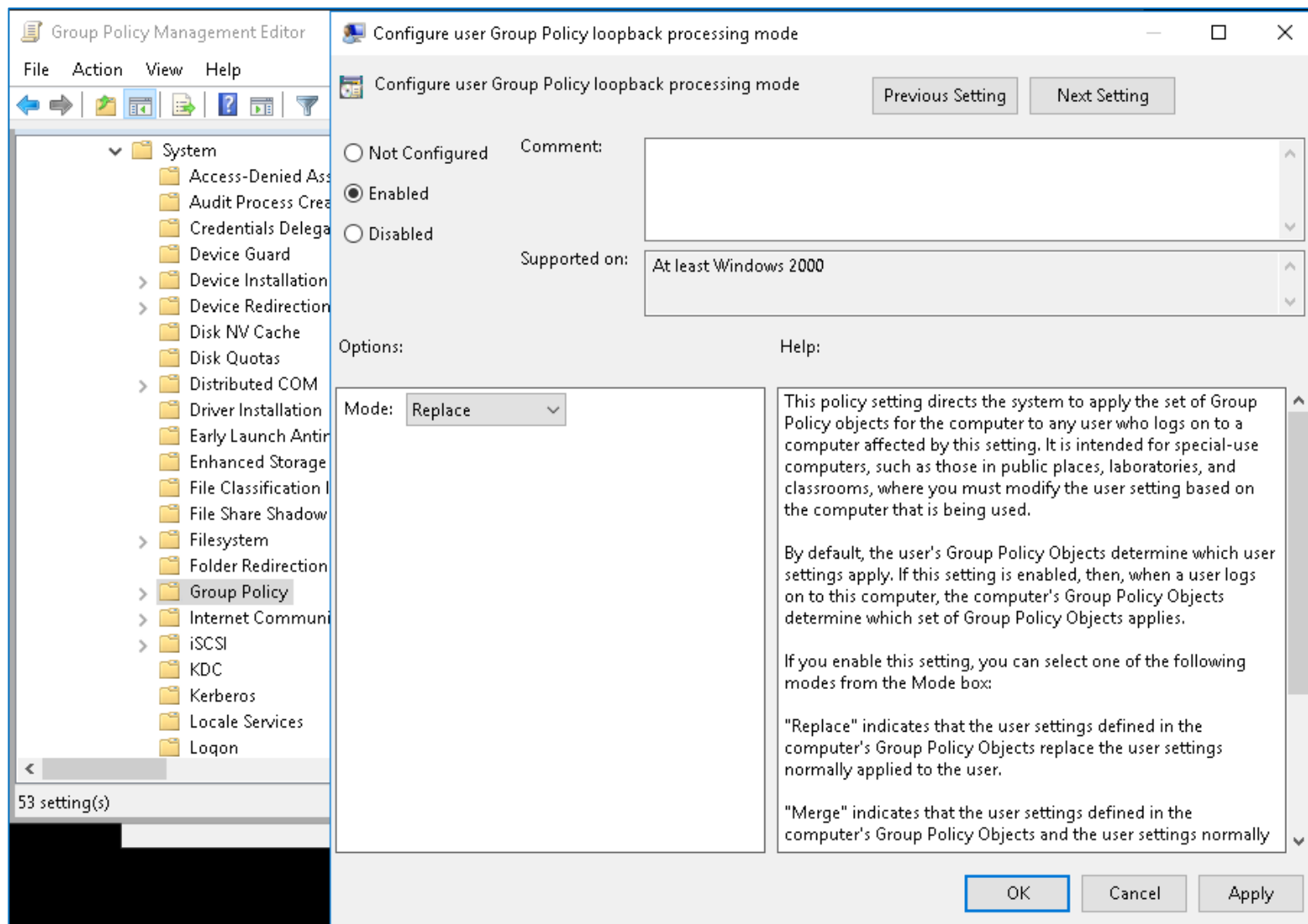


Loopback policy processing

- Provides the ability to apply user Group Policy settings based on the computer to which the user is signing in
- Replace mode:
 - Only the list of GPOs based on the computer object is used
- Merge mode:
 - The list of the GPOs based on the computer have higher precedence than the list of GPOs based on the user
- Useful in closely managed environments and special-use computers, such as:
 - Terminal servers, public-use computers, and classrooms



Loopback policy processing



Considerations for slow links and disconnected systems

- Slow link detection:
 - By default, connection speeds below 500 kbps
 - The following CSEs apply by default:
 - Security Settings
 - Administrative Templates
- Disconnected computers:
 - Cache Group Policy so that settings still apply
 - Perform Group Policy refresh when reconnecting with the domain network if a background refresh has been missed

Identifying when settings become effective

- GPO replication must occur
- Group changes must replicate
- Group Policy refresh must occur
- User must sign out and sign in or the computer must restart
- You must perform a manual refresh
- Most CSEs do not reapply unchanged GPO settings

Lab A: Implementing a Group Policy infrastructure

- Exercise 1: Creating and configuring GPOs
- Exercise 2: Managing GPO scope

Logon Information

Virtual machines:	20742B-LON-DC1 20742B-LON-CL1
User name:	Adatum\Administrator
Password:	Pa55w.rd

Estimated Time: 40 minutes

Lab Scenario

Your manager asked you to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent access to certain programs on local computers.

You configured Group Policy to lock computer screens when users leave computers unattended for 10 minutes or more. However, after some time, you were made aware that a critical application used by the Research engineering team fails when the screen saver starts. An engineer asked you to prevent the GPO setting from applying to any member of the Research security group. He also asked you to configure conference room computers to be exempt from corporate policy. However, you must ensure that the conference room computers use a 2-hour time out.

Create the policies that you need to evaluate the RSoPs for users in your environment. Make sure to optimize the Group Policy infrastructure and verify that all policies are applied as they were intended.

Lab Review

- Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs typically are linked very high in the Active Directory logical structure—to the domain itself or to a first-level OU. What advantages do you gain by using security group filtering rather than GPO links to manage a GPO's scope?
- Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?
- Do you use loopback policy processing in your organization? In which scenarios and for which policy settings can loopback policy processing add value?

Lesson 4: Troubleshooting the application of GPOs

- Refreshing GPOs
- What is RSoP?
- Generating RSoP reports
- Demonstration: Performing a what-if analysis with Group Policy Modeling Wizard
- Examining Group Policy event logs
- Detecting Group Policy health issues

Refreshing GPOs

- When you apply GPOs, remember that:
 - Computer settings apply at startup
 - User settings apply at sign-in
 - Policies refresh at regular, configurable intervals
 - Security settings refresh at least every 16 hours
 - Policies refresh manually by using:
 - The **gpupdate** command-line utility
 - The Windows PowerShell cmdlet **Invoke-gpupdate**
 - With the Remote Group Policy Refresh feature, you can refresh policies remotely

What is RSoP?

RSoP is the net effect of GPOs applied to a user or computer

Group Policy Management

The screenshot displays the Group Policy Management console. The left pane shows the tree structure: Group Policy Management > Forest: Adatum.com > Sites > Group Policy Modeling > Group Policy Results > Alan on LON-CL1. The right pane shows the 'Summary' tab for 'Alan on LON-CL1'. The main content area is titled 'Group Policy Results' and shows 'ADATUMAlan on ADATUMLON-CL1' with data collected on 11/12/2013 1:30:59 AM. Below this, there are sections for 'Computer Details', 'General', 'Component Status', 'Settings', and 'Policies'. The 'Component Status' section contains a table with the following data:

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	484 Millisecond(s)	11/12/2013 1:29:45 AM	View Log
Registry	Success	437 Millisecond(s)	11/6/2013 2:52:48 AM	View Log
Security	Success	8 Second(s) 313 Millisecond(s)	11/6/2013 2:52:56 AM	View Log

The 'Settings' section is expanded, showing 'Policies' with sub-items: 'Windows Settings', 'Security Settings', 'Account Policies/ Password Policy', 'Account Policies/ Account Lockout Policy', and 'Local Policies/ Security Options'. Each sub-item has a 'hide' or 'show' link next to it.



What is RSoP?

Group Policy Modeling Wizard

Group Policy Modeling Wizard

User and Computer Selection

You can view simulated policy settings for a selected user (or a container with user information) and computer (or a container with computer information).

Example container name: CN=Users,DC=Adatum,DC=com
Example user or computer: ADATUM\Administrator

Simulate policy settings for the following:

User information

☒ Container:

☐ User:

Computer information

☐ Container:

☒ Computer:

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

< Back **Next >** Cancel



Generating RSoP reports

- RSoP reports show the actual settings being applied to the user and computer
- Might show the time taken to apply Group Policy
- You can generate RSoP reports by using:
 - **Group Policy Results Wizard**
 - **GPRResults**
 - **Get-GPResultantSetOfPolicy**
- Target computer must be online
- Remote WMI must be enabled



Generating RSoP reports

Group Policy Results Wizard

The screenshot displays the Group Policy Management console. The left pane shows the tree structure with 'Administrator on LON-CL1' selected under 'Group Policy Results'. The right pane shows the 'Group Policy Results' for 'ADATUM\administrator on ADATUM\LON-CL1', with data collected on 6/6/2012 9:05:16 AM. The 'Summary' tab is active, showing 'Computer Details' and 'General' information. Below this is a 'Component Status' table.

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	3 Second(s) 703 Millisecond(s)	6/6/2012 9:01:22 AM	View Log
Registry	Success	47 Millisecond(s)	5/14/2012 6:12:58 AM	View Log
Security	Success	1 Second(s) 78	5/14/2012	View Log



Demonstration: Performing a what-if analysis with Group Policy Modeling Wizard

In this demonstration, you will learn how to:

- Use **GPRresult.exe** to create a report
- Use **Group Policy Reporting Wizard** to create a report
- Use **Group Policy Modeling Wizard** to create a report

Examining Group Policy event logs

Event Viewer

File Action View Help

Operational Number of events: 1,280

Level	Date and Time	Source	Event ID
Information	6/6/2012 9:06:04 AM	Group...	5315
Information	6/6/2012 9:06:04 AM	Group...	8006
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5320
Information	6/6/2012 9:06:04 AM	Group...	5314
Information	6/6/2012 9:06:04 AM	Group...	5313
Information	6/6/2012 9:06:04 AM	Group...	5312
Information	6/6/2012 9:06:04 AM	Group...	5017
Information	6/6/2012 9:06:04 AM	Group...	4017
Information	6/6/2012 9:06:04 AM	Group...	5017

Event 5315, GroupPolicy (Microsoft-Windows-GroupPolicy)

General Details

Next policy processing for ADATUM\LON-DC1\$ will be attempt

Refreshes the current selection.

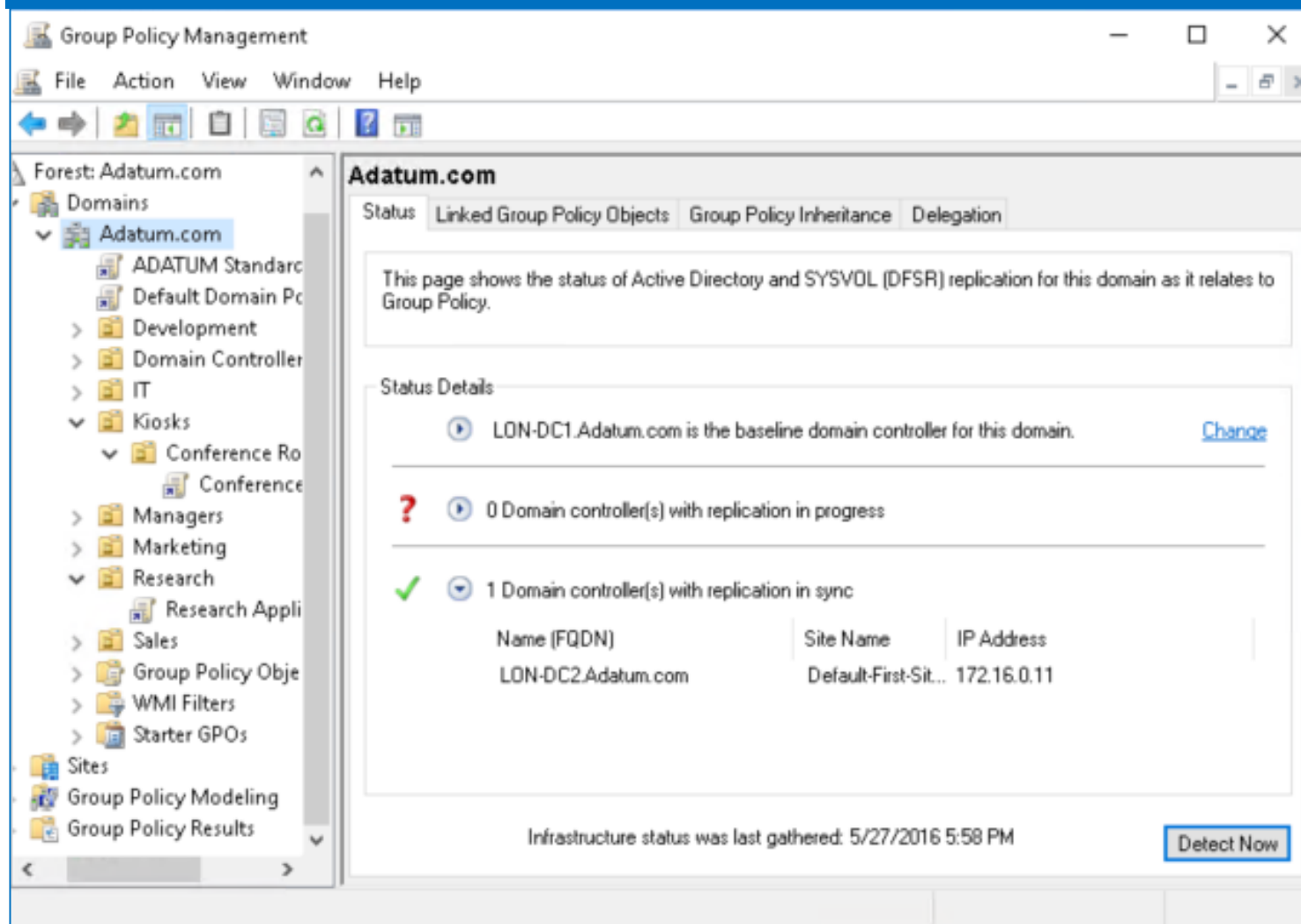
Actions

Operational

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this...
- View
- Refresh
- Help
- Event 5315, GroupP...
- Event Properties
- Attach Task To This...

Detecting Group Policy health issues

Group Policy health check in Group Policy Management Console



The screenshot displays the Group Policy Management console window. The left-hand tree view shows the hierarchy: Forest: Adatum.com > Domains > Adatum.com. The right-hand pane is titled 'Adatum.com' and contains several tabs: Status, Linked Group Policy Objects, Group Policy Inheritance, and Delegation. The 'Status' tab is active, showing a message: 'This page shows the status of Active Directory and SYSVOL (DFS) replication for this domain as it relates to Group Policy.' Below this, the 'Status Details' section lists the baseline domain controller as LON-DC1.Adatum.com. It then reports '0 Domain controller(s) with replication in progress' (indicated by a red question mark icon) and '1 Domain controller(s) with replication in sync' (indicated by a green checkmark icon). A table lists the domain controller details:

Name (FQDN)	Site Name	IP Address
LON-DC2.Adatum.com	Default-First-Sit...	172.16.0.11

At the bottom of the console, it states 'Infrastructure status was last gathered: 5/27/2016 5:58 PM' and includes a 'Detect Now' button.



Detecting Group Policy health issues

In Group Policy Management Console:

- The **Status** tab displays information that indicates the health of the Group Policy infrastructure:
 - Domain
 - GPO
- Information displayed includes:
 - Domain controllers
 - Permissions on the Group Policy container and the Group Policy template
 - GPO replication
 - GPO versioning
- Domain controllers not reachable or inconsistent with the baseline domain controller are added to the **Domain controller(s) with replication in progress** list



Lab B: Troubleshooting Group Policy infrastructure

- Exercise 1: Verifying GPO application
- Exercise 2: Troubleshooting GPOs

Logon Information

Virtual machines:	20742B-LON-DC1 20742B-LON-CL1
User name:	Adatum\Administrator
Password:	Pa55w.rd

Estimated Time: 40 minutes

Lab Scenario

After configuring settings for the Research department and computers in the conference rooms, you want to make sure that all settings apply as intended. You want to do this by creating RSoP reports from both **Group Policy Management Console** and a client. You do not have access to a computer in the conference rooms, so you have to simulate how settings will apply by using Group Policy modeling analyses. You want to investigate what events are stored in Event Viewer regarding Group Policy.

After some time, you receive a Help desk ticket opened by a user. The issue is that the Screen Saver settings that was applied is not the correct settings for the user. You have to investigate the issue and make sure that the correct settings apply to the user.

Lab Review

- In what situations have you used RSoP reports to troubleshoot Group Policy application in your organization?
- In what situations have you used Group Policy modeling? If you have not done this yet, in what situations can you anticipate using Group Policy modeling?

Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips