Diploma in Infocomm & Security

IT2654: Systems Administration & Security

TOPIC 4: IMPLEMENTING AND USING GROUP POLICY

Module Overview

- Introducing Group Policy
- Implementing and Administering GPOs
- Group Policy Scope and Group Policy Processing
- Deploy and manage software using Group Policy
- Troubleshooting the Application of GPOs

Lesson 1: Introducing Group Policy

- What Is Configuration Management?
- Overview of Group Policies
- Benefits of Using Group Policy
- Group Policy Objects
- GPO Scope
- Group Policy Client and Client-Side Extensions

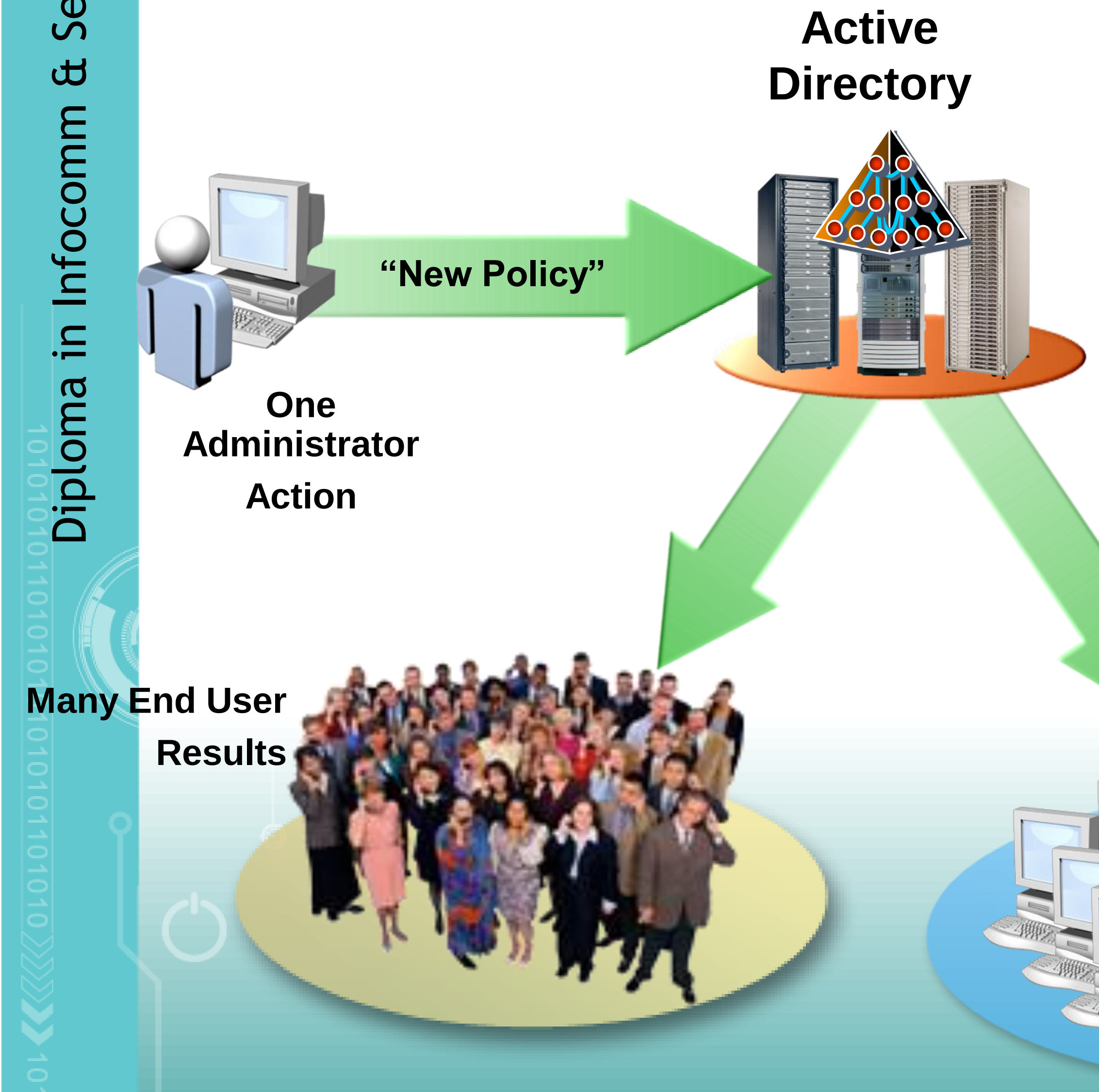
Introduction to Group Policy

- **Group policy** centralizes management of user and computer configuration settings throughout a network
- A **group policy object** is an Active Directory object used to configure policy settings for user and computer objects
- There are two default Group Policy Objects:
  - Default Domain Policy (linked to domain container)
  - Default Domain Controllers Policy (linked to domain controller OU)

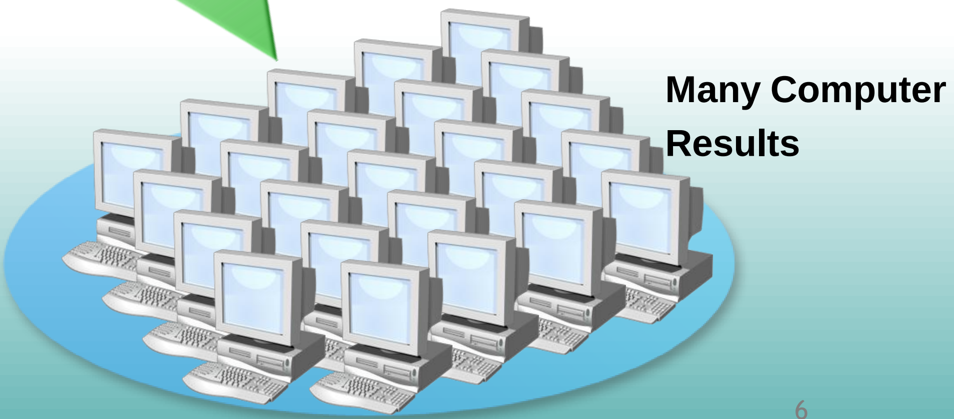
What Is Configuration Management?

- Configuration management is a centralized approach to applying one or more changes to one or more users or computers
- The key elements of configuration management are:
  - Setting
  - Scope
  - Application

Configuration Management



- Group Policy enables administrators to set and maintain a desired computing state
- Allows for mass-customization – scalability without sacrificing flexibility to customize
- Group Policy Management Console (GPMC) for administration



Overview of Group Policies

- The most granular component of Group Policy is known as a *policy* and defines a specific configuration change
- Most policy settings can have three states:
  - Not Configured
  - Enabled
  - Disabled
- Many policy settings are complex, and the effect of enabling or disabling them might not be obvious

Diploma in Infocomm & Security

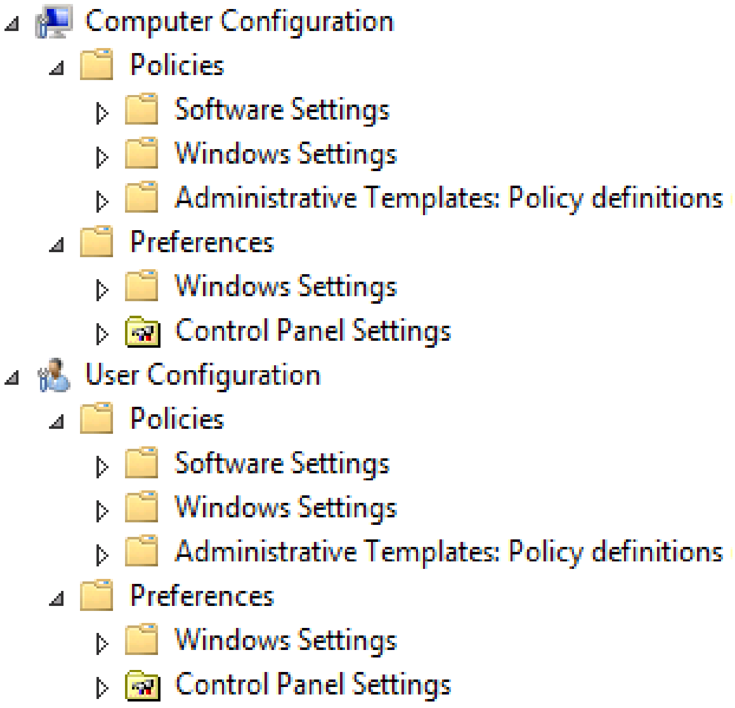
Benefits of Using Group Policy

- GPOs are very powerful administrative tools and you can use them to enforce various types of settings to a large number of users and computers
- Typically, GPOs are used in the following way:
  - 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 the Group Policy Management Editor (GPME)
- Applied to a specific level in the AD DS hierarchy



```
◢ Computer Configuration
    ◢ Policies
        ▷ Software Settings
        ▷ Windows Settings
        ▷ Administrative Templates: Policy definitions
    ◢ Preferences
        ▷ Windows Settings
        ▷ Control Panel Settings
◢ User Configuration
    ◢ Policies
        ▷ Software Settings
        ▷ Windows Settings
        ▷ Administrative Templates: Policy definitions
    ◢ Preferences
        ▷ Windows Settings
        ▷ Control Panel Settings
```

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

Group Policy Client and Client-Side Extensions (CSE)

1. Group Policy Client retrieves GPOs
2. Client downloads and caches GPOs
3. CSEs process the settings

- Policy settings in the Computer Configuration node are applied at system startup and every 90–120 minutes thereafter
- User Configuration policy settings are applied at logon and every 90–120 minutes thereafter

Lesson 2: Implementing and Administering GPOs

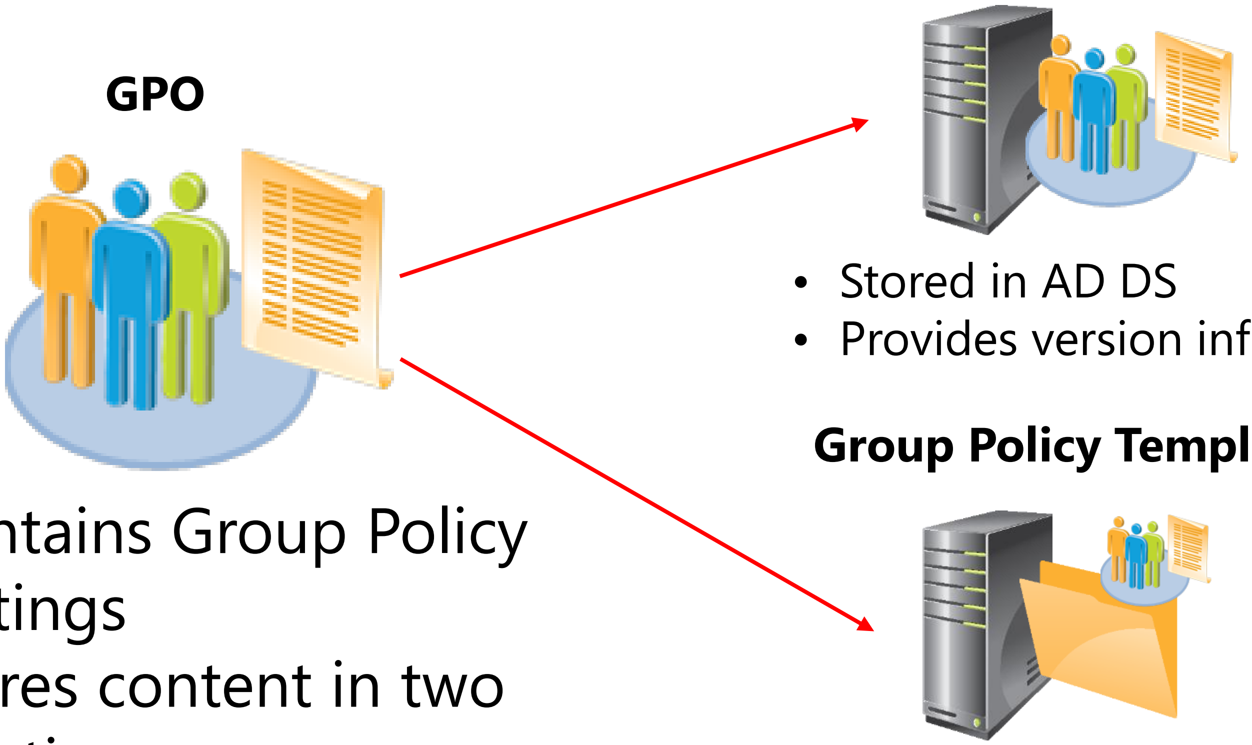
- Domain-Based GPOs
- GPO Storage
- Starter GPOs
- Common GPO Management Tasks
- Managing GPOs with Windows PowerShell

Default GPOs

There are two default GPOs:

- **Default Domain Policy**
  - Used to define the account policies for the domain:
    - Password
    - Account lockout
    - Kerberos protocol
- **Default Domain Controllers Policy**
  - Used to define auditing policies
  - Defines user rights on domain controllers

GPO Storage



GPO

- Contains Group Policy settings
- Stores content in two locations

Group Policy Container

- Stored in AD DS
- Provides version information

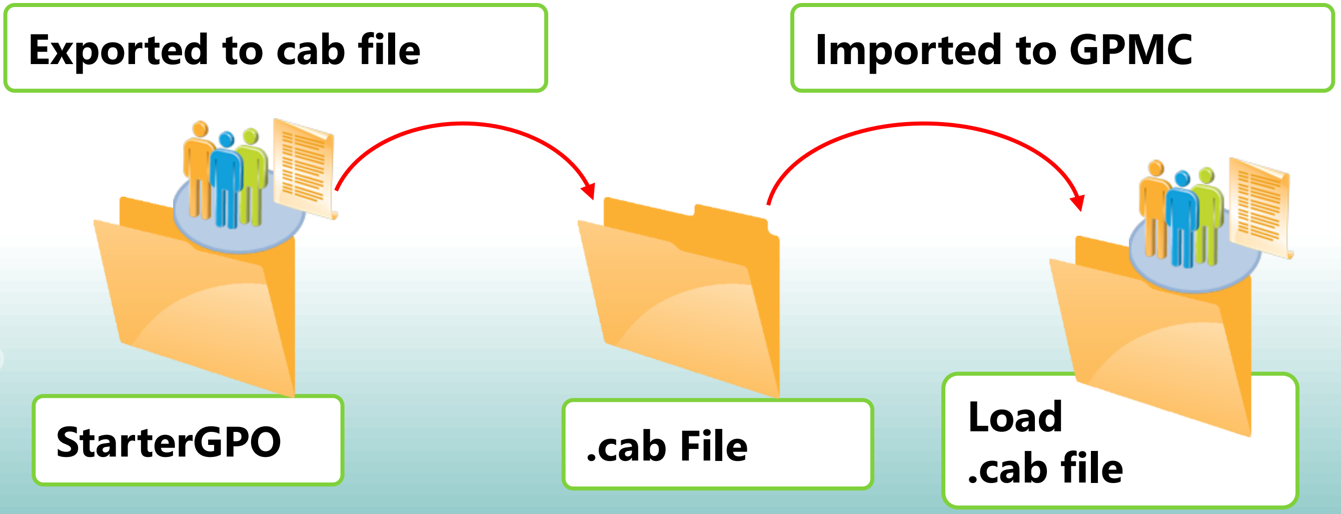
Group Policy Template

- Stored in a shared **SYSVOL** folder
- Provides Group Policy settings

Default Domain Policy – GUID: {31B2F340-016D-11D2-945F-00C04FB984F9}
Default Domain Controllers Policy – GUID: {6AC1786C-016F-11D2-945F-00C04FB984F9}

Starter GPOs

- Stores Administrative Template settings on which the new GPOs will be based
- Can be exported to .cab files
- Can be imported into other areas of the enterprise

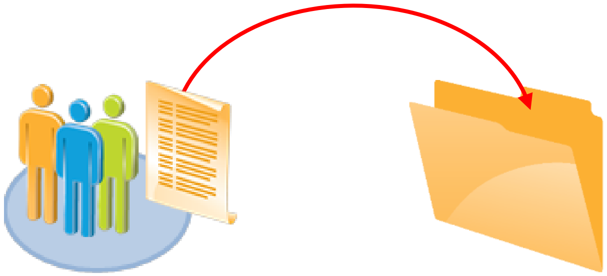


Diploma in Infocomm & Security

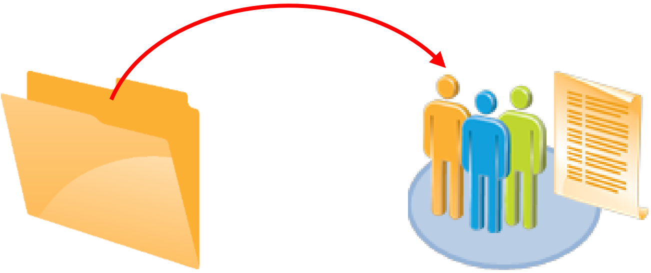
Common GPO Management Tasks

GPMC provides several options for managing the state of GPOs

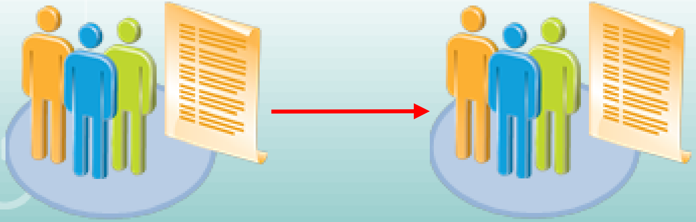
Backup GPOs



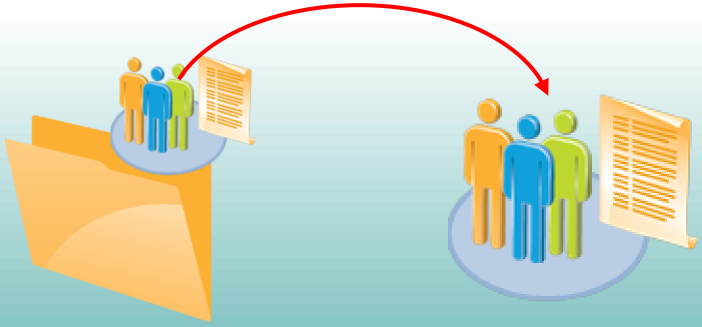
Restore GPOs



Copy GPOs



Import GPOs



Managing GPOs with Windows PowerShell

In addition to using GPMC and the Group Policy Management Editor, you can also perform common GPO administrative tasks by using Windows PowerShell

Examples:

- Create a new GPO called Sales:
  New-GPO -Name Sales -comment "This the sales GPO"
- Import the settings from the backup Sales GPO in the C:\Backups folder into the NewSales GPO:
  import-gpo -BackupGpoName Sales -TargetName NewSales -path c:\backups

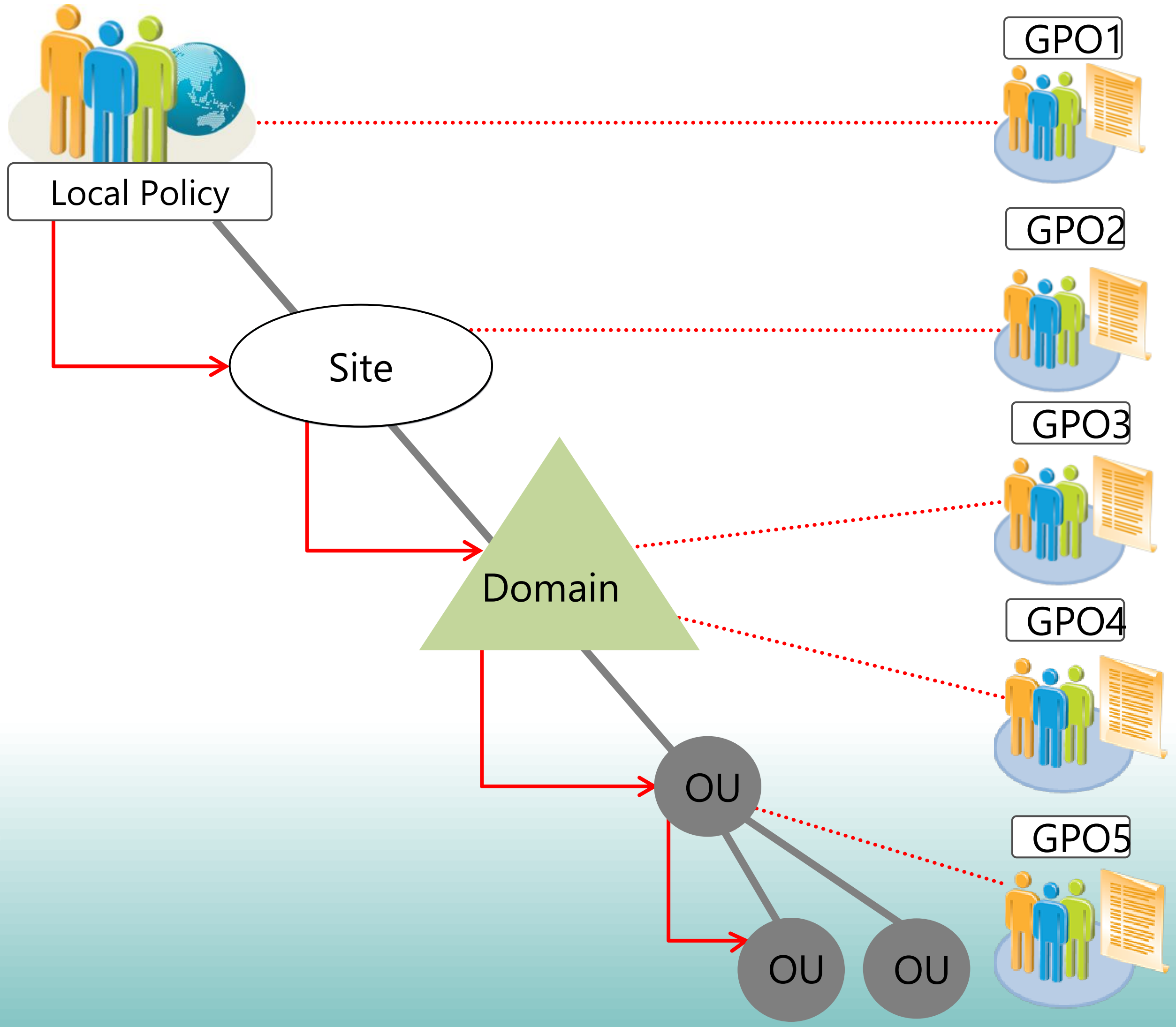
Lesson 3: Group Policy Scope and Group Policy Processing

- GPO Links
- Group Policy Processing Order
- Configuring GPO Inheritance and Precedence
- Using Security Filtering to Modify Group Scope
- WMI Filters
- Identifying When Settings Become Effective

GPO Links

- ❖ To deliver settings to an object, a GPO must be linked to a container
- ❖ Disabling a link removes the settings from the container
- ❖ Deleting a link does not delete the GPO
- ❖ GPOs can be linked to:
  - **Sites**
  - **Domains**
  - **OUs**
- ❖ GPOs cannot be linked to:
  - **Users**
  - **Groups**
  - **Computers**
  - **System containers**

Group Policy Processing Order

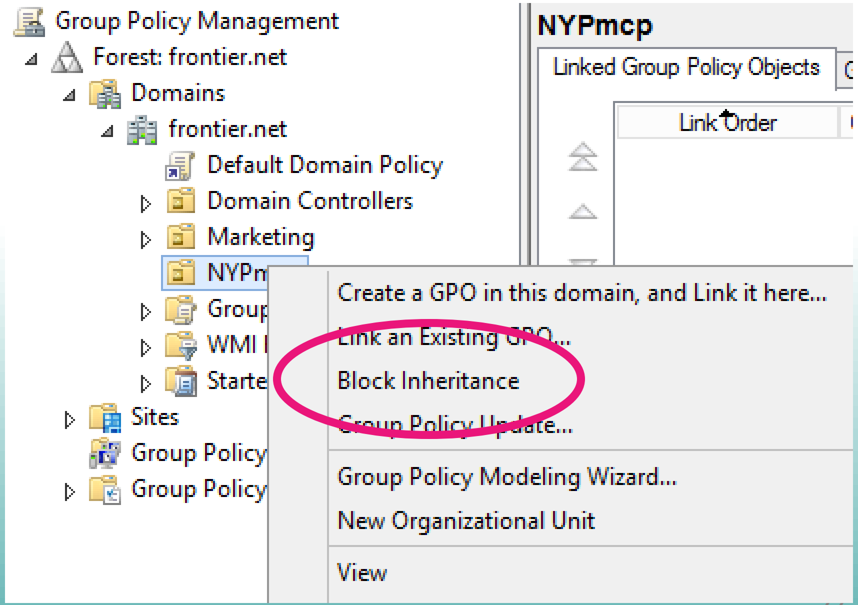


Configuring GPO Inheritance and Precedence

1. The application of GPOs that are 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**
2. Link order (attribute of GPO Link)
   - Lower number → Higher on list → Precedent
3. Block Inheritance (attribute of OU)
   - Blocks the processing of GPOs from above
4. Enforced (attribute of GPO link)
   - Enforced GPOs “blast through” Block Inheritance
   - Enforced GPO settings win over conflicting settings in lower GPOs

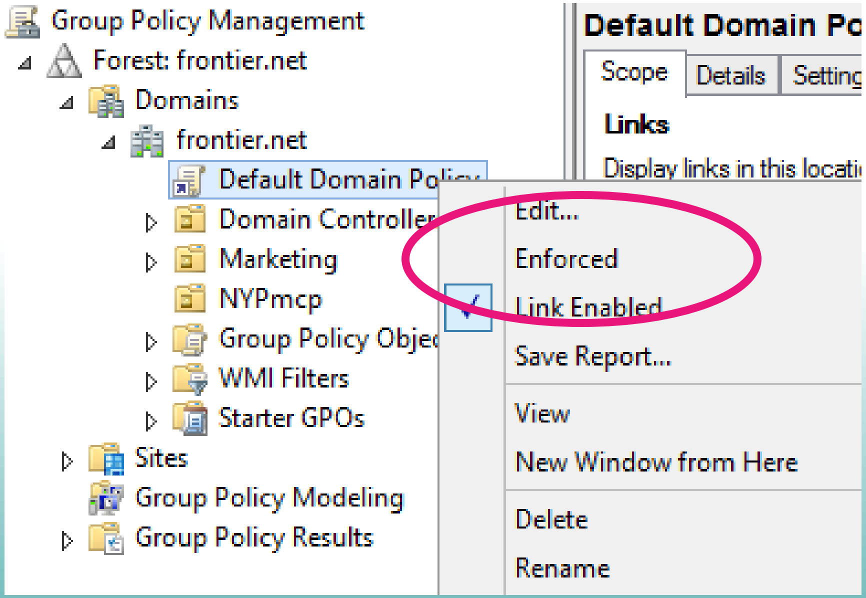
Blocking Group Policy Inheritance

- To change default inheritance, use the Block Policy inheritance check box on the Group Policy tab for a child container
  - Child will not inherit parent’s policies
  - Useful if one OU needs to be managed separately



Configuring Enforced

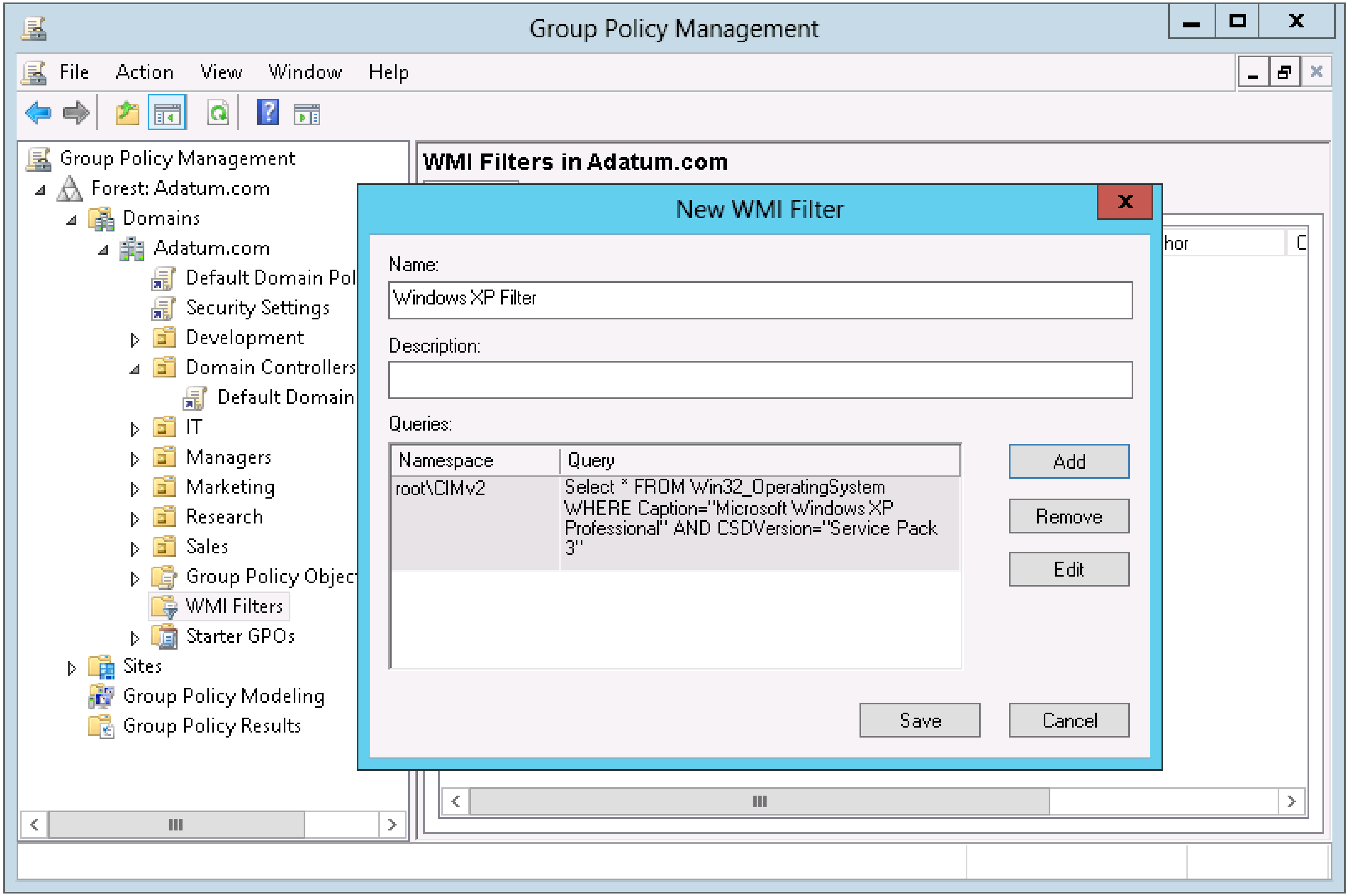
- If a policy is configured with Enforced
  - It will be enforced despite conflicts in lower-level policies
  - It will be enforced on lower-level containers with Block Policy inheritance set



Modify Group Scope thru Security Filtering

- How can I get a GPO to apply to a group?
- Group Policy permission
  - ACL (Access Control List) – GPO → Delegation
  - ACL Editor – GPO → Delegation tab → Advanced
- Apply GPO to only users in selected (Global) groups
  - Remove Authenticated Users
  - Add appropriate GLOBAL groups
    - Must be Global groups (GPOs do not scope to domain local)

WMI Filters



Name: Windows XP Filter

Description:

Queries:

Namespace	Query
root\CIMv2	Select * FROM Win32_OperatingSystem WHERE Caption="Microsoft Windows XP Professional" AND CSDVersion="Service Pack 3"

Identifying When Settings Become Effective

- GPO replication must happen
- Group Policy refresh must occur
- User must log off or log on, or the computer must restart
- Manual refresh – **gpupdate /force**
- Most CSEs do not reapply unchanged GPO settings

Lesson 4: Deploying Software Using Group Policy

- Applications that can be deployed using Group Policy include:
  - Business applications (e.g., Microsoft Office)
  - Anti-virus software, software updates
- Four phases of software rollout
  1. Software preparation
  2. Deployment
  3. Software maintenance
  4. Software removal

Software Preparation

- Microsoft Windows installer package (MSI)
    - MSI file contains all of the information needed to install an application in a variety of configurations
    - Software vendors include preconfigured MSI packages
    - For older applications, can create MSI packages using 3rd party utilities (e.g., VERITAS)
- To install, place MSI file in a shared folder and configure Group Policy to access for installation

Software Preparation (continued)

- If application doesn’t have an MSI package can use ZAP file
  - Text file used by Group Policy to deploy an application
  - Can only be published and not assigned
  - Is not resilient
  - Requires user intervention and proper permissions

Deployment

- Two ways to deploy an application
  1) Assigning applications
  2) Publishing applications

Assigning Applications

- When a policy is created to assign an application
  - Any user which the policy applies to has a shortcut on the Start menu
    - Application is installed when user clicks shortcut the first time or opens it with an associated document
  - If policy configured in computer section, application is installed next time the computer is started
  - Applications are resilient (if files are corrupted, will reinstall itself)

Publishing Applications

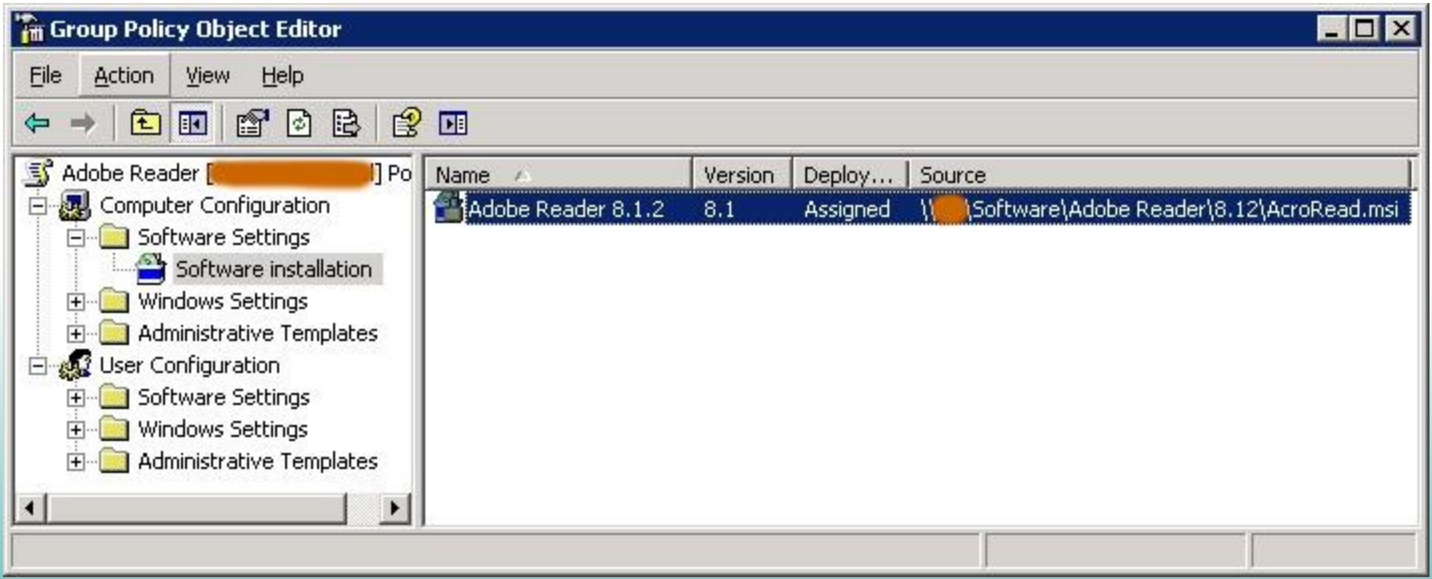
- When a policy is created to publish an application
  - Not advertised in Start menu
  - Installed using the Add/Remove Programs (or equivalent) applet or by opening an associated document
  - Only published to users and not computers

Configuring the Deployment

- Create or edit a GPO and specify deployment options
- Assign or publish application to computers or users to install at the appropriate time

Software Maintenance

- Software must be maintained with patches and updates
- Update via Group Policy
  - Update file must be in MSI format

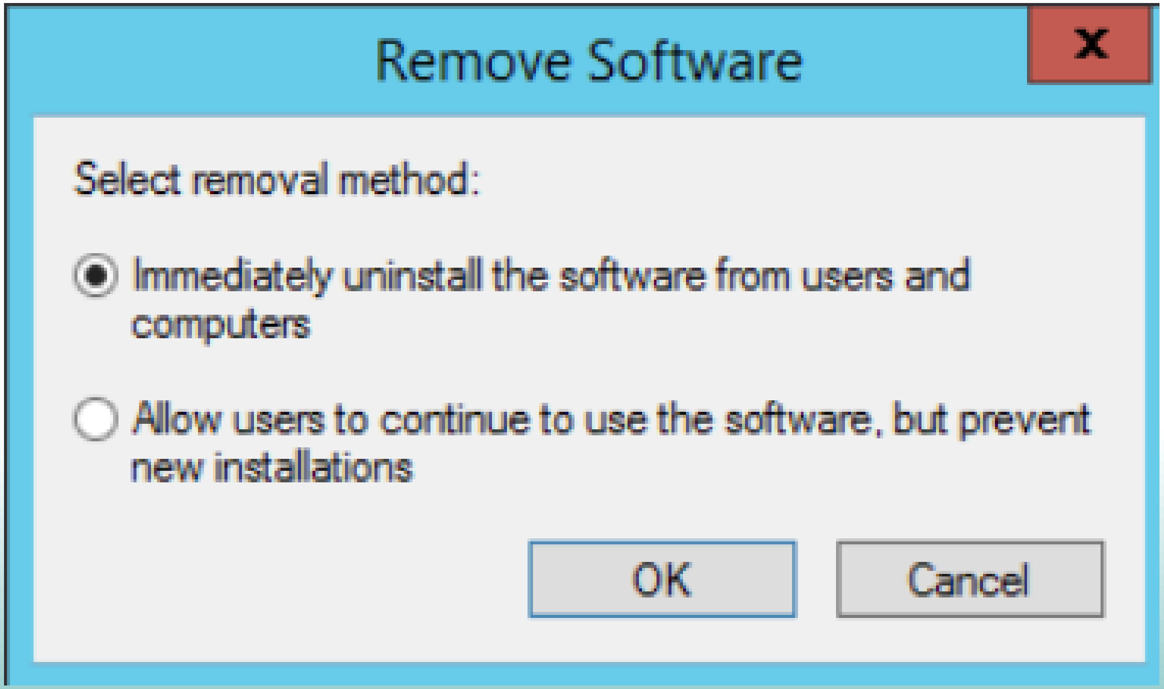


Adobe Reader [[redacted]] Po
- Computer Configuration
  - Software Settings
    - Software installation
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Name	Version	Deploy...	Source
Adobe Reader 8.1.2	8.1	Assigned	\\[redacted]\Software\Adobe Reader\8.12\AcroRead.msi

Software Removal

- Application must have been originally installed using a Windows installer package
- Removal can be:



Remove Software

Select removal method:

● Immediately uninstall the software from users and computers

○ Allow users to continue to use the software, but prevent new installations

Lesson 5: Troubleshooting the Application of GPOs

1) Refreshing GPOs
2) gpresult
3) RSoP
4) Policy Event Logs

Refreshing GPOs

- When you apply GPOs, remember that:
  - Computer settings apply at startup
  - User settings apply at logon
  - Polices refresh at regular, configurable intervals
  - Security settings refresh at least every 16 hours
  - Policies refresh manually by using:
    - The **gpupdate** command
    - The Windows PowerShell cmdlet **Invoke-GPUpdate**
  - new Remote Policy Refresh feature in Windows Server - can remotely refresh policies

gpresult

Use gpresult to:

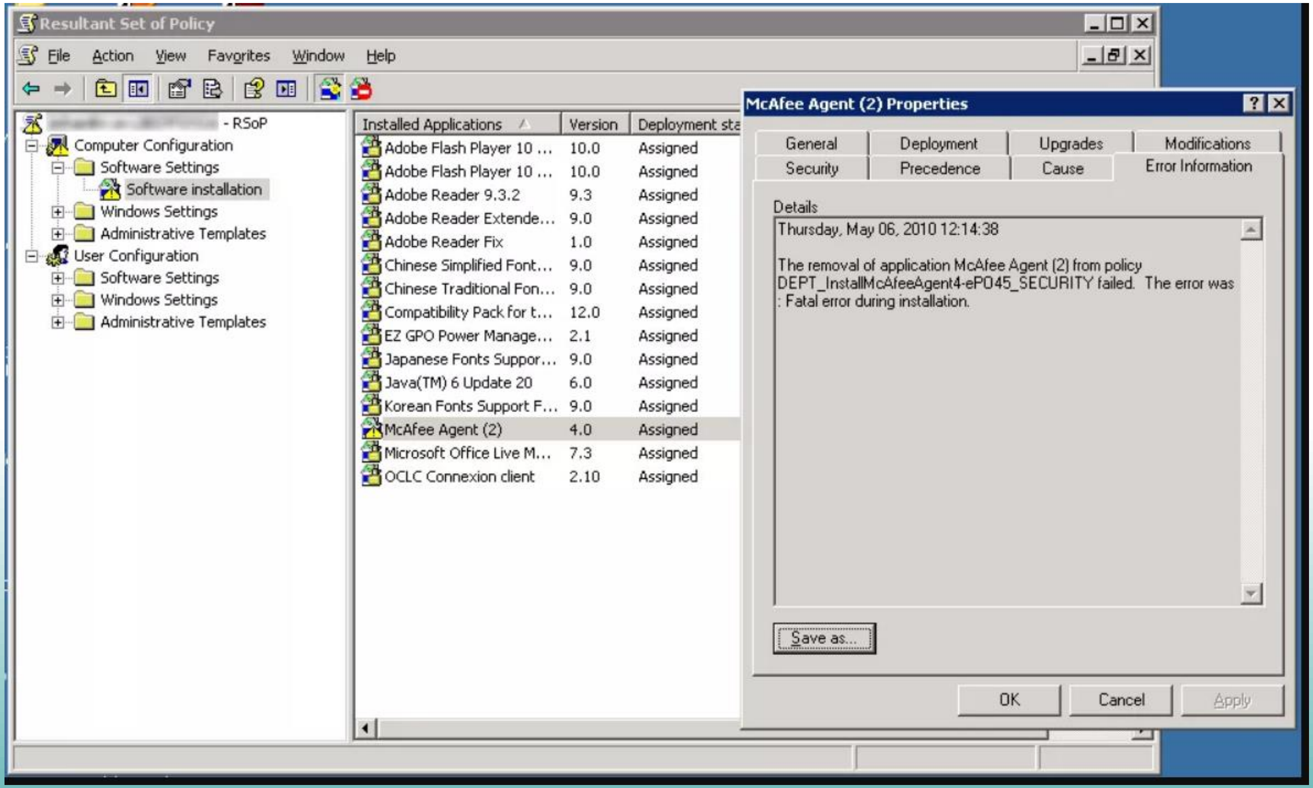
- Display the resulting set of policies for a user or computer
- Redirect the resulting set of policies information to a file

Example:

```
gpresult  /user  administrator  /V
```

RSoP

- Resultant Set of Policy
- rsop.msc
- Not all policies reported – gpresult more complete



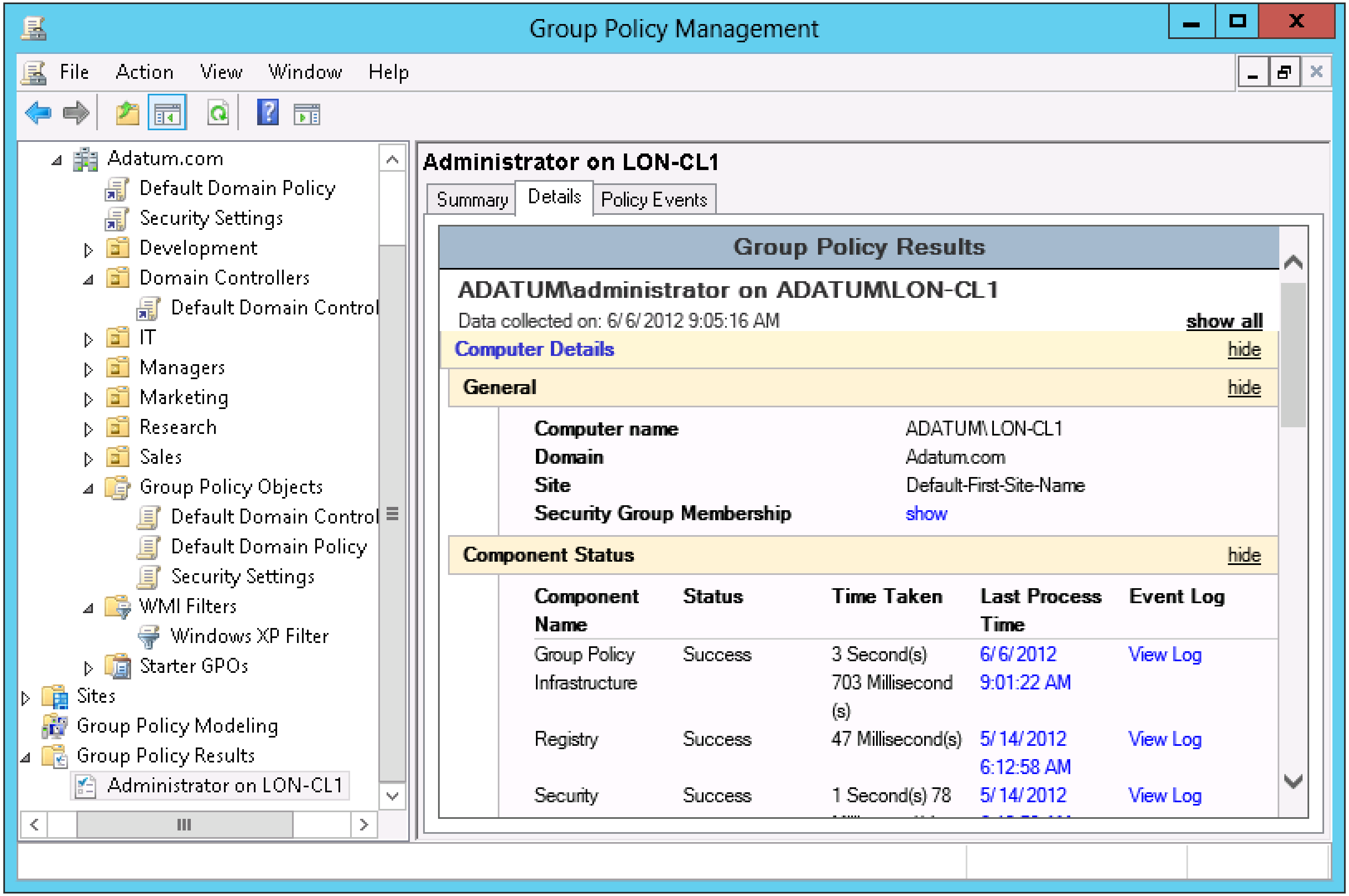
Installed Applications	Version	Deployment sta
Adobe Flash Player 10 ...	10.0	Assigned
Adobe Flash Player 10 ...	10.0	Assigned
Adobe Reader 9.3.2	9.3	Assigned
Adobe Reader Extende...	9.0	Assigned
Adobe Reader Fix	1.0	Assigned
Chinese Simplified Font...	9.0	Assigned
Chinese Traditional Fon...	9.0	Assigned
Compatibility Pack for t...	12.0	Assigned
EZ GPO Power Manage...	2.1	Assigned
Japanese Fonts Suppor...	9.0	Assigned
Java(TM) 6 Update 20	6.0	Assigned
Korean Fonts Support F...	9.0	Assigned
McAfee Agent (2)	4.0	Assigned
Microsoft Office Live M...	7.3	Assigned
OCLC Connexion client	2.10	Assigned

Details

Thursday, May 06, 2010 12:14:38

The removal of application McAfee Agent (2) from policy DEPT_InstallMcAfeeAgent4-eP045_SECURITY failed. The error was : Fatal error during installation.

Generate RSoP Reports



Administrator on LON-CL1

Group Policy Results

ADATUM\administrator on ADATUM\LON-CL1

Data collected on: 6/6/2012 9:05:16 AM — show all

Computer Details — hide

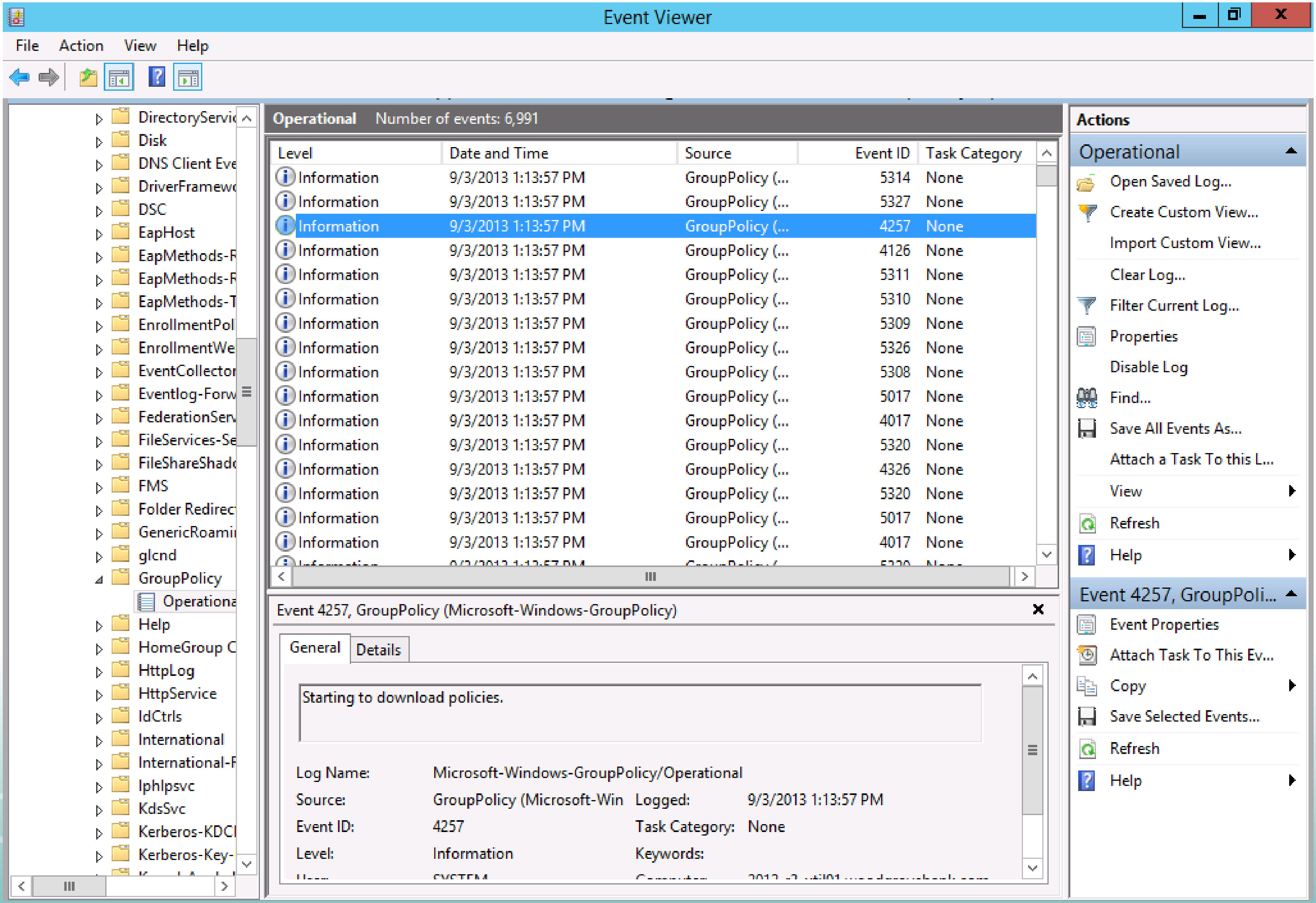
General — hide

Computer name	ADATUM\LON-CL1
Domain	Adatum.com
Site	Default-First-Site-Name
Security Group Membership	show

Component Status — hide

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

Policy Event Logs



Operational Number of events: 6,991

Level	Date and Time	Source	Event ID	Task Category
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5314	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5327	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	4257	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	4126	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5311	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5310	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5309	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5326	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5308	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5017	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	4017	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5320	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	4326	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5320	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	5017	None
Information	9/3/2013 1:13:57 PM	GroupPolicy (...	4017	None

Event 4257, GroupPolicy (Microsoft-Windows-GroupPolicy)

Starting to download policies.

Log Name: Microsoft-Windows-GroupPolicy/Operational
Source: GroupPolicy (Microsoft-Win Logged: 9/3/2013 1:13:57 PM
Event ID: 4257 Task Category: None
Level: Information Keywords:

Summary

- A Group Policy Object is an object in Active Directory used to configure and apply settings for user and computer objects
- Two default GPOs created when Active Directory is installed:
  - Default Domain Policy
  - Default Domain Controllers Policy
- Two mechanisms for creating GPOs
  - Microsoft Management Console Group Policy Editor snap-in
  - Group Policy Management

Summary

- GPOs can be used:
  - to control user desktop settings and security settings
  - to apply scripts on user logon and logoff and computer startup and shutdown
  - for folder redirection
- GPOs are applied in a specific order
- GPOs are inherited by default
  - Can be changed by Blocking Group Policy inheritance, configuring No Override, or filtering using user permissions
- Use GPRESULT or Resultant Set of Policy tool to view effective Group Policy settings
- GPOs are useful in deploying and maintaining software applications