Hunan University of Arts and Science

# Networking Theory & Applications

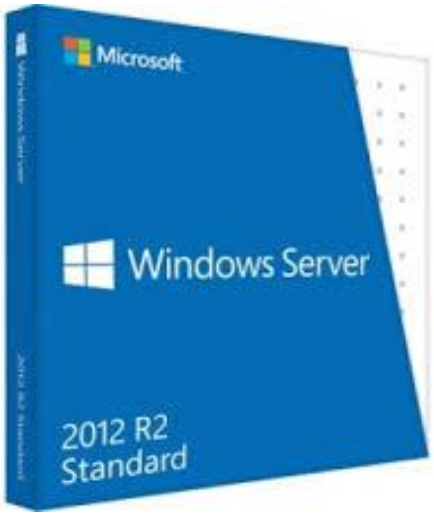
CIS 291

2018 – 2019

# Windows Server® 2012

## Part 3

# Chapter 6
# Creating and managing Group Policy
# 創建和管理組策略 (GPOs)




## Objectives in this chapter: 本章的目标

1- Create Group Policy Objects (GPOs)

2- Configure security policies

3- Configure application restriction policies

4- Configure Windows Firewall

# Objective 6.3: Configure Application Restriction Policies

- The options in the Software Restriction Policies node provide organizations greater control in preventing potentially dangerous applications from running.
- Software restriction policies are designed to identify software and control its execution. In addition, administrators can control who will be affected by the policies.

# 1- Using software restriction policies

- The Software Restriction Policies node is found in the Windows Settings\Security Settings node of the User Configuration or the Computer Configuration node of a GPO.
- By default, the Software Restriction Policies folder is empty. When you create a new policy, two subfolders appear: Security Levels and Additional Rules.
- In the following sections, you learn how to set the security level for a software restriction policy and how to define rules that will govern the execution of program files.

# A- Enforcing restrictions

- If a policy does not perform restrictions, executable files run based on the permissions that users or groups have in the NTFS file system.
- When considering the use of software restriction policies, you must determine your approach to enforcing restrictions.
- There are three basic strategies for doing restrictions:
  1. **Unrestricted** This approach enables all applications to run
  2. **Disallowed** This approach prevents all applications from running
  3. **Basic User** This approach prevents any applications from running that require administrative rights, but enables programs to run that only require resources that are accessible by normal users.
- By default, the Software Restriction Policies area has an Unrestricted value in the Default Security Level setting.
- For example, you might want to enable only specified applications to run in a high-security environment. In this case, you would set the Default Security Level to Disallowed.
- To modify the Default Security Level setting to Disallowed, use the following procedure. Lab practice …..

# B- Configuring software restriction rules

- When you create a new software restriction policy, the Additional Rules subfolder appears. This folder enables you to create rules that specify the conditions under which programs can be executed or denied.

---

- These rules can override the Default Security Level setting when necessary.
- You create new rules of your own in the Additional Rules folder using a dialog box like the one shown in Figure 6-15.
  - There are four types of software restriction rules:
    - Hash rules
    - Certificate rules
    - Path rules
    - Network zone rules
  - There is also a fifth type of rule—the default rule—that applies when an application does not match any of the other rules you have created.
  - To configure the default rule, select one of the policies in the Security Levels folder and, on its Properties sheet, click Set As Default.

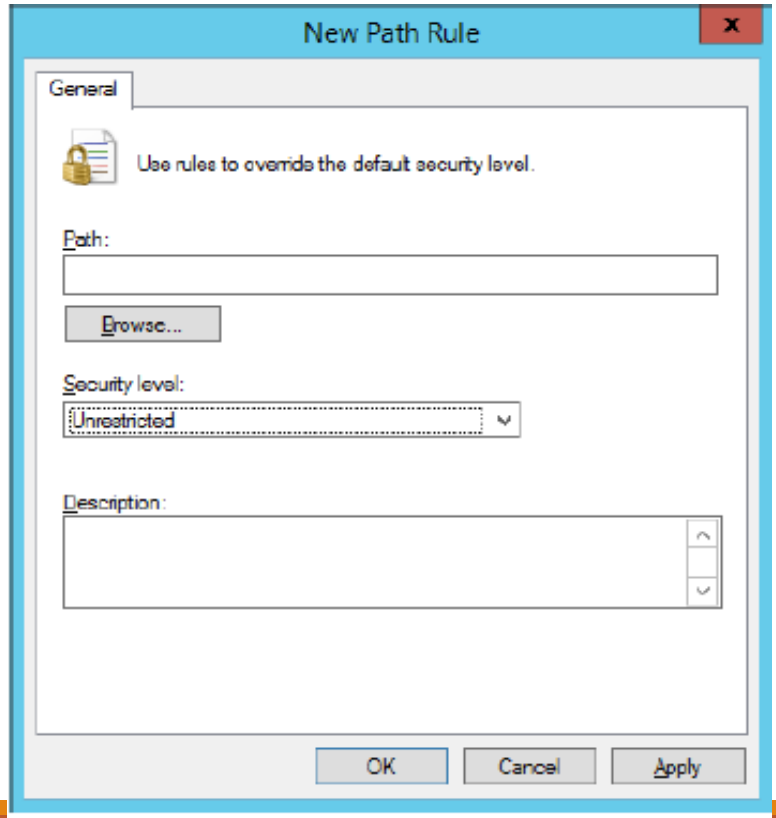



**FIGURE 6-15** The New Path Rule dialog box

## HASH RULES

If you create a hash rule and a user attempts to run a program affected by the rule, the system checks the hash value of the executable file and compares it with the hash value stored in the software restriction policy. If the two match, the policy settings will apply. Therefore, creating a hash rule for an application executable prevents the application from running if the hash value is not correct.

## CERTIFICATE RULES

A certificate rule uses the digital certificate associated with an application to confirm its legitimacy. You can use certificate rules to enable software from a trusted source to run or to prevent software that does not come from a trusted source from running.

## PATH RULES

A path rule identifies software by specifying the directory path where the application is stored in the file system. Path rules can specify either a location in the file system where application files are located or a registry path setting.

## NETWORK ZONE RULES

Network zone rules apply only to Windows Installer packages that attempt to install from a specified zone, such as a local computer, a local intranet, trusted sites, restricted sites, or the Internet. You can configure this type of rule to enable Windows Installer packages to be installed only if they come from a trusted area of the network.

# C- Using multiple rules

- You can define a software restriction policy by using multiple rule types to allow and disallow program execution.
- For example, you might want to specify a path rule that prevents programs from running from the \\Server1\Accounting shared folder and a path rule that enables programs to run from the \\Server1\Application shared folder.
- You can also choose to incorporate certificate rules and hash rules into your policy.
- systems apply the rules in the same order of precedence as mentioned before in slide 7
- When a conflict occurs between rule types, such as between a hash rule and a path rule, the hash rule prevails because it is higher in the order of preference.

# Break

# 2- Configuring software restriction properties

- Within the Software Restriction Policies folder, you can configure three specific properties to provide additional settings that apply to all policies when implemented.
- These three properties are:
  - Enforcement
  - Designated file types
  - Trusted publishers

# A- ENFORCEMENT PROPERTIES

- The Enforcement properties enable you to determine whether the policies apply to all files or whether library files, such as dynamic link library (DLL) files, are excluded.
- Excluding DLLs is the default. This is the most practical method of enforcement.
- For example, if the Default Security Level for the policy is set to Disallowed and the Enforcement properties are set to All Software Files, you would have to create a rule that checked every DLL before the program could be allowed or denied.
- By contrast, excluding DLL files by using the default Enforcement property does not require an administrator to define individual rules for each DLL file.

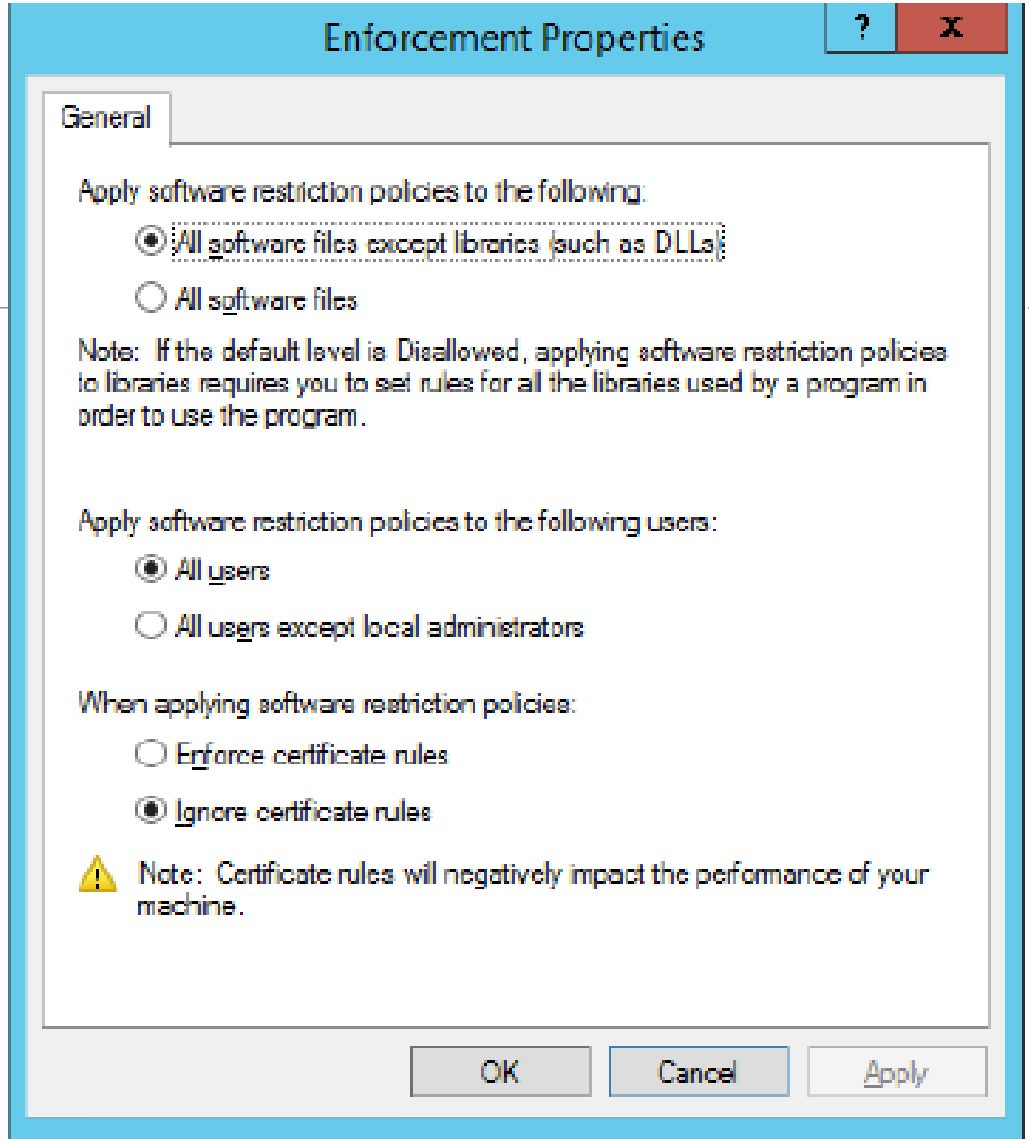



**FIGURE 6-16** Configuring Enforcement properties

# B- DESIGNATED FILE TYPES PROPERTIES

- The Designated File Types properties within the Software Restriction Policies folder, specify file types that are considered executable.

- File types that are designated as executable or program files are shared by all rules, although you can specify a list for a computer policy that is different from one that is specified for a user policy.

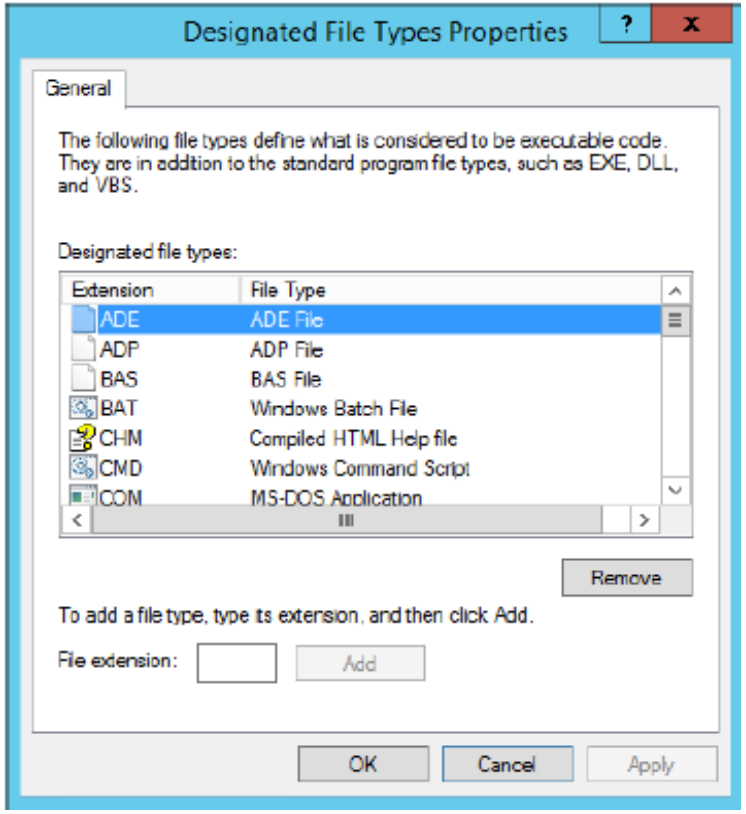



FIGURE 6-17 Configuring Designated File Types properties

# C-TRUSTED PUBLISHERS PROPERTIES

- Trusted Publishers properties enable an administrator to control how systems handle certificate rules. In the Properties dialog box for Trusted Publishers, shown in Figure 6-18, the first setting enables you to specify which users are permitted to manage trusted certificate sources.
- By default, local computer administrators have the right to specify trusted publishers on the local computer and enterprise administrators have the right to specify trusted publishers in an OU.
- From a security standpoint, in a high-security network, users should not be allowed to determine the sources from which certificates can be obtained.
- The Trusted Publisher Properties sheet also lets you decide if you wish to verify that a certificate has not been revoked.

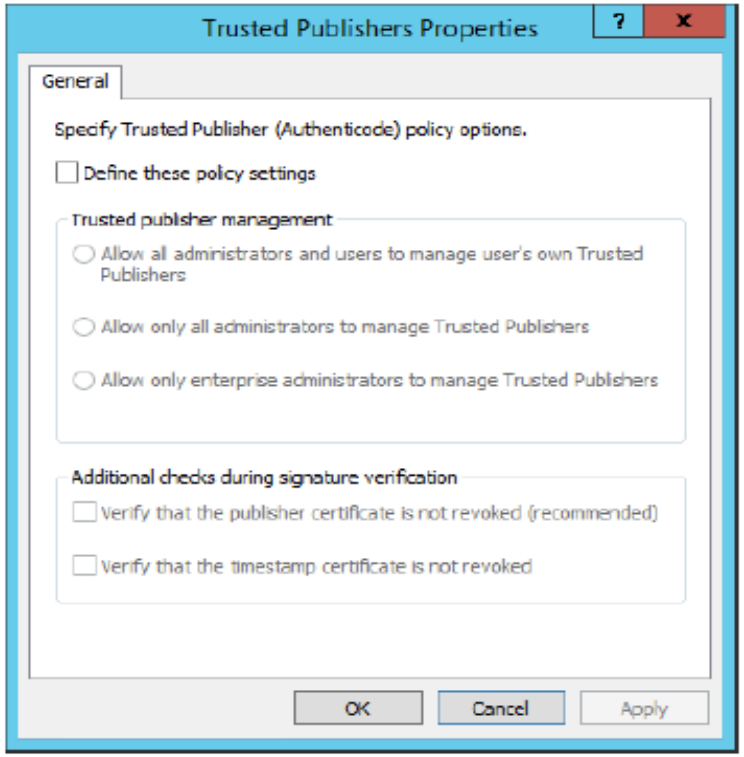



**FIGURE 6-18** Configuring Trusted Publishers properti

# 3- AppLocker

- **AppLocker**, also known as **application control policies**, is a Windows feature that is an updated version of the concept implemented in software restriction policies.
- Uses rules, which you must manage, using a wizard-based interface.
- More flexible than software restriction policies
- You can apply AppLocker rules to specific users and groups and also create rules that support all future versions of an application.
- The primary disadvantage of AppLocker is that you can apply the policies only to computers running Windows 7 and Windows Server 2008 R2 or later.
- The AppLocker settings are located in GPOs in the Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker container, as shown in Figure 6-19.

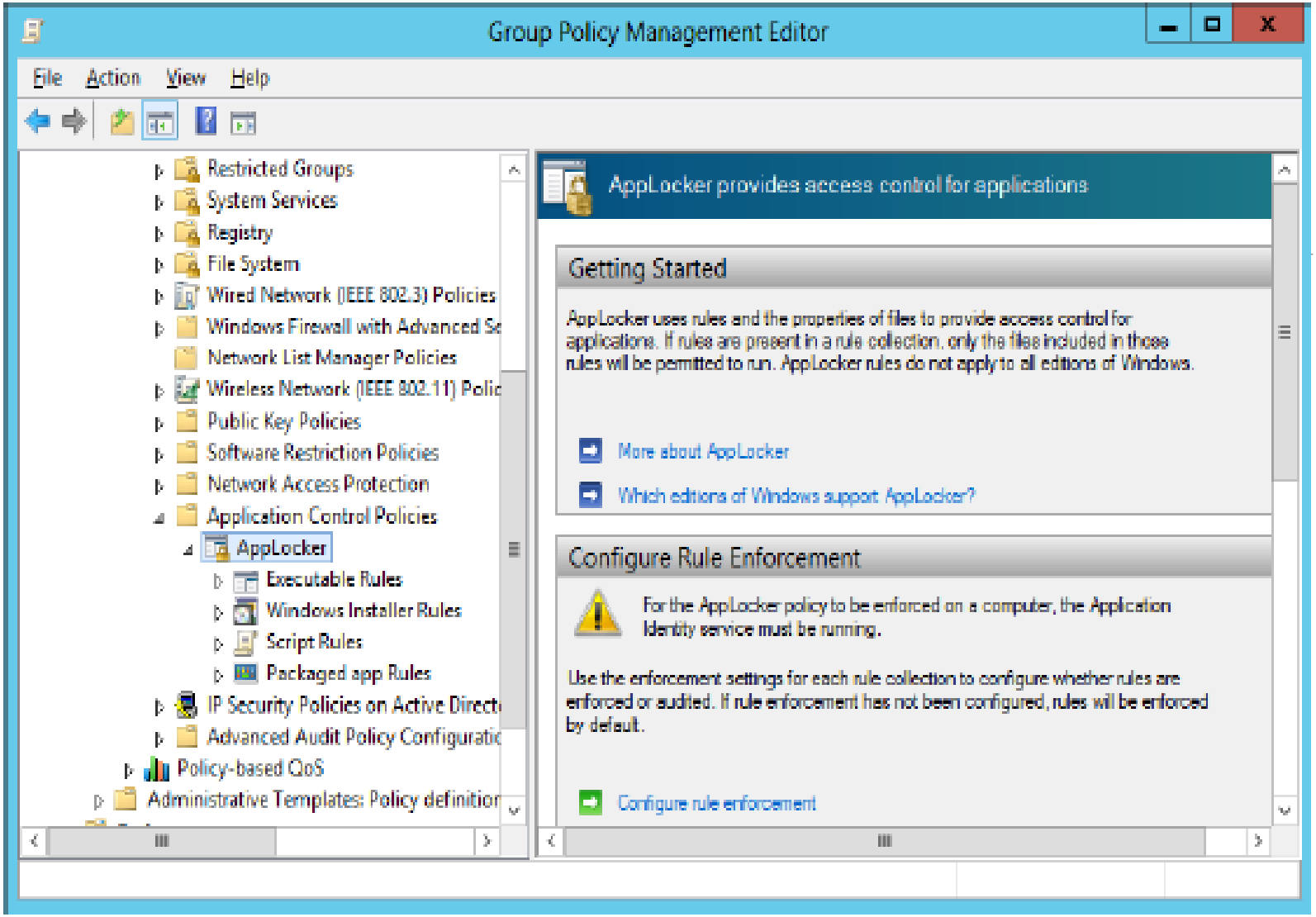



**FIGURE 6-19** The AppLocker container in a GPO

In the AppLocker container, there are four nodes that contain the basic rule types:

■■ **Executable Rules** Contains rules that apply to files with .exe and .com extensions

■■ **Windows Installer Rules** Contains rules that apply to Windows Installer packages with .msi and .msp extensions

■■ **Script Rules** Contains rules that apply to script files with .ps1, .bat, .cmd, .vbs, and .js extensions

■■ **Packaged App Rules** Contains rules that apply to applications purchased through the Windows Store Each of the rules you create in each of these containers can allow or block access to specific resources

## Creating rules automatically

- The greatest advantage of AppLocker over software restriction policies is the ability to create rules automatically. When you right-click one of the rules containers and select Automatically Generate Rules from the shortcut menu, the Automatically Generate Rules Wizard starts.
- The wizard then displays a summary of its results on the Review Rules page and adds the rules to the container.

# 4- Creating Rules Manually

- You can also create rules manually, by using a wizard-based interface.
- The wizard prompts you for the following:
  - **Action:** Specifies whether you want to allow or deny the user or group access to the resource. In AppLocker, explicit deny rules always override allow rules.
  - **User or group:** Specifies the name of the user or group to which the policy should apply.
  - **Conditions:** Specifies whether you want to create a publisher, path, or file hash rule. The wizard generates an additional page for whichever option you select, enabling you to configure its parameters.
  - **Exceptions:** Enables you to specify exceptions to the rule you create, using any of the three conditions: publisher, path, or file hash.