Module 6

Creating and Configuring Group Policies

Windows Server 2016

Module Overview

- Understand Group Policy
- Implement GPOs
- A Deeper Look at Settings and GPOs
- Manage Group Policy Scope
- Group Policy Processing
- Troubleshoot Policy Application

Lesson 1: Understand Group Policy

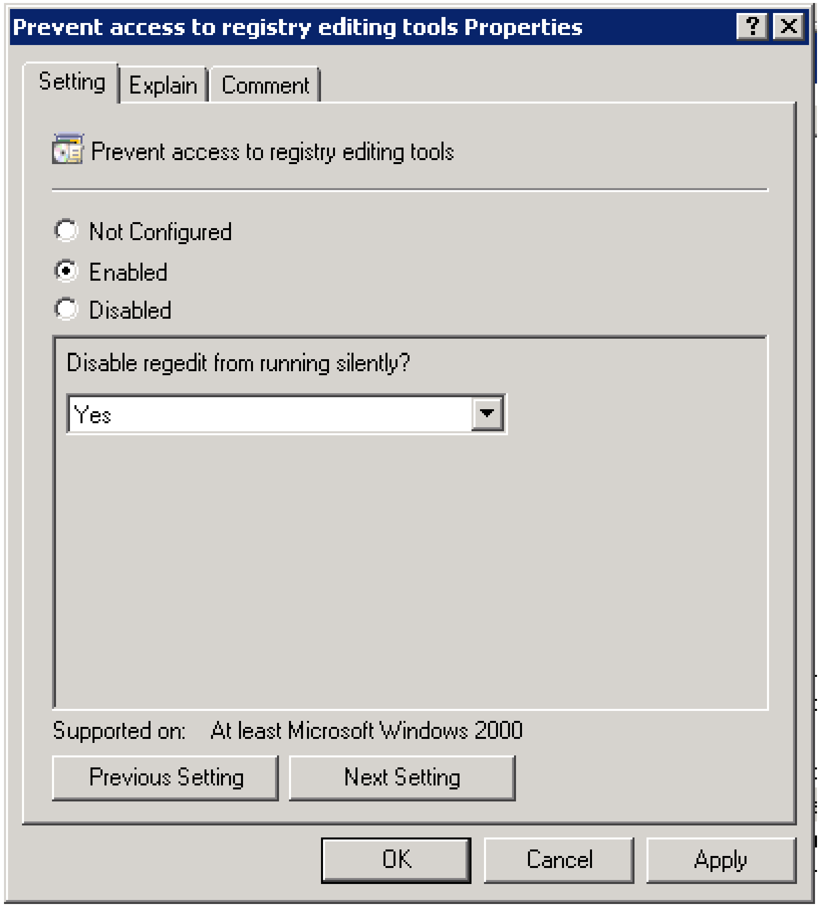
- What is Configuration Management?
- Policy Settings (Also Known as *Policies*)
- Group Policy Objects
- GPO Scope
- Group Policy Client and Client-Side Extensions
- Group Policy Refresh
- Resultant Set of Policy
- Review and Discuss the Components of Group Policy

What Is Configuration Management?

- A centralized approach to applying one or more changes to one or more users or computers
- *Setting*: Definition of a change or configuration
- *Scope*: Definition of the user(s) or computer(s) to which the change applies
- *Application*: A mechanism that applies the setting to users and computers within the scope
- Group Policy: The framework for configuration management in an AD DS domain
  - Setting
  - Scope
  - Application
  - Tools for management, configuration, and troubleshooting

Policy Settings (Also Known as *Policies*)

- The granular definition of a change or configuration
  - Prevent access to registry-editing tools
  - Rename the Administrator account
- Divided between
  - User Configuration ("user policies")
  - Computer Configuration ("computer policies")
- Define a setting
  - Not configured (default)
  - Enabled
  - Disabled
- Read explanatory text
- Test all settings



Prevent access to registry editing tools Properties

Prevent access to registry editing tools

○ Not Configured
● Enabled
○ Disabled

Disable regedit from running silently?

Yes

Supported on: At least Microsoft Windows 2000

Group Policy Objects

- The container for one or more policy settings
- Managed with the Group Policy Management console (GPMC)
  - Group Policy Objects container
- Edited with the Group Policy Management Editor (GPME)

GPO Scope

- **Scope.** Definition of objects (users or computers) to which GPO applies
- **GPO link.** GPO can be linked to site, domain, or organizational unit (OU) (SDOU)
  - GPO can be linked to multiple site(s) or OU(s)
  - GPO link(s) define *maximum* scope of GPO
- **Security group filtering**
  - Apply or deny application of GPO to members of global security group
  - Filter application of scope of GPO within its link scope
- **WMI filtering**
  - Refine scope of GPO within link based on WMI query
- **Preference targeting**

Group Policy Client and Client-Side Extensions

- How GPOs and their settings are *applied*
- *Group Policy Client* retrieves *ordered list of GPOs*
- GPOs are downloaded (then cached)
- Components called *client-side extensions (CSEs)* process the settings to apply the changes
  - One for each major category of policy settings: security, registry, script, software installation, mapped drive preferences, etc.
  - Most CSEs apply settings only if GPO (as a whole) has changed
    - Improves performance
    - Security CSE applies changes every 16 hours
  - GPO application is client driven ("pull")

Group Policy Refresh

- When GPOs and their settings are *applied*
- Computer Configuration
  - Startup
  - Every 90-120 minutes
  - Triggered: GPUpdate command
- User Configuration
  - Logon
  - Every 90-120 minutes
  - Triggered: GPUpdate command

Resultant Set of Policy

- The "cumulative" effect of Group Policy
  - A user or computer is usually within the scope of many GPOs
  - Potentially conflicting settings: precedence
- Tools to report the settings that were applied and which GPO "won" in the case of conflicting settings
- Tools to model the effects of changes to the Group Policy infrastructure or to the location of objects in Active Directory

Review and Discuss the Components of Group Policy

- Setting
- Scope
- Application
- Tools

Lesson 2: Implement GPOs

- Local GPOs
- Domain-Based GPOs
- Demonstration: Create, Link, and Edit GPOs
- GPO Storage
- Demonstration: Policy Settings

Local GPOs

- Apply before domain-based GPOs
  - Any setting specified by a domain-based GPO will override the setting specified by the local GPOs.
- Local GPO
  - *One* local GPO in Windows 2000, Windows XP, Windows Server® 2003
  - Multiple local GPOs in Windows Vista® and later
    - Local GPO: Computer settings and settings for all users
    - Administrators GPO: Settings for users in Administrators
    - Non-administrators GPO: Settings for users not in Admins
    - Per-user GPO: Settings for a specific user
- If domain members can be centrally managed using domain-linked GPOs, in what scenarios might local GPOs be used?

Domain-Based GPOs

- Created in Active Directory, stored on domain controllers
- Two default GPOs
  - Default Domain Policy
    - Define account policies for the domain: Password, account lockout, and Kerberos policies
  - Default Domain Controllers Policy
    - Define auditing policies for domain controllers and Active Directory

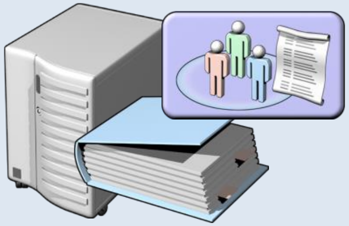
GPO Storage

Group Policy Object (GPO)

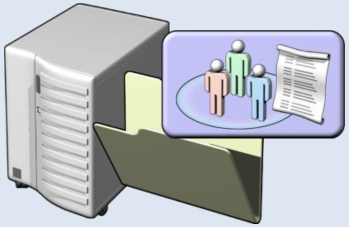
- What we call a GPO is actually two things, stored in two places

Group Policy Container (GPC)

- Stored in AD DS
- Friendly name, globally unique identifier (GUID)
- Version



Group Policy Template (GPT)



- Stored in SYSVOL on domain controllers (DCs)
- Contains all files required to define and apply settings
- .ini file contains Version

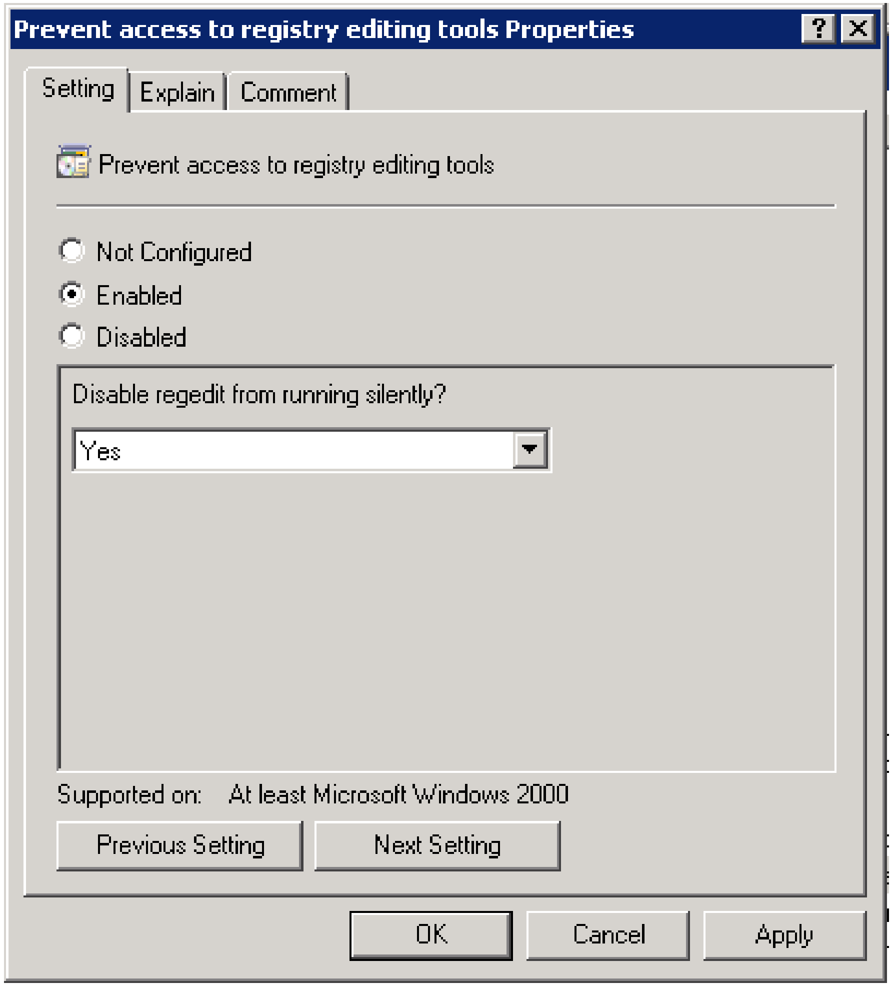
- Separate replication mechanisms
- GPOTool
  - Microsoft® Downloads Center

Lesson 3: A Deeper Look at Settings and GPOs

- Registry Policies in the Administrative Templates Node
- Managed Settings, Unmanaged Settings, and Preferences
- Administrative Templates
- The Central Store
- Demonstration: Work with Settings and the GPOs
- Managed GPOs and their Settings

Registry Policies in the Administrative Templates Node

- Policy settings in the Administrative Templates node make changes to the registry
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
  - DisableRegeditMode
    - 1 – Regedit UI tool only
    - 2 – Also disable regedit /s



Prevent access to registry editing tools Properties

Prevent access to registry editing tools

○ Not Configured
● Enabled
○ Disabled

Disable regedit from running silently?

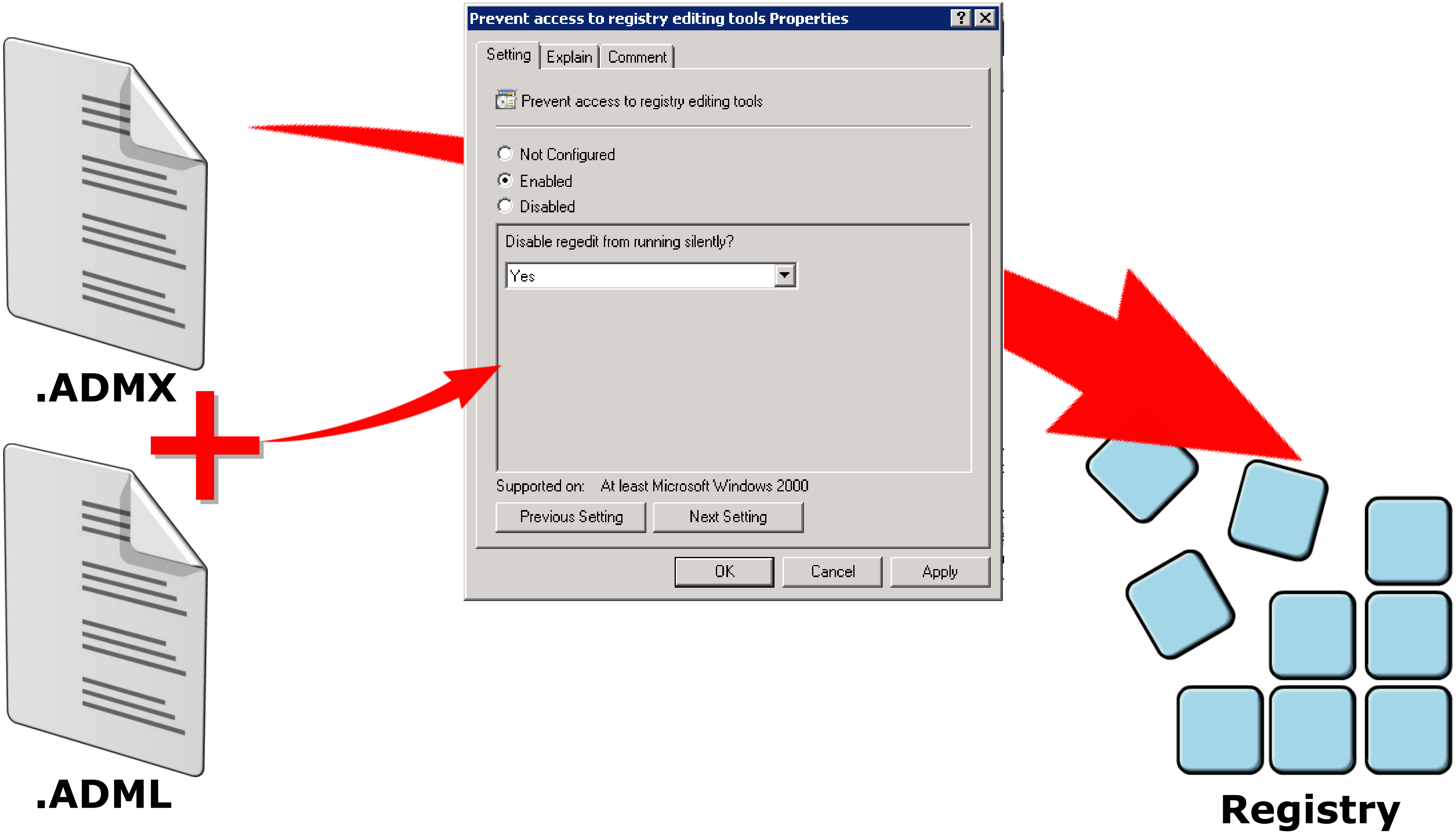
Yes

Supported on: At least Microsoft Windows 2000

Managed Settings, Unmanaged Settings, and Preferences

- Administrative templates
  - Managed policy setting
    - User interface (UI) is locked; user cannot make a change to the setting
    - Changes are made in one of four reserved registry keys
    - Change and UI lock are "released" when the user/computer falls out of scope
  - Unmanaged policy setting
    - UI not locked
    - Makes a change that is persistent; "tattoos" the registry
  - Only managed setting shown by default
  - Set Filter Options to view unmanaged settings
- Preferences
  - Effects vary

Administrative Templates



Prevent access to registry editing tools Properties

Prevent access to registry editing tools

○ Not Configured
● Enabled
○ Disabled

Disable regedit from running silently?

Yes

Supported on: At least Microsoft Windows 2000

The Central Store

- .ADM files
  - Stored in the GPT
  - Leads to version control and GPO bloat problems
- .ADMX/.ADML files
  - Retrieved from the client
  - Problematic if the client doesn't have the appropriate files
- Central Store
  - Create a folder called PolicyDefinitions on a DC
    - Remotely: \\contoso.com\SYSVOL\contoso.com\Policies\PolicyDefinitions
    - Locally: %SystemRoot%\SYSVOL\contoso.com\Policies\PolicyDefinitions
  - Copy .ADMX files from your %SystemRoot%\PolicyDefinitions
  - Copy .ADML file from language-specific subfolders (such as en-us)

Manage GPOs and Their Settings

- *Copy* (and *Paste* into a Group Policy Objects container)
  - Create a new "copy" GPO and modify it
  - Transfer a GPO to a trusted domain, such as test-to-production
- *Back Up* all settings, objects, links, permissions (access control lists [ACLs])
- *Restore* into same domain as backup
- *Import Settings* into a new GPO in same or any domain
  - Migration table for source-to-destination mapping of UNC paths and security group names
  - *Replaces all settings* in the GPO – not a "merge"
- *Save Report*
- *Delete*
- *Rename*

Discussion

- Describe the relationship between administrative template files (both .ADMX and .ADML files) and the GPME.
- When does an enterprise get a central store? What benefits does it provide?
- What are the advantages of managing Group Policy from a client running the latest version of Windows? Do settings you manage apply to previous versions of Windows?

Lesson 4: Manage Group Policy Scope

- GPO Links
- GOP Inheritance and Precedence
- Group Policy Processing Order
- Use Security Filtering to Modify GPO Scope
- WMI Filters
- Enable or Disable GPOs and GPO Nodes
- Target Preferences
- Loopback Policy Processing

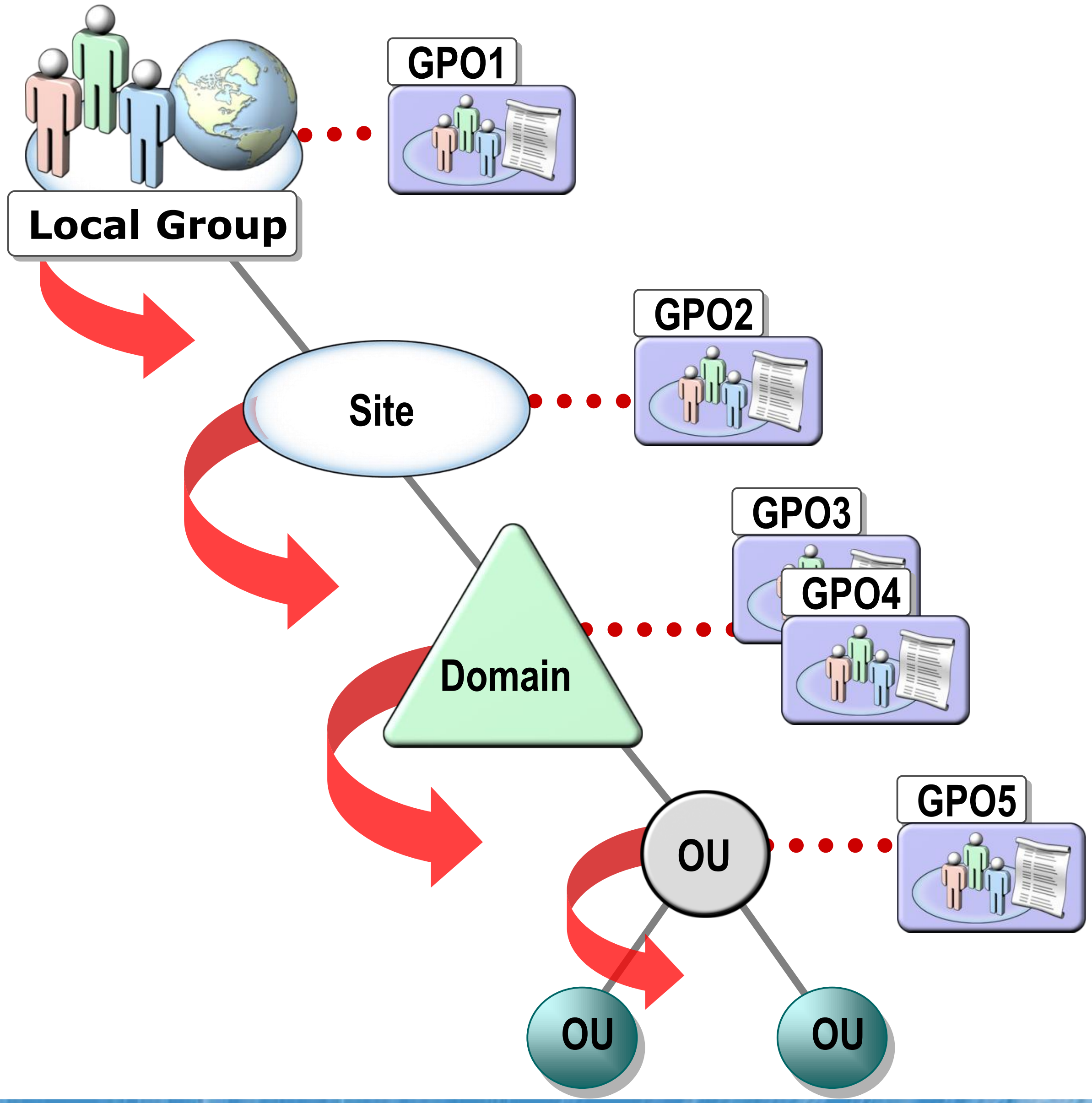
GPO Links

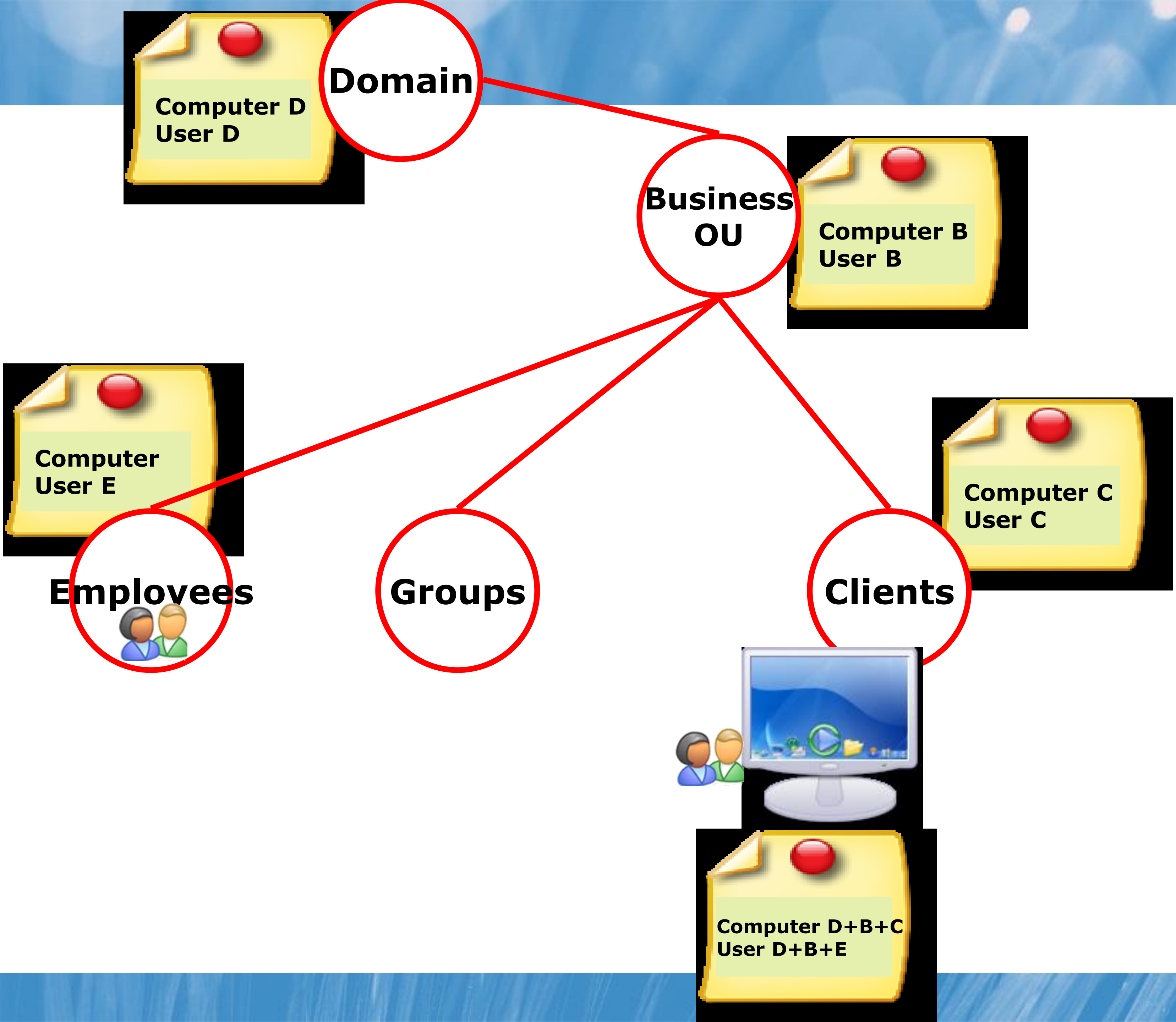
- GPO link
  - Causes policy settings in GPO to apply to *users* or *computers* within that container
  - Links GPO to site, domain, or OU (SDOU)
    - Must enable sites in the GPM console
  - GPO can be linked to multiple sites or OUs
  - Link can exist but be disabled
  - Link can be deleted, but GPO remains

GPO Inheritance and Precedence

- The application of GPOs linked to each container results in a cumulative effect called *inheritance*
  - Default Precedence: Local → Site → Domain → OU → OU… (LSDOU)
  - Seen on the Group Policy Inheritance tab
- Link order (attribute of GPO Link)
  - Lower number → Higher on list → Precedent
- Block Inheritance (attribute of OU)
  - Blocks the processing of GPOs from above
- Enforced (attribute of GPO Link)
  - Enforced GPOs “blast through” Block Inheritance
  - Enforced GPO settings win over conflicting settings in lower GPOs

Group Policy Processing Order





Domain

Computer D
User D

Business OU

Computer B
User B

Computer
User E

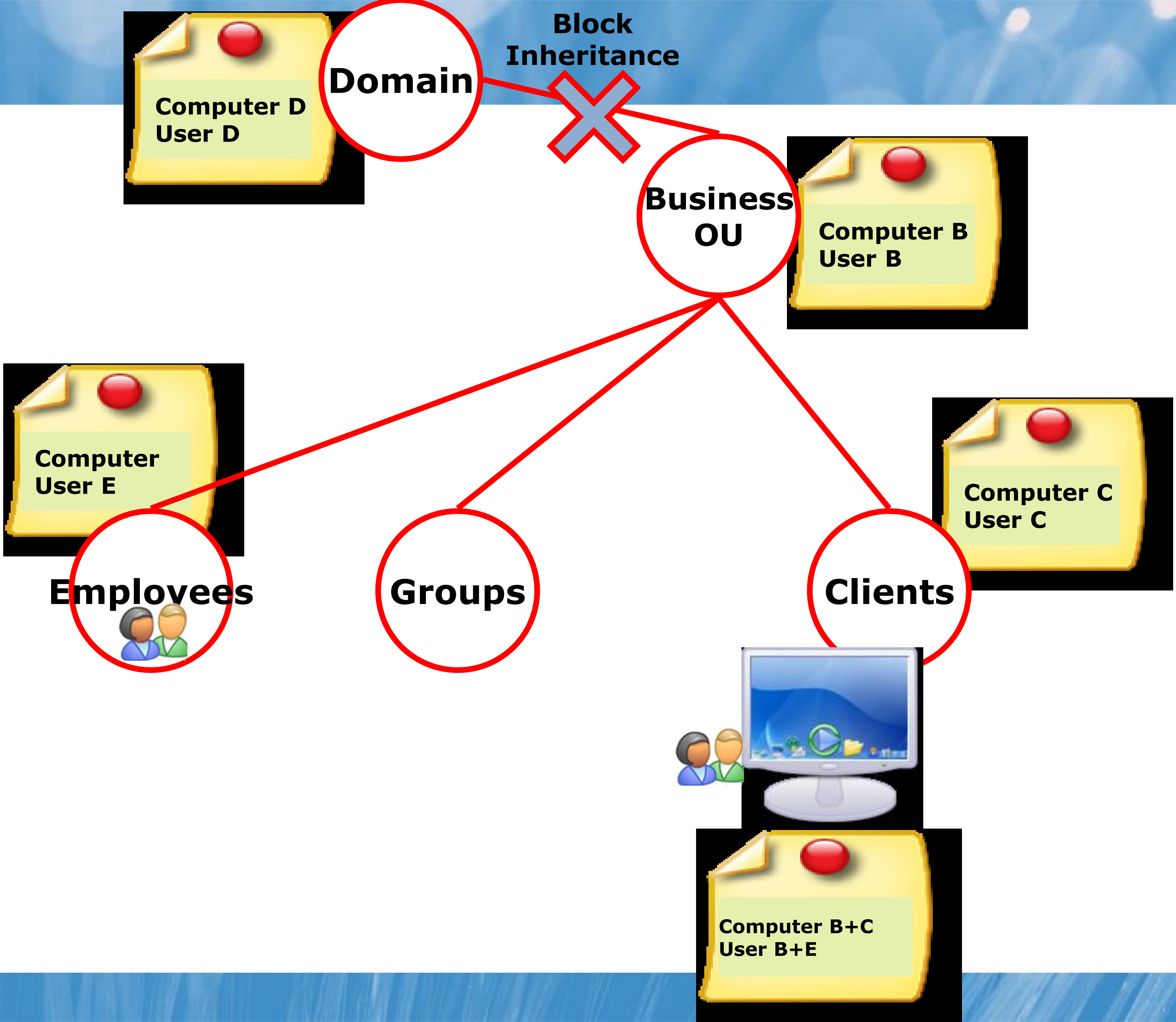
Employees

Groups

Clients

Computer C
User C

Computer D+B+C
User D+B+E



Domain

Computer D
User D

Block Inheritance

Business OU

Computer B
User B

Computer
User E

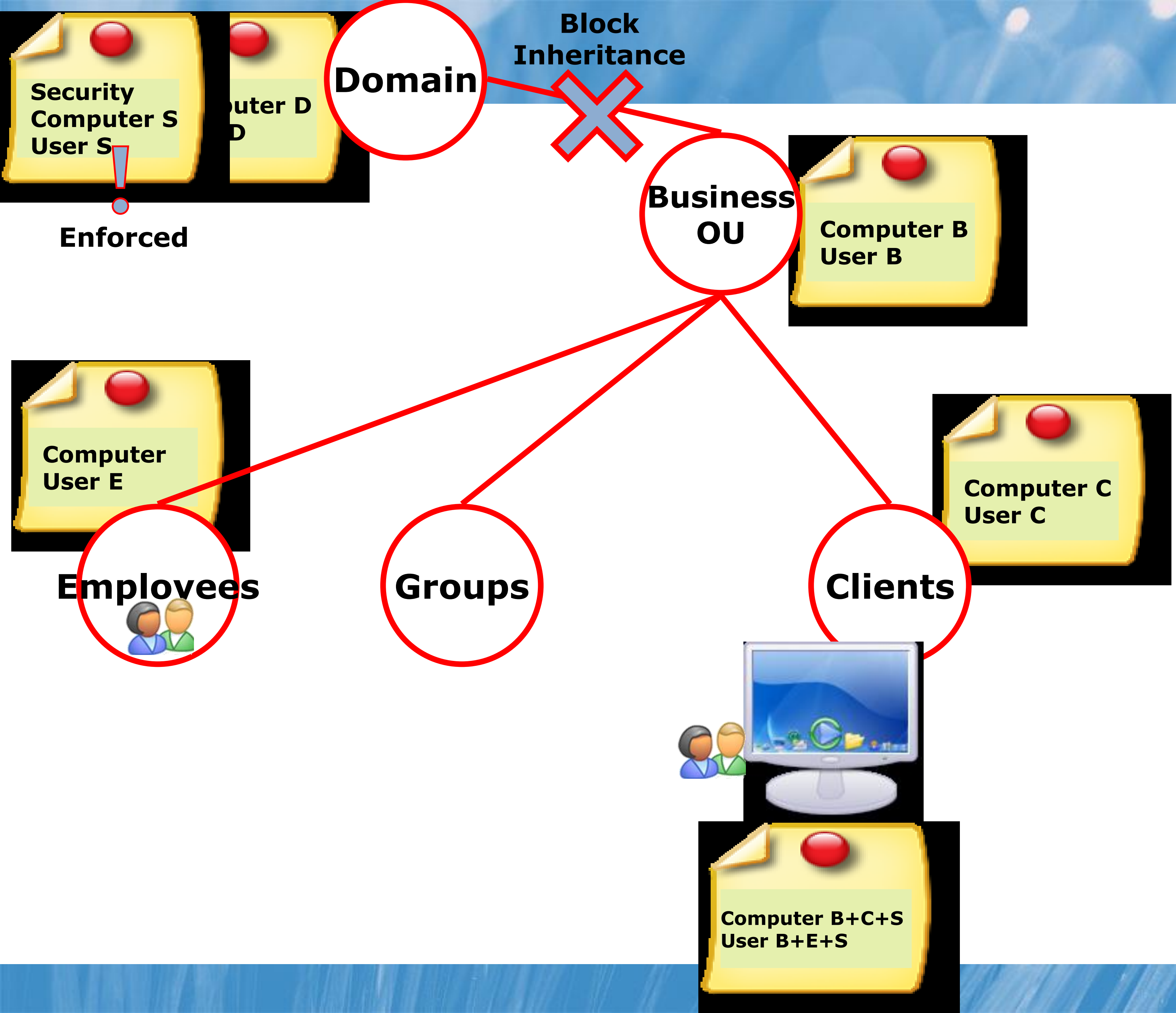
Employees

Groups

Clients

Computer C
User C

Computer B+C
User B+E



Security
Computer S
User S

uter D
D

Enforced

Domain

Block
Inheritance

Business
OU

Computer B
User B

Computer
User E

Employees

Groups

Clients

Computer C
User C

Computer B+C+S
User B+E+S

Use Security Filtering to Modify GPO Scope

- Apply Group Policy permission
  - GPO has an ACL (Delegation tab → Advanced)
  - Default: Authenticated Users have Allow Apply Group Policy
- Scope *only* to users in selected global group(s)
  - Remove Authenticated Users
  - Add appropriate *global* groups
    - Must be *global* groups (GPOs don’t scope to domain local)
- Scope to users *except for* those in selected group(s)
  - On Delegation tab, click Advanced
  - Add appropriate *global* groups
  - *Deny* Apply Group Policy permission
  - Does not appear on Delegation tab or in filtering section ☹

WMI Filters

- Windows Management Instrumentation (WMI)
- WMI Query Language (WQL)
  - Similar to T-SQL

  -
    ```
    Select * FROM Win32_OperatingSystem WHERE
    Caption="Microsoft Windows XP Professional" AND
    CSDVersion="Service Pack 3"
    ```
- Create a WMI filter
- Use the filter for one or more GPOs

Enable or Disable GPOs and GPO Nodes

- GPO Details tab → GPO Status drop-down list
- Enabled: Both Computer Configuration and User Configuration settings will be applied by CSEs
- All settings disabled: CSEs will not process the GPO
- Computer Configuration settings disabled: CSEs will not process settings in Computer Configuration
- User Configuration settings disabled: CSEs will not process settings in User Configuration

Lesson 5: Group Policy Processing

- A Detailed Review of Group Policy Processing
- Slow Links and Disconnected Systems
- Understand When Settings Take Effect

A Detailed Review of Group Policy Processing

- Computer starts; Remote Procedure Call System Service (RPCSS) and Multiple Universal Naming Convention Provider (MUP) are started
- Group Policy Client starts and obtains an ordered list of GPOs that are scoped to the computer
  - Local → Site → Domain → OU → Enforced GPOs
- GPC processes each GPO in order
  - Should it be applied? (enabled/disabled/permission/WMI filter)
  - CSEs are triggered to process settings in GPO
    - Settings configured as Enabled or Disabled are processed
- User logs on
- Process repeats for user settings
- Every 90-120 minutes after startup, computer refresh
- Every 90-120 minutes after logon, user refresh

Slow Links and Disconnected Systems

- Group Policy Client determines whether link to domain should be considered slow link
  - By default, less than 500 kilobits per second (kbps)
  - Each CSE can use determination of slow link to decide whether it should process or not
    - Software CSE, for example, does not process
- Disconnected
  - Settings previously applied will continue to take effect
  - Exceptions include startup, logon, logoff, and shutdown scripts
- Connected
  - Windows Vista and later operating systems detect new connection and perform Group Policy refresh if refresh window was missed while disconnected

Understand When Settings Take Effect

- GPO replication must happen
  - GPC and GPT must replicate
- Group changes must be incorporated
  - Logoff/logon for user; restart for computer
- Group Policy refresh must occur
  - Windows XP, Windows Vista, and Windows 7 clients
  - Always wait for network at startup and logon
- Settings may require logoff/logon (user) or restart (computer) to take effect
- Manually refresh: GPUpdate [/force] [/logoff] [/boot]
- Most CSEs do not re-apply settings if GPO has not changed
  - Configure in Computer\Admin Templates\System\Group Policy

Lesson 6: Troubleshoot Policy Application

- Resultant Set of Policy
- Generate RSoP Reports
- Perform What-If Analyses with the Group Policy Modeling Wizard
- Examine Policy Event Logs

Resultant Set of Policy

- Inheritance, filters, loopback, and other policy scope and precedence factors are complex!
- RSoP
  - The "end result" of policy application
  - Tools to help evaluate, model, and troubleshoot the application of Group Policy settings
- RSoP analysis
  - The Group Policy Results Wizard
  - The Group Policy Modeling Wizard
  - GPResult.exe

Generate RSoP Reports

- Group Policy Results Wizard
  - Queries WMI to report *actual* Group Policy application
- Requirements
  - Administrative credentials on the target computer
  - Access to WMI (firewall)
  - User must have logged on at least once
- RSoP report
  - Can be saved
  - View in Advanced mode
    - Shows some settings that do not show in the HTML report
    - View Group Policy processing events
- `GPResult.exe /s` *`ComputerName`* `/h` *`filename`*

Perform What-If Analyses with the Group Policy Modeling Wizard

- Group Policy Modeling Wizard
  - Emulates Group Policy application to report *anticipated* RSoP

Examine Policy Event Logs

- System log
  - High-level information about Group Policy
  - Errors elsewhere in the system that could impact Group Policy
- Application log
  - Events recorded by CSEs
- Group Policy Operational log
  - Detailed trace of Group Policy application