ISHIK UNIVERSITY
2008

Department of Information Technology

Lesson 7: Creating Group Policy Objects

Server Management

Zina Yaaqub

Overview

- Create Group Policy Objects
- Introducing Group Policy
- Using the Group Policy Management Console
- Creating Multiple Local GPOs

Introducing Group Policy

- **Group Policy** is a mechanism for controlling and deploying operating system settings to computers all over your network.
- Consists of user and computer settings for the various Microsoft Windows operating systems.
- Implemented during computer startup and shutdown and user logon and logoff.
- Configure one or more Group Policy objects (GPOs) and then use a process called **linking** to associate them with specific Active Directory Domain System (AD DS) objects.
- When you link a GPO to a container object, all of the objects in that container receive the settings you configured in the GPO.

Group Policy: User Benefits

- Users can access their files, even when network connectivity is intermittent by using folder redirection and offline files.
- Users can work with a consistent computing environment, regardless of which workstation or location they use to log on.
- User files redirected to a server location can be backed up regularly, saving users from data loss due to workstation failure.
- Applications that become damaged or need to be updated can be reinstalled or maintained automatically.

Group Policy: Administrative Benefits

- Administrators have control over centralized configuration of user settings, application installation, and desktop configuration.
- Problems due to missing application files and other minor application errors often can be alleviated by the automation of application repairs.
- Centralized administration of user files eliminates the need and cost of trying to recover files from a damaged drive.
- The need to manually make security changes is reduced by the rapid deployment of new settings through Group Policy.

Group Policy Objects (GPOs)

- **Group Policy objects (GPOs**) contain all the Group Policy settings that administrators can deploy to user and computer objects within a site, domain, or organizational unit.
- To deploy a GPO, an administrator must associate it with the container to which it is deployed (linking).
- Administrative tasks for Group Policy include:
  - Creating GPOs
  - Specifying where GPOs are stored
  - Managing the AD DS links

Types of GPOs

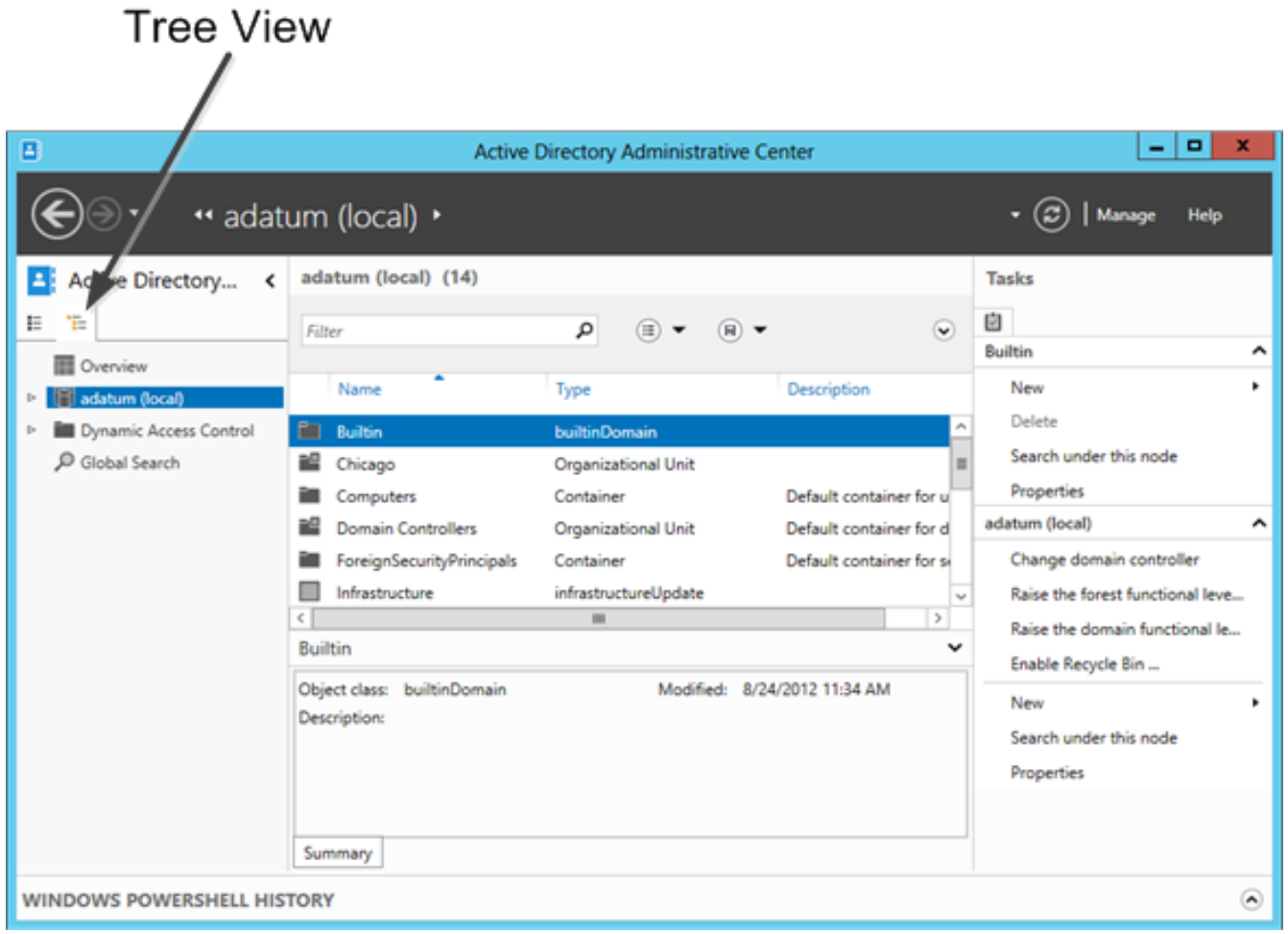
There are three types of GPOs:

- **Local GPOs**: On the local computer only
- **Domain GPOs**: Created in Active Directory
  - Linked to sites, domains, or OUs
- **Starter GPOs**: Template GPO based on a standard collection of settings

Viewing the Group Policy Container

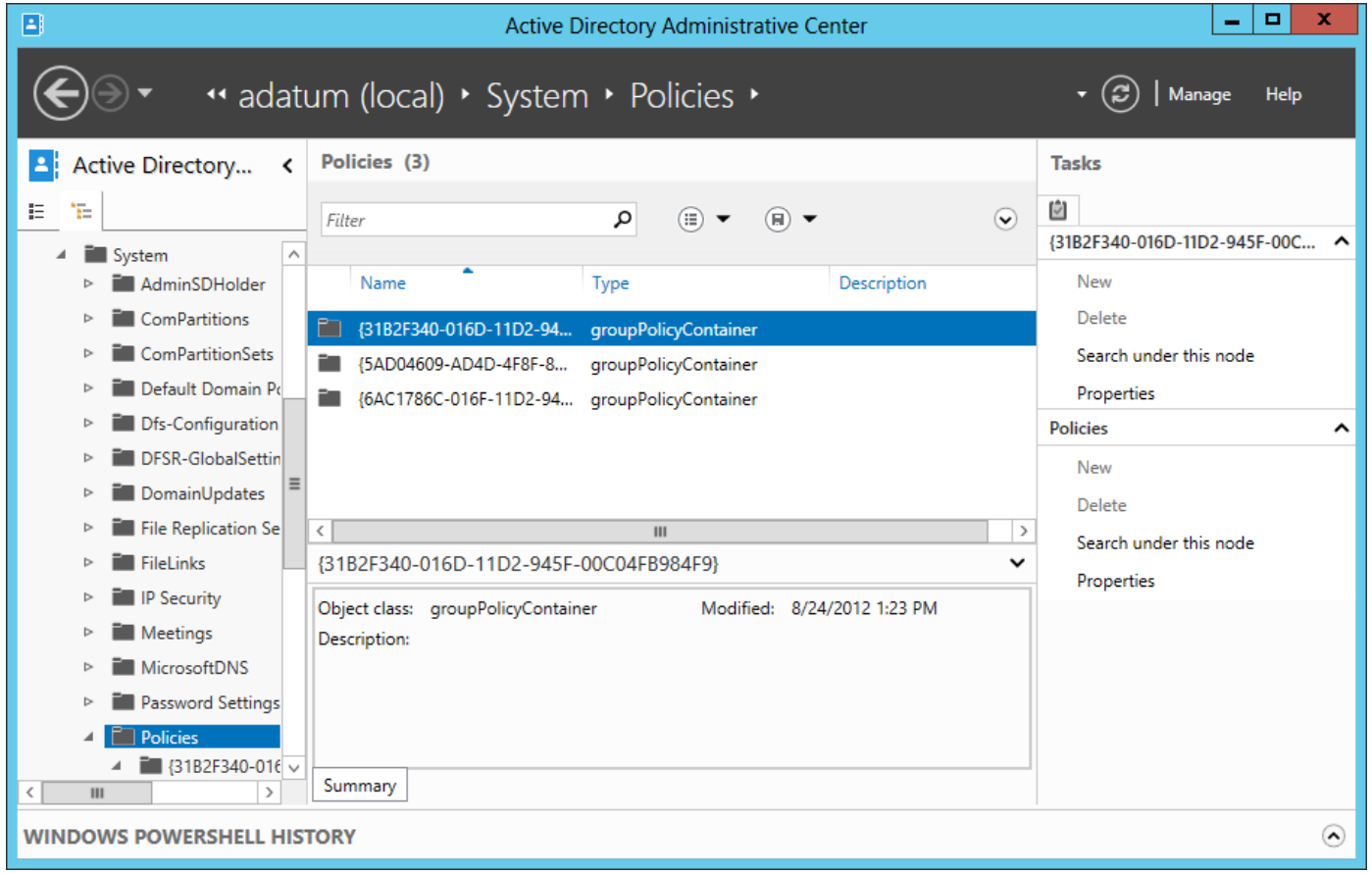
- The **Group Policy container (GPC)** directory object includes subcontainers that hold GPO policy information
- Two GPOCs, corresponding to the two default GPOs: **Default Domain Policy** and **Default Domain Controller Policy**
- Each GPC contains two subcontainers—one for machine **(computer) configuration** information and another for **user configuration** information

View the Group Policy Container



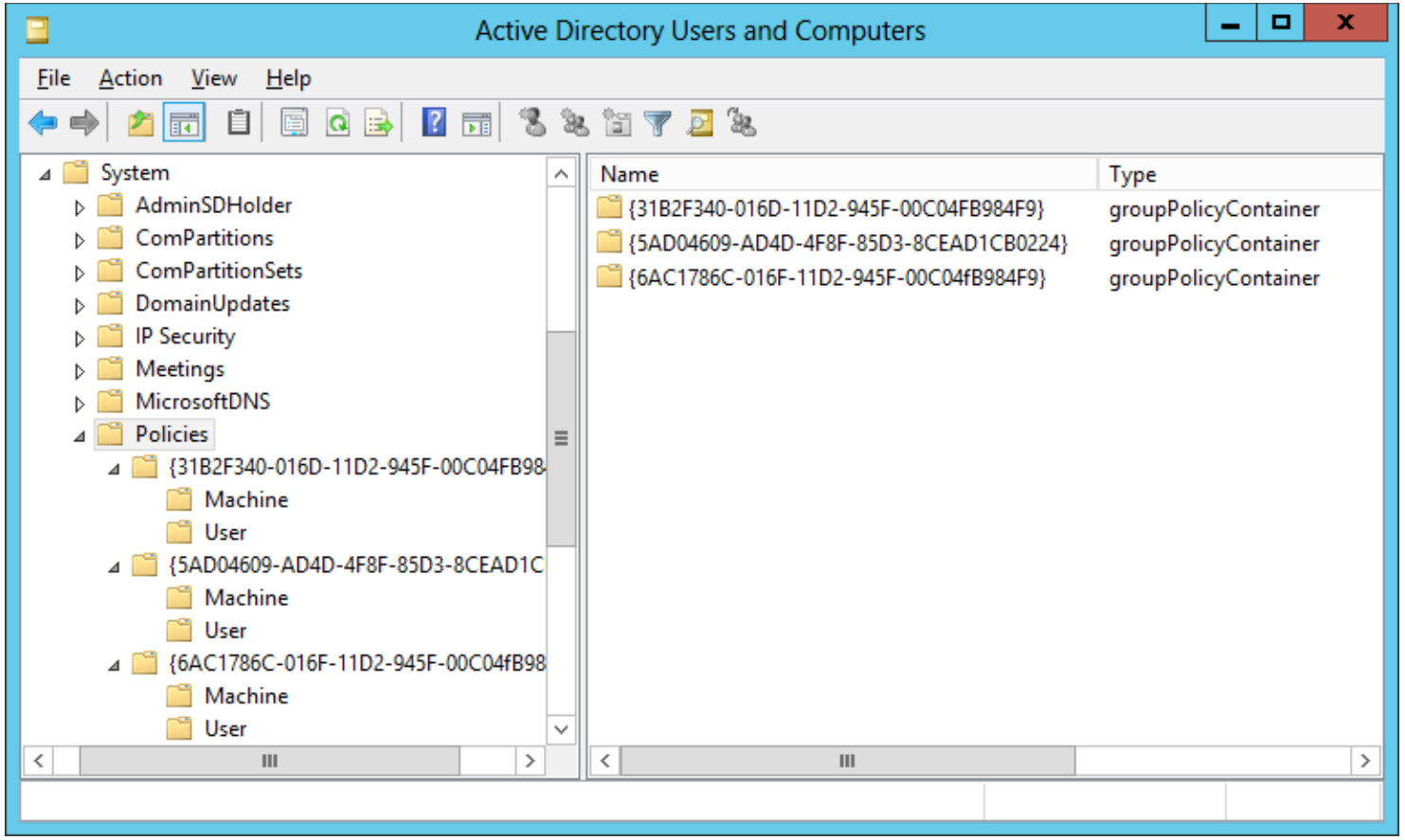
Tree view in Active Directory Administrative Center

View the Group Policy Container



Contents of the Policies folder in Active Directory Administrative Center

View the Group Policy Container



Group Policy Containers in Active Directory Users and Computers

Viewing Group Policy Templates

- The **Group Policy Templates (GPT)** is a folder structure that is located in the shared SYSVOL folder on a domain controller.
- Contains the default settings for a new GPO.
- The path to the default GPT structure for a domain is:
  %systemroot%\SYSVOL\sysvol\<*domain name*>\Policies

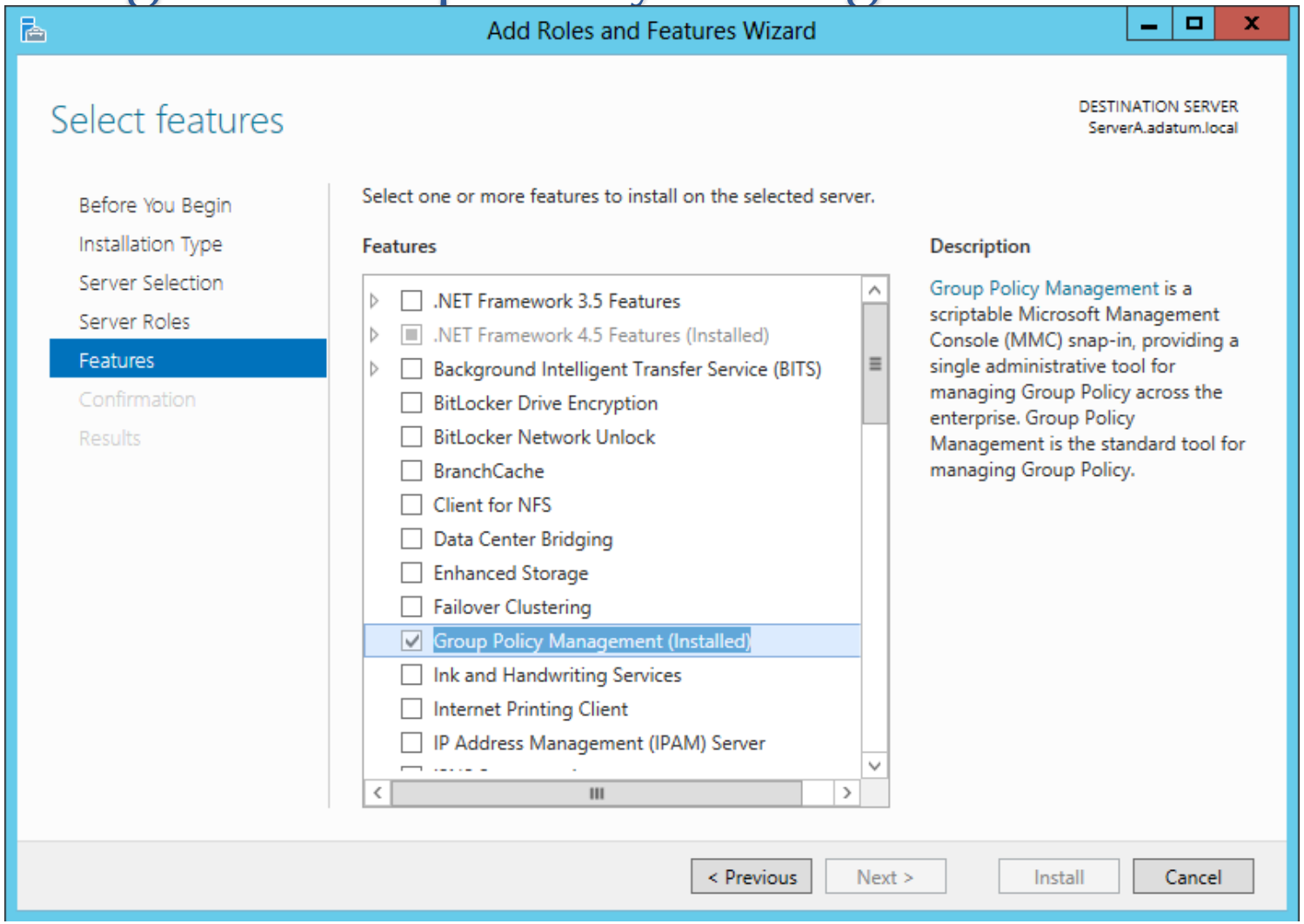
Configuring a Central Store

- A **Central Store** is a centralized copy of the Administrative Templates (ADMX files).
- Having these files centrally stored and accessible means that they don't have to be replicated to the SYSVOL volumes on the domain controllers.
- Prevents maintaining multiple copies of the same data.

Using the Group Policy Management Console

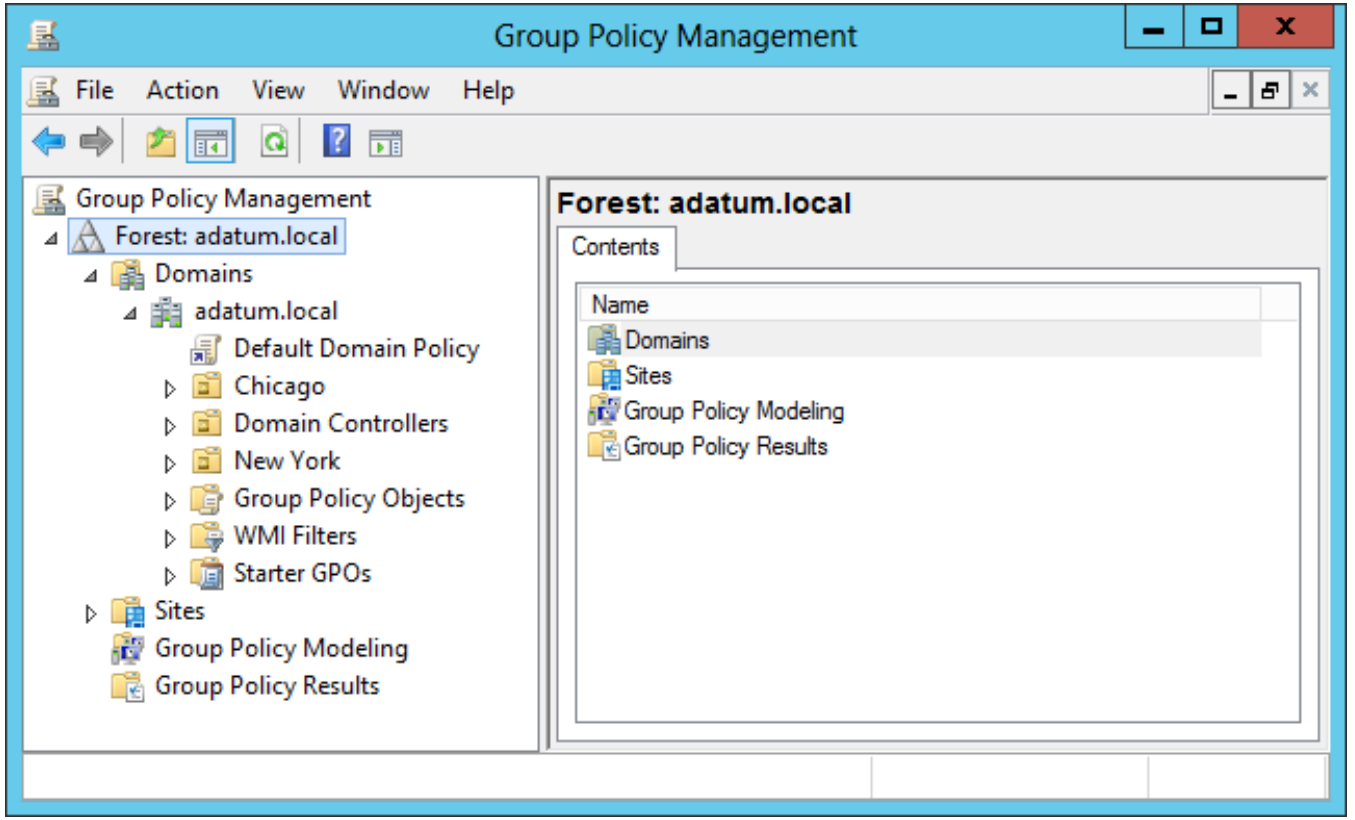
- The **Group Policy Management Console** is the Microsoft Management Console (MMC) snap-in that administrators use to create Group Policy objects and manage their deployment to Active Directory Domain Services objects.
- The **Group Policy Management Editor** is a separate snap-in that opens GPOs and enables you to modify their settings.

Using the Group Policy Management Console



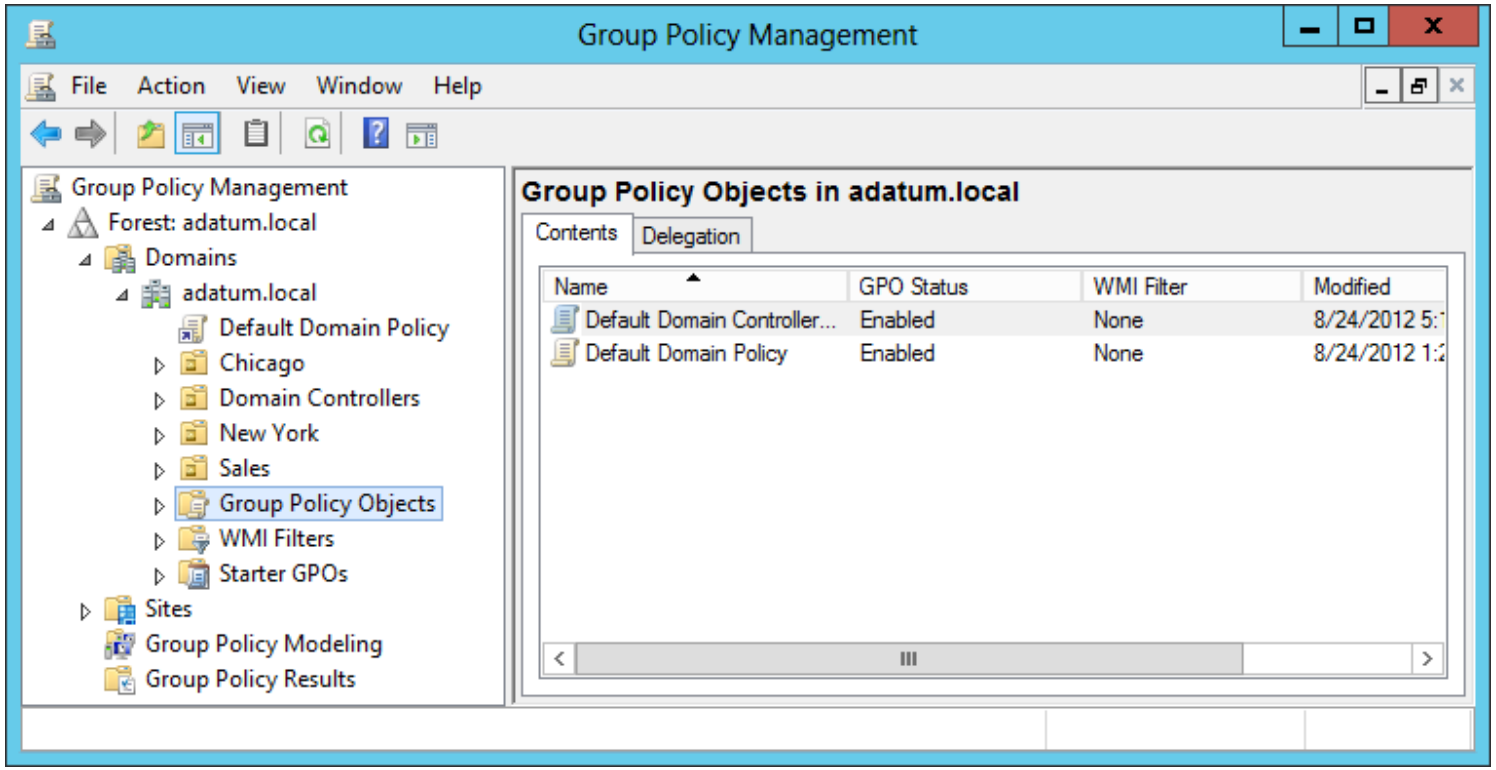
Wizard

Creating and Linking Nonlocal GPOs



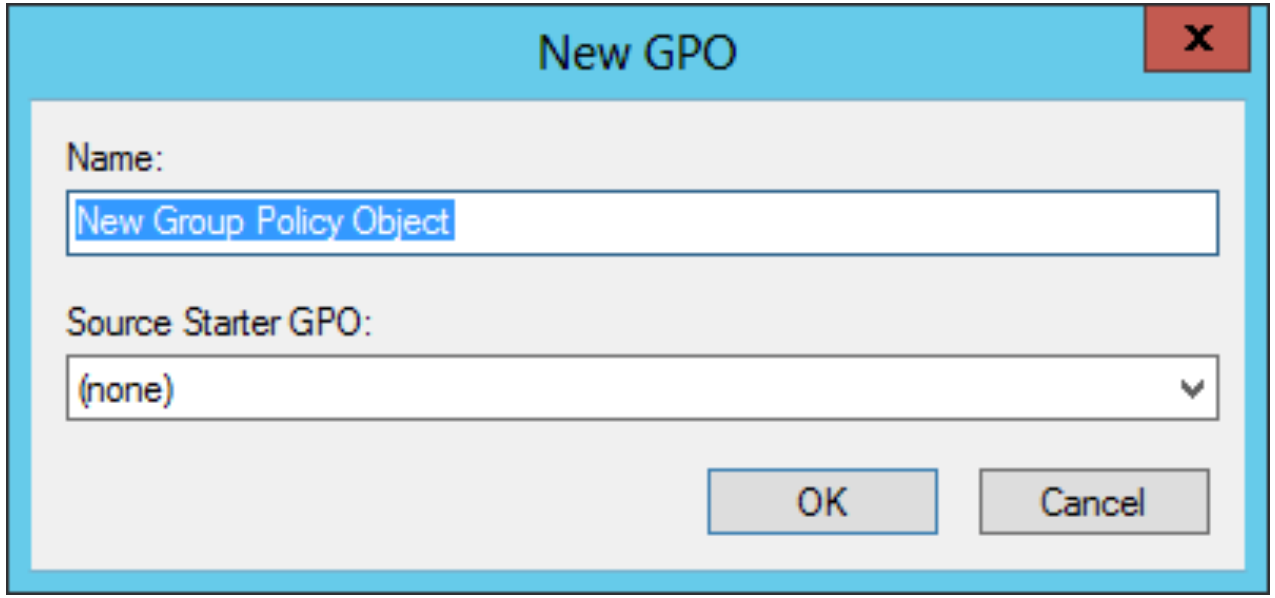
The Group Policy Management console

Creating and Linking Nonlocal GPOs



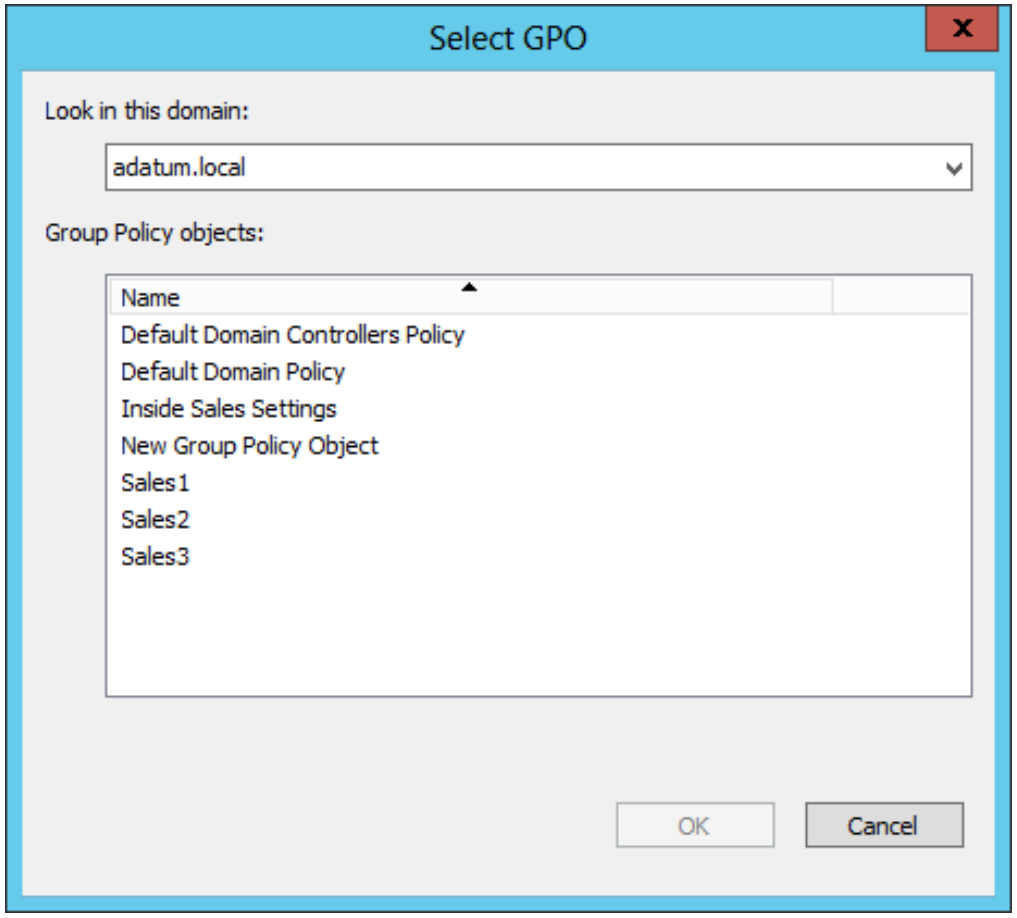
Contents of the Group Policy Objects folder

Creating and Linking Nonlocal GPOs



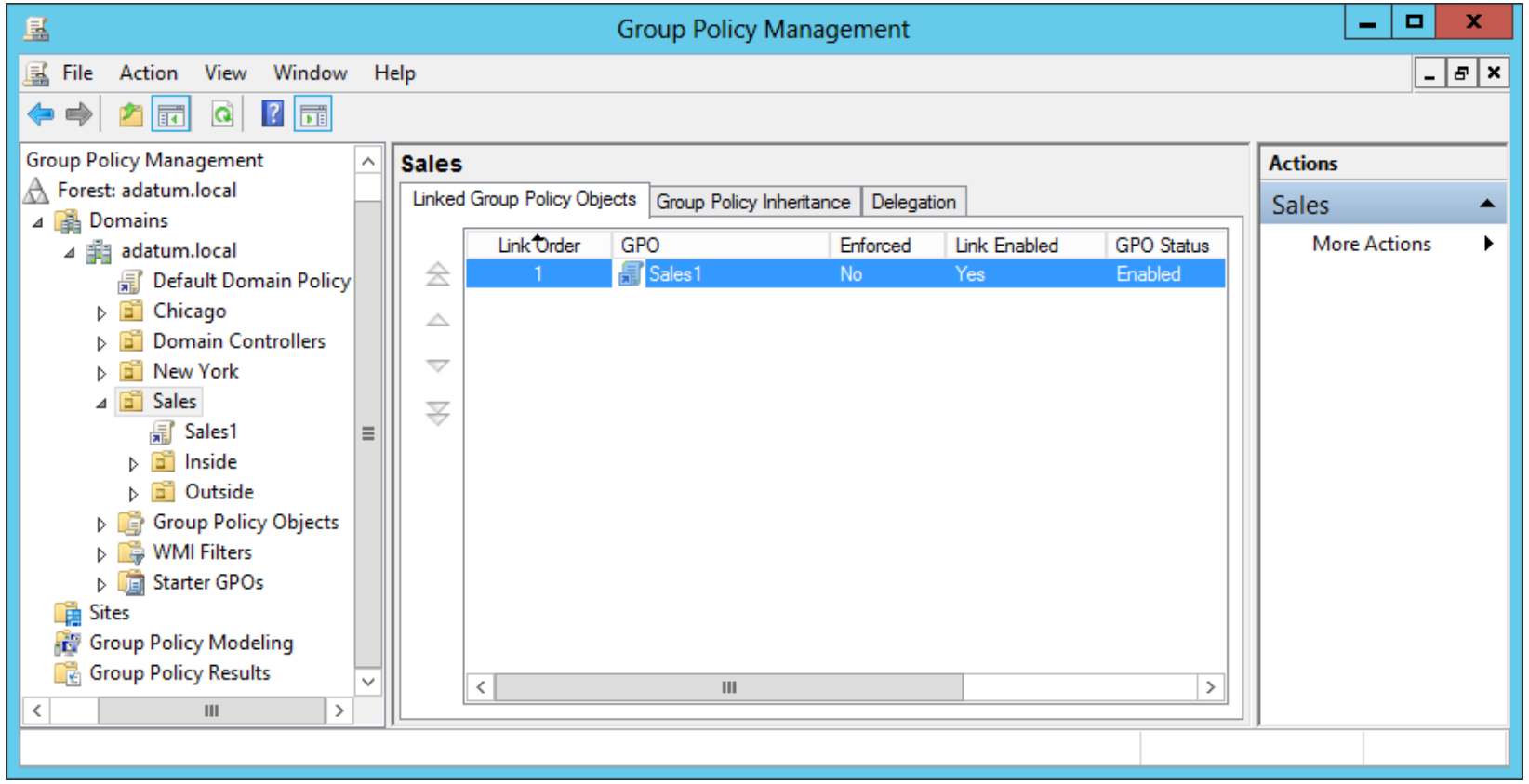
The New GPO dialog box

Creating and Linking Nonlocal GPOs



The Select GPO dialog box

Creating and Linking Nonlocal GPOs

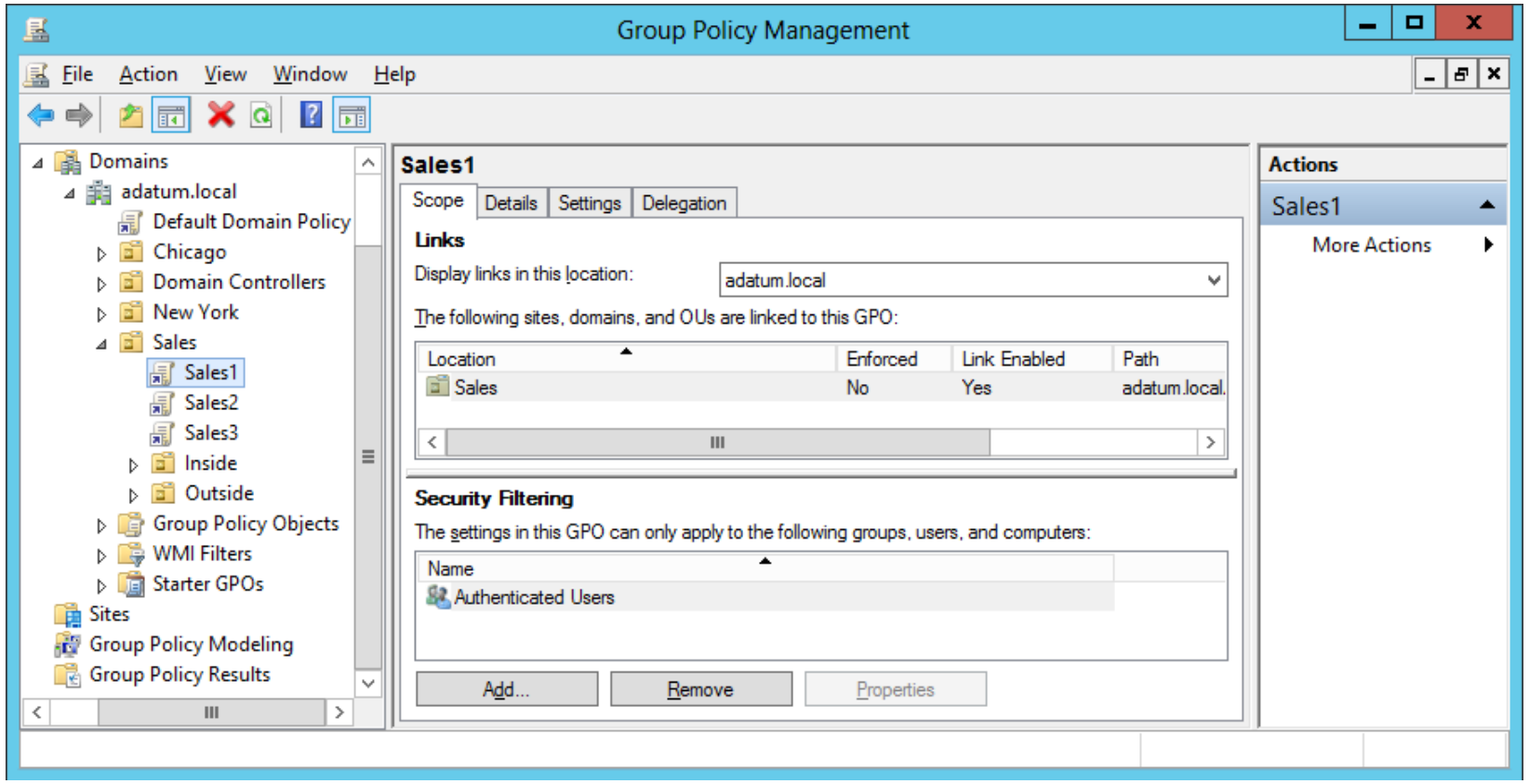


The Linked Group Policy Objects tab

Using Security Filtering

- Linking a GPO to a container causes all the users and computers in that container to receive the GPO settings, by default.
- **Security filtering** is a technique you use to modify the default permission assignments so that only certain users and computers receive the permissions for the GPO.

Using Security Filtering

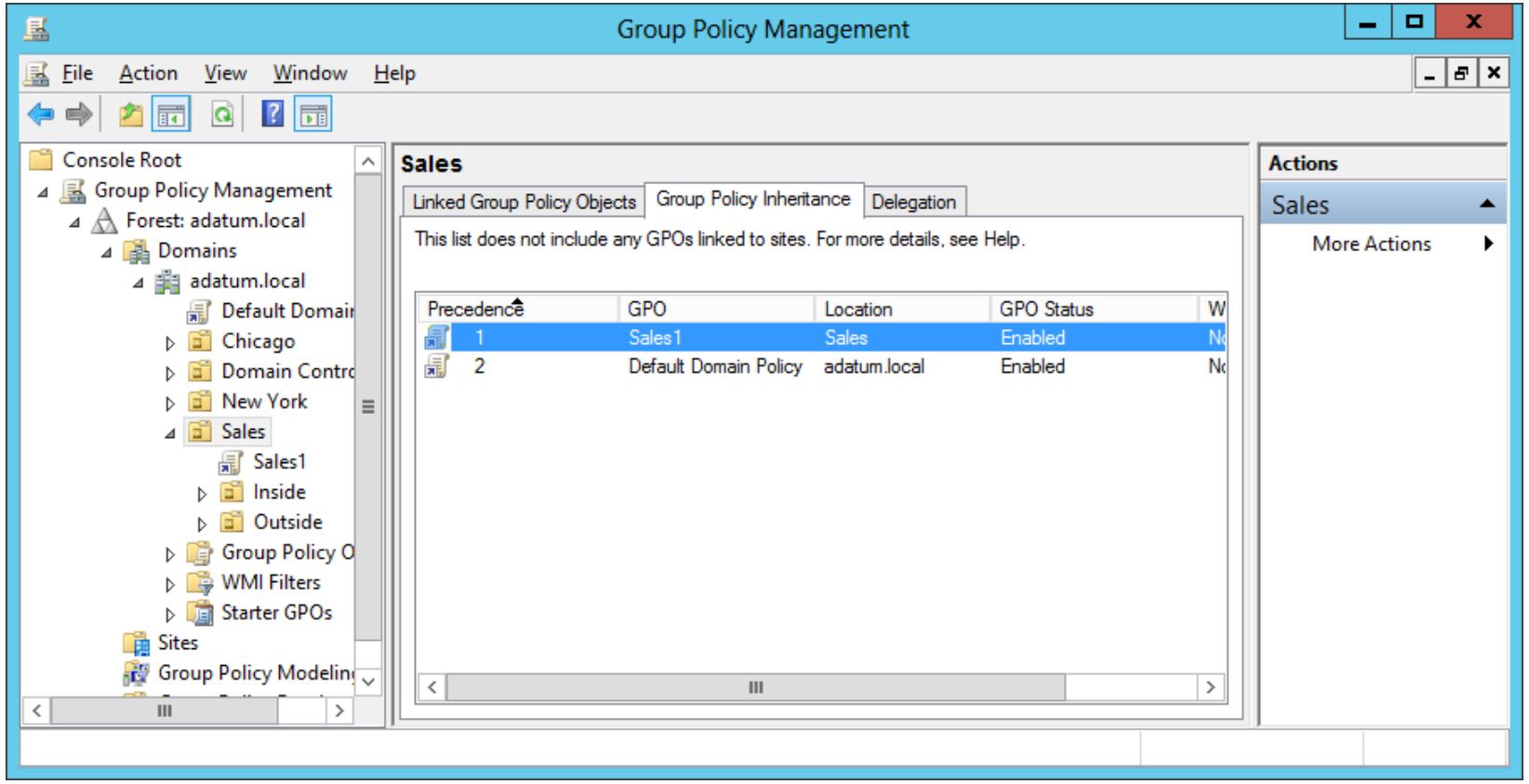


Security filtering in the Group Policy Management console

Group Policy Processing

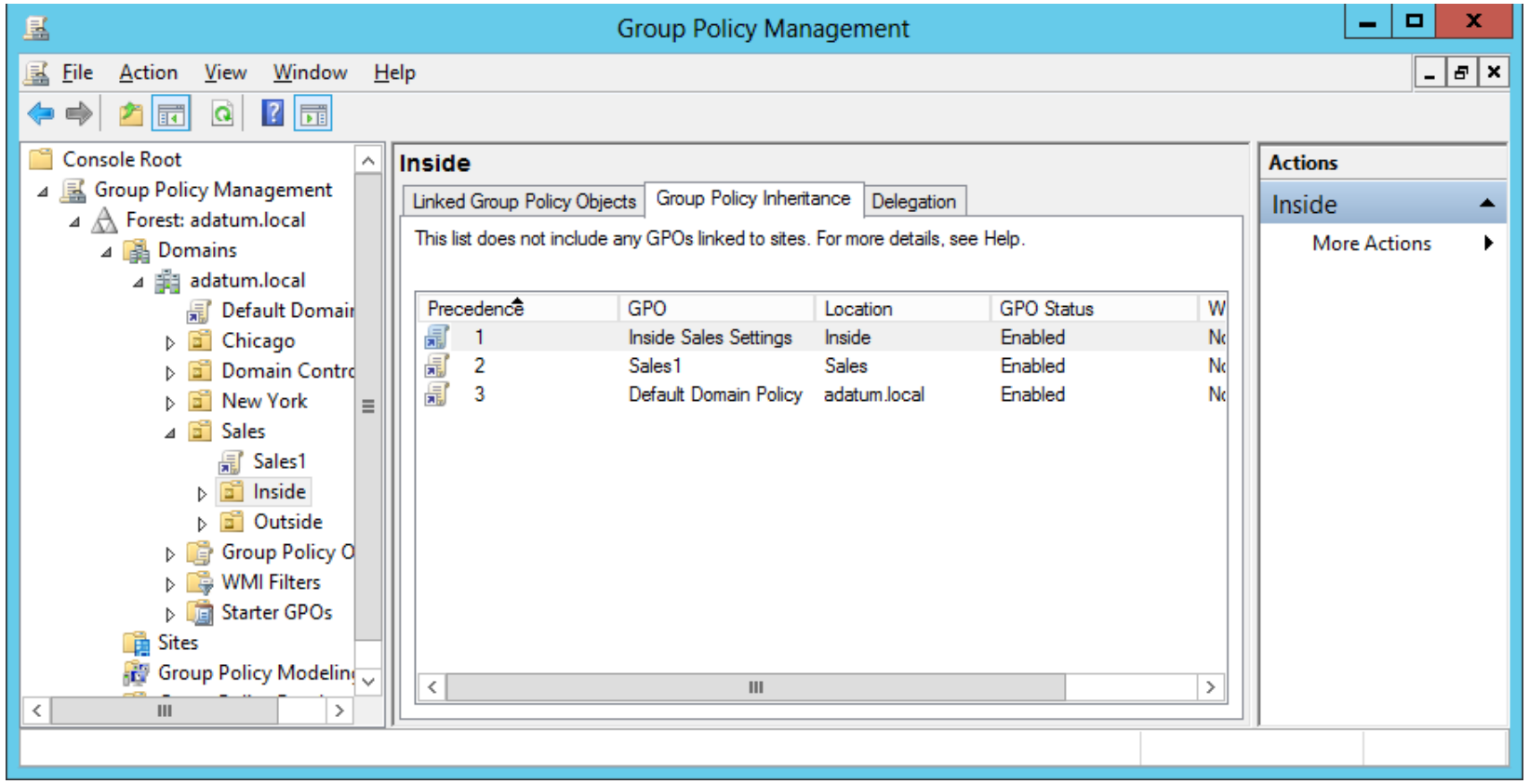
- You can have local policies, site policies, domain policies, and OU policies within your domain structure.
- Windows systems receiving GPOs from multiple sources process them in the following order, typically referred to as **LSDOU**:
  1. Local policies
  2. Site policies
  3. Domain policies
  4. OU policies

Group Policy Processing



The Group Policy Inheritance tab, showing OU and domain inheritance

Group Policy Processing

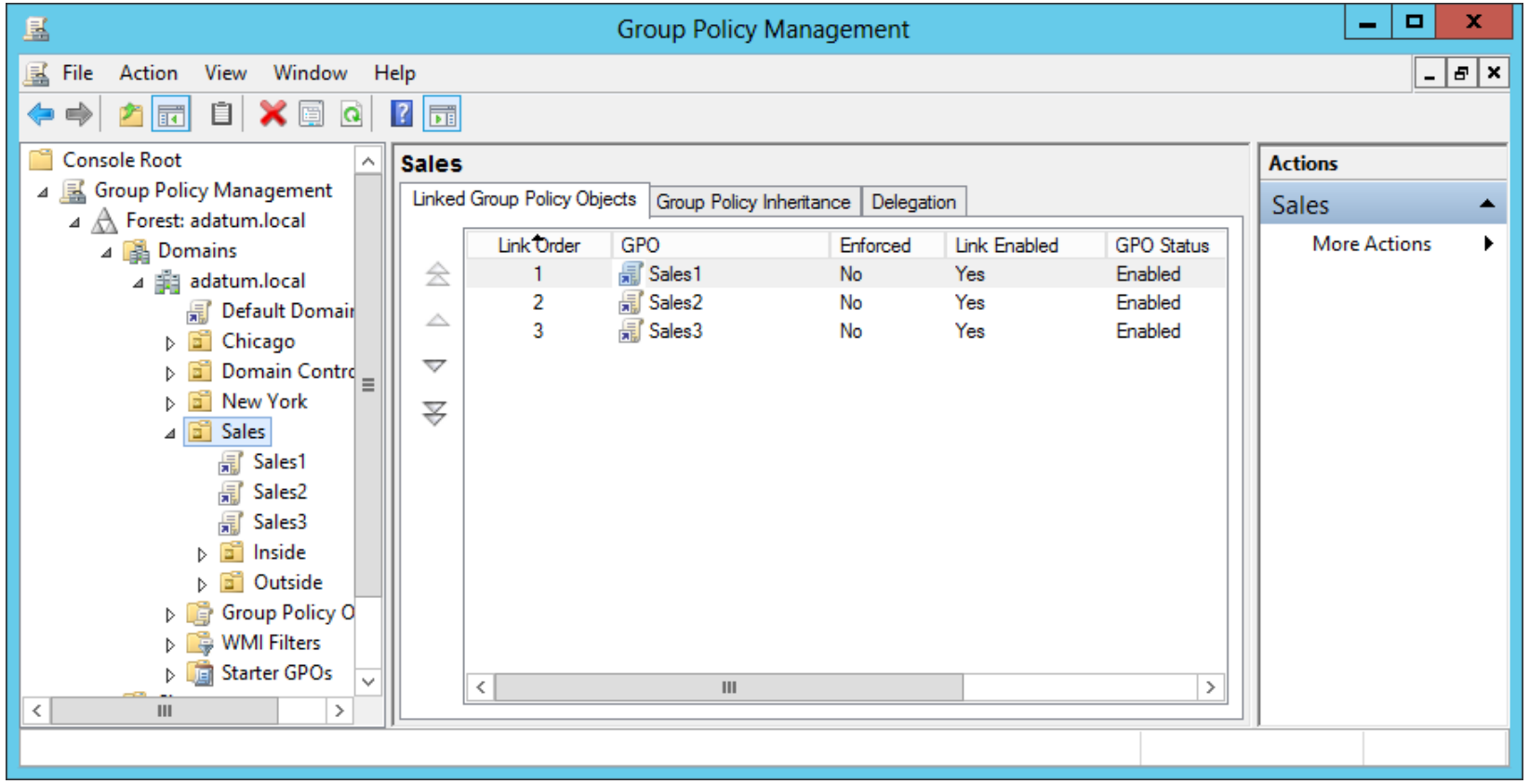


The Group Policy Inheritance tab, showing two layers of OU inheritance, plus domain inheritance

Processing Multiple GPOs

- You can link multiple GPOs to domains, sites, and OUs.
- Many administrators prefer to create individual GPOs for each system configuration task, rather than create one large GPO.
- When multiple GPOs linked to a single AD DS object, you can control the order in which systems apply the GPO settings by using the Linked Group Policy Objects tab in the Group Policy Management console.

Processing Multiple GPOs



The Linked Group Policy Objects tab, with multiple GPOs linked to a single OU

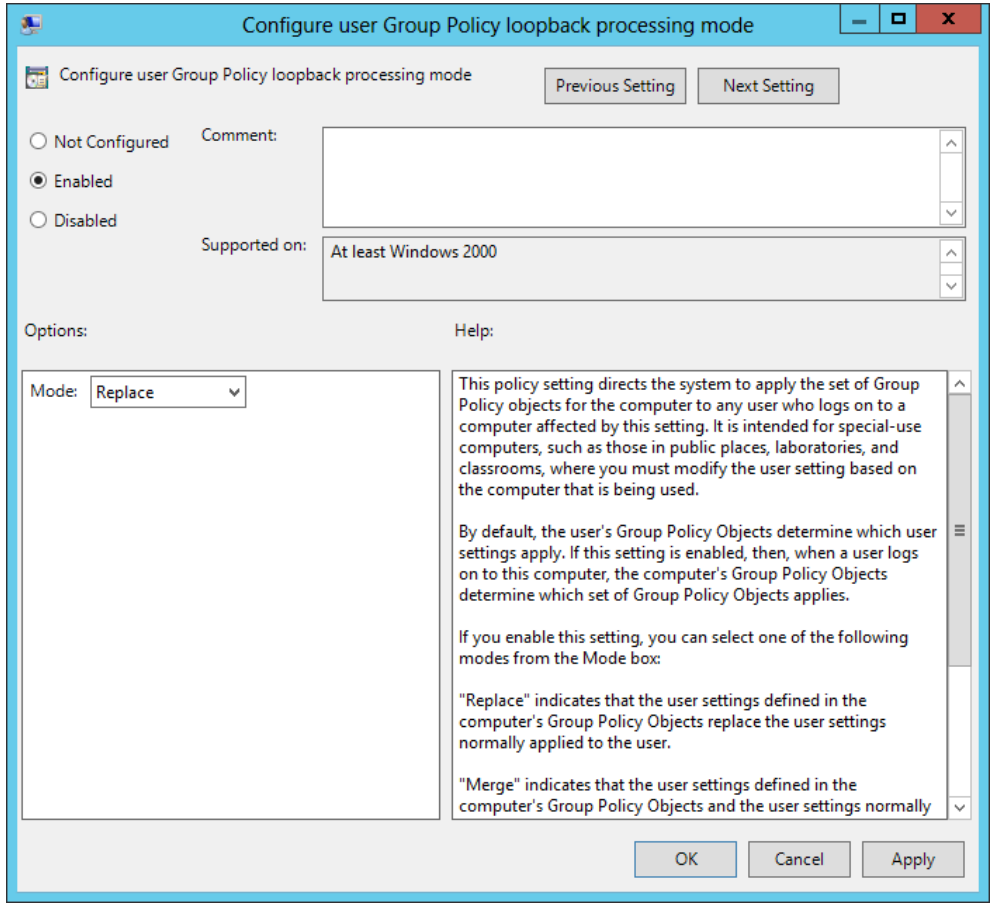
GPO Settings Application

- Windows systems process Computer Configuration settings when the computer starts, along with the computer startup scripts.
- The system processes the User Configuration settings and user logon scripts when a user logs on.
- User logoff scripts and computer shutdown scripts run during the shutdown process.

Configuring Exceptions to GPO Processing

- The **Enforce** setting on an individual GPO link forces a particular GPO's settings to flow down through the AD DS hierarchy, without being blocked by any child OUs.
- The **Block Policy Inheritance** setting on a container object such as a site, domain, or OU blocks all policies from parent containers from flowing to this container.
- **Loopback Processing** is a Group Policy option that provides an alternative method of obtaining the ordered list of GPOs to be processed for the user. When set to Enabled, this setting has two options: merge and replace.

Exceptions to GPO Processing

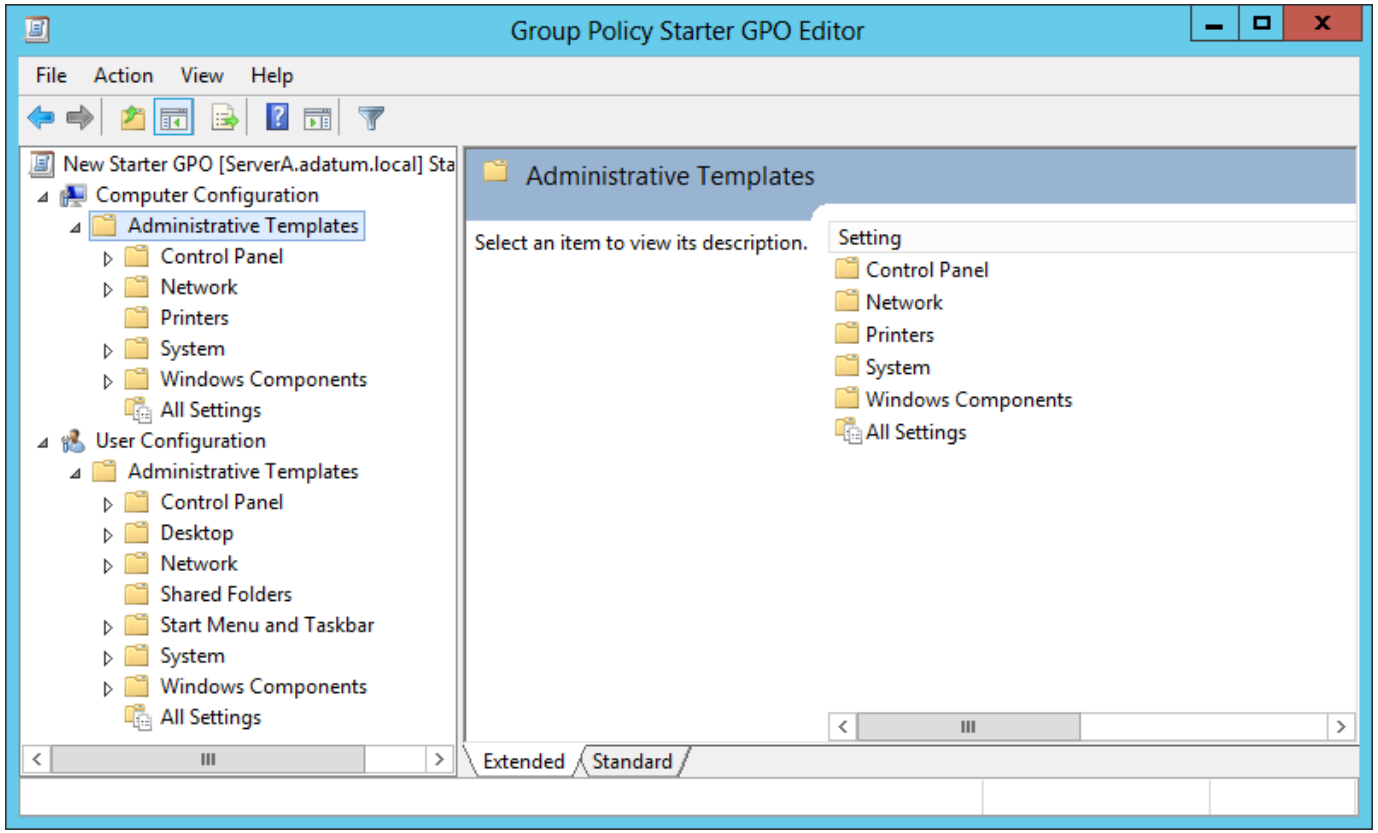


The Configure User Group Policy Loopback Processing Mode policy

Managing Starter GPOs

- **Starter GPOs** are templates that you can use to create multiple GPOs with the same set of baseline Administrative Templates settings
- You create and edit starter GPOs just as you would any other Group Policy object.

Managing Starter GPOs



A starter GPO in the Group Policy Management Editor

Configuring Group Policy Settings

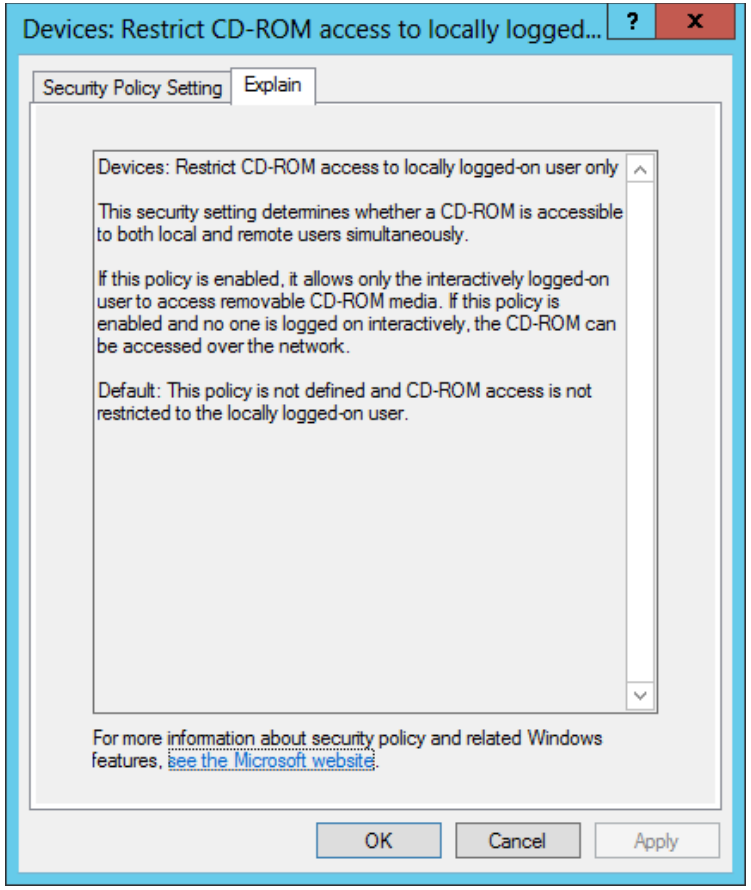
- Group Policy settings enable you to customize the configuration of a user's desktop, environment, and security settings.
- Settings are divided into two subcategories: Computer Configuration and User Configuration.
- Subcategories are referred to as Group Policy nodes.
- A node is a parent structure that holds all related settings specific to computer configurations and user configurations.

Configuring Group Policy Settings

Within the Computer Configuration and User Configuration nodes, the subnodes are as follows:

- Software Settings
- Windows Settings
- Administrative Templates

Policy Explanations



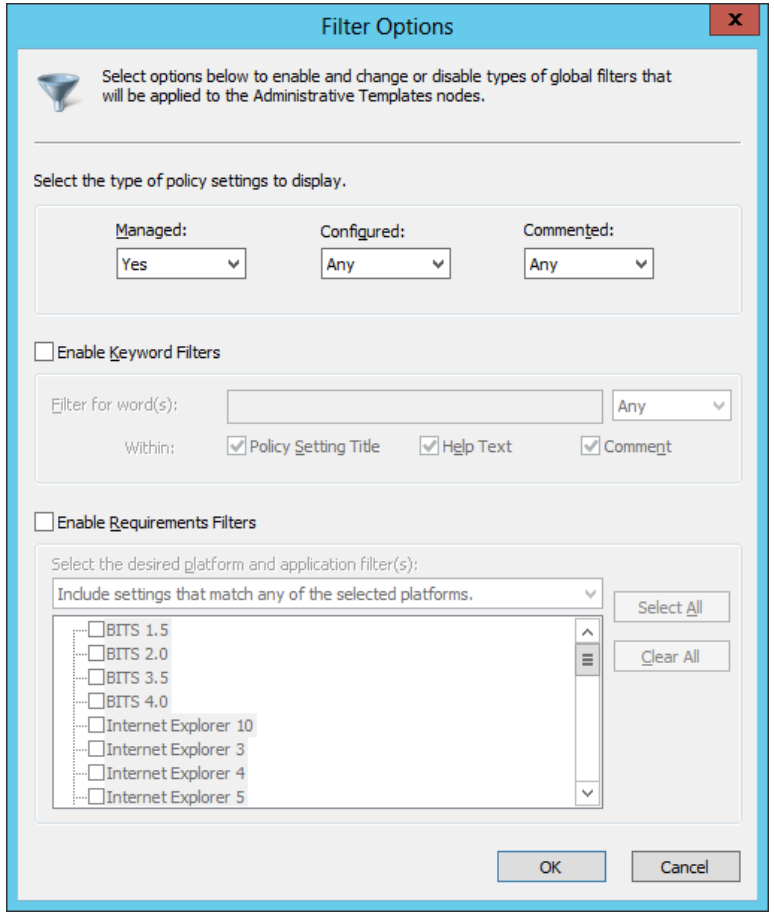
Explanations of Group Policy settings

Policy States

To work with Administrative Template settings, you must understand the three different states of each policy setting:

- **Not Configured**: No modification to the registry from its default state occurs as a result of the policy. Not Configured is the default setting for the majority of GPO settings. When a system processes a GPO with a Not Configured setting, the registry key affected by the setting is not modified or overwritten, no matter what its current value might be.
- **Enabled**: The policy function is explicitly activated in the registry, whatever its previous state.
- **Disabled**: The policy function is explicitly deactivated in the registry, whatever its previous state.

Searching Policies



The Filter Options dialog box

Creating Multiple Local GPOs

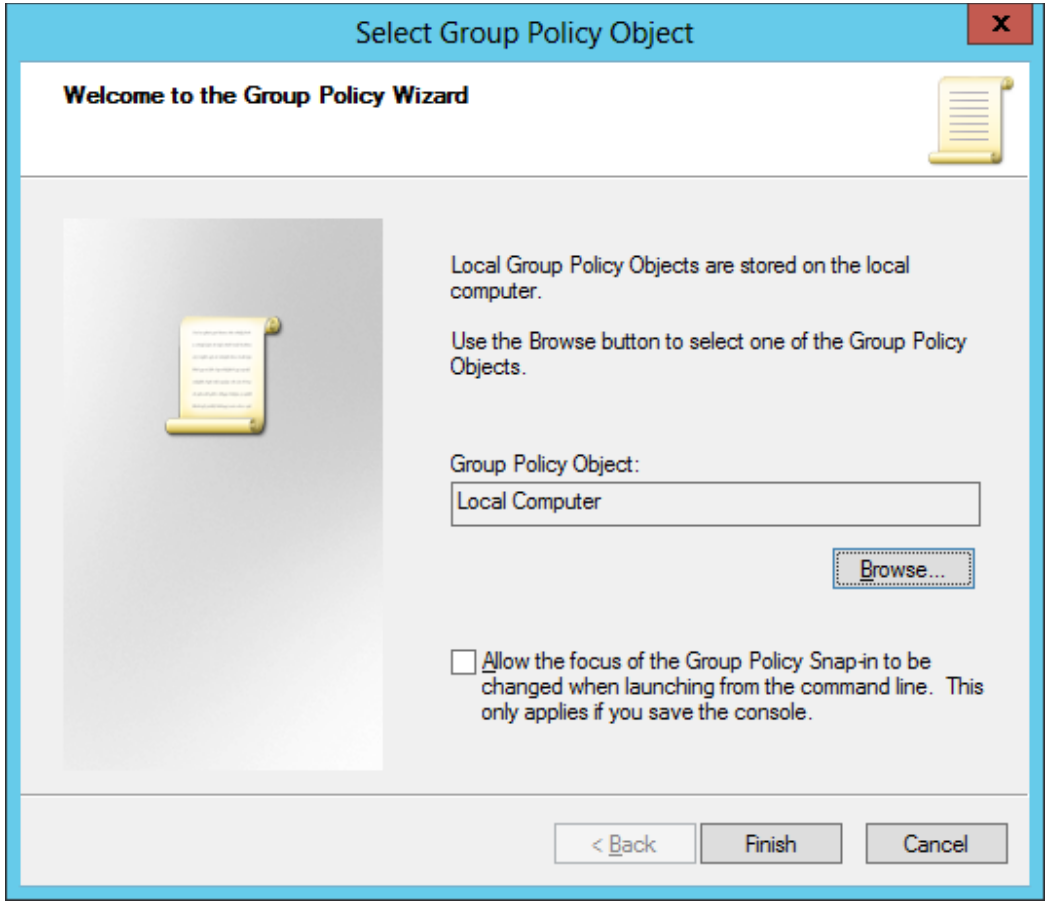
- Computers that are members of an AD DS domain benefit from a great deal of flexibility when it comes to Group Policy configuration.
- Standalone (non-AD DS) systems can achieve some of that flexibility, as long as they are running at least Windows Vista or Windows Server 2008 R2. These operating systems enable administrators to create multiple local GPOs that provide different settings for users, based on their identities.

Creating Multiple Local GPOs

Windows systems supporting multiple local GPOs have three layers of Group Policy support:

- **Local Group Policy**: Consists of both Computer and User settings and applies to all system users, administrative or not. This is the only local GPO that includes computer settings, so to apply Computer Configuration policies, you must use this GPO.
- **Administrators and Non-administrators Group Policy:** Consists of two GPOs, one of which applies to members of the local Administrators group and one that applies to all users that are not members of the local Administrators group.
- **User-specific Group Policy:** Consists of GPOs that apply to specific local user accounts created on the computer. These GPOs can apply to individual users only, not to local groups.

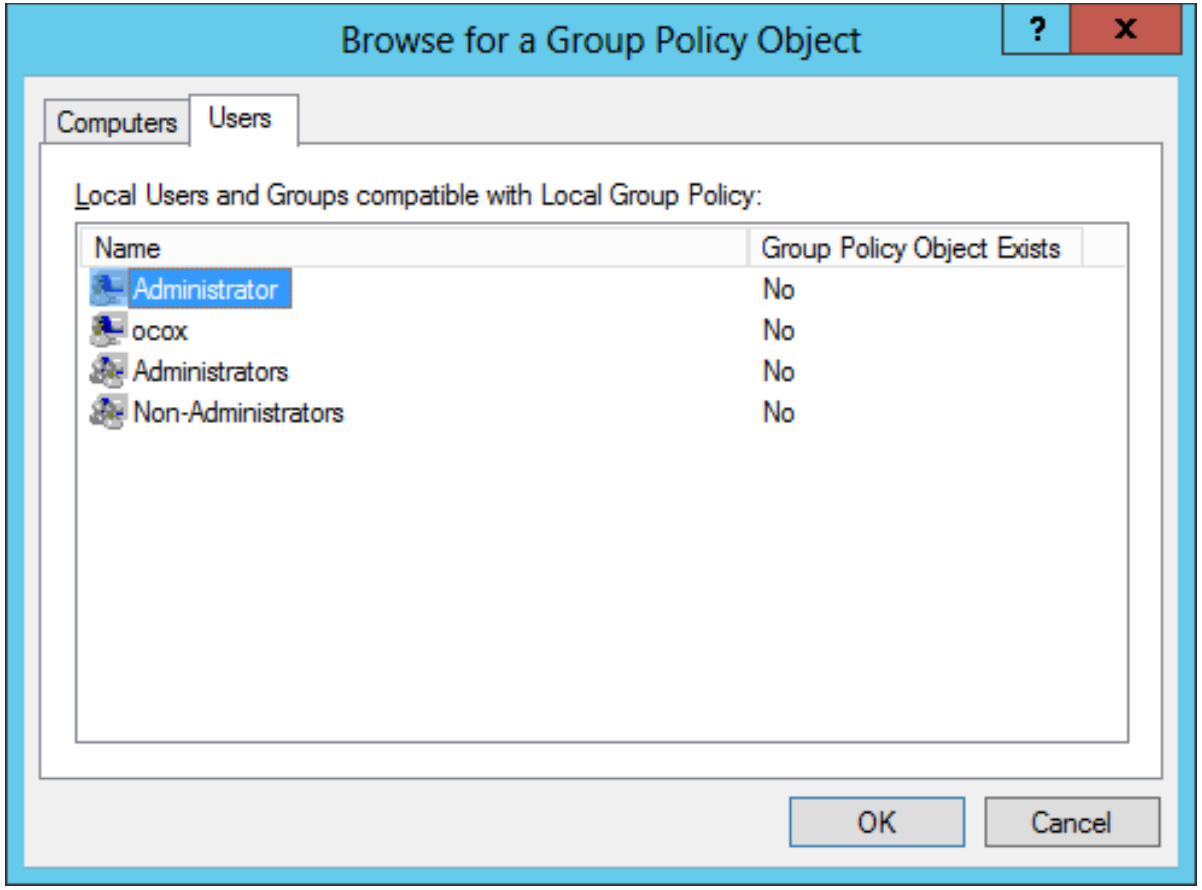
Create Local GPOs



The Select Group Policy Object page

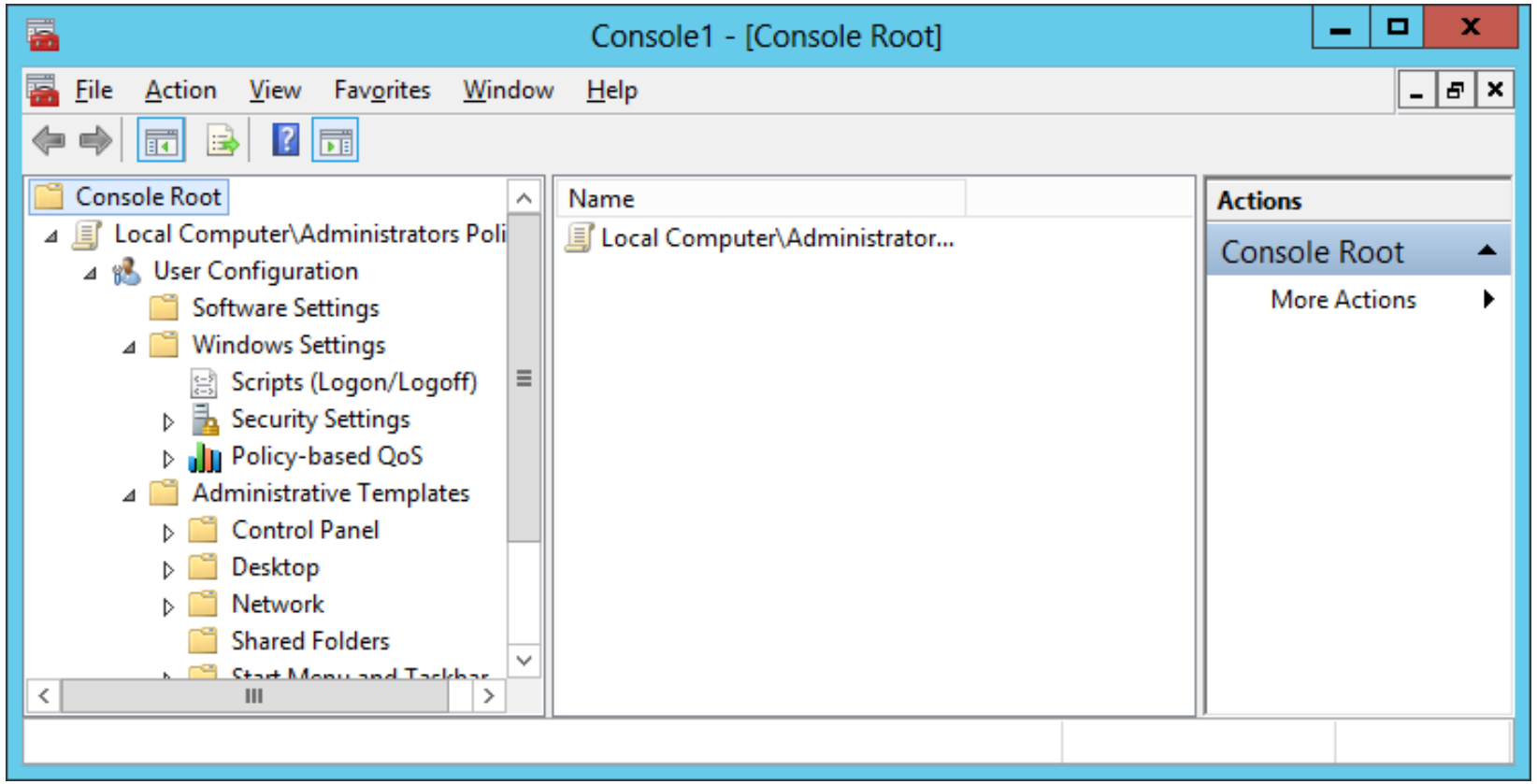
.

Create Local GPOs



The Users tab of the Browse for a Group Policy Object dialog box

Create Local GPOs



A Group Policy Object Editor console