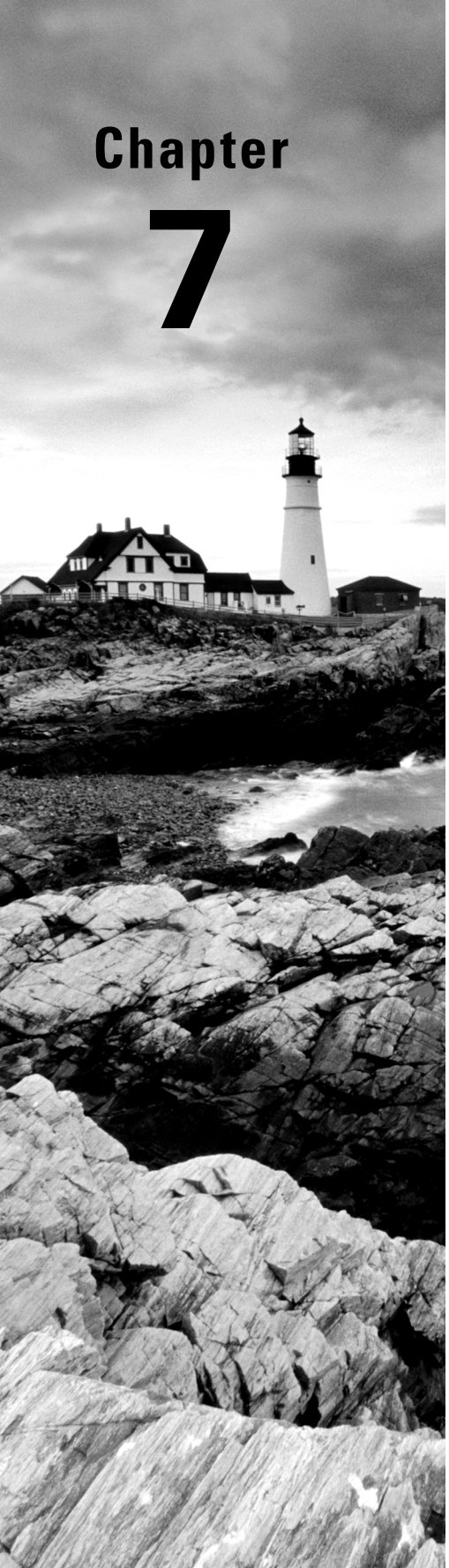


Chapter 7

Manage Security

THE FOLLOWING 70-410 EXAM OBJECTIVES ARE COVERED IN THIS CHAPTER:

✓ **Configuring security policies**

- Configure User Rights Assignment
- Configure Security Options settings
- Configure Security templates
- Configure Audit Policy
- Configure Local Users and Groups
- Configure User Account Control (UAC)

✓ **Configuring Windows Firewall**

- Configure rules for multiple profiles using Group Policy
- Configure connection security rules
- Configure Windows Firewall to allow or deny applications, scopes, ports, and users
- Configure authenticated firewall exceptions
- Import and export settings

As an IT Director and Microsoft Trainer, I can explain the importance of every chapter in this book, but some chapters are more important for real-world use. This is one of them.

Setting up security so that only people who need access to resources are the ones who get access to those resources is one of the most important jobs an IT member can have. This helps protect your data from hackers and, believe it or not, your own users.

In this chapter, you will learn how to protect data on your network. I will also discuss how to protect your individual system by using Windows Firewall.

Managing Security

One of the fundamental design goals for Active Directory is to define a single, centralized repository of users and information resources. Active Directory records information about all of the users, computers, and resources on your network. Each domain acts as a logical boundary, and members of the domain (including workstations, servers, and domain controllers) share information about the objects within them.

The information stored within Active Directory determines which resources are accessible to which users. Through the use of *permissions* that are assigned to Active Directory objects, you can control all aspects of network security.

You should be sure that you have implemented appropriate access control settings for the file system, network devices, and other resources. Let's look at the various components of network security, which include working with security principals and managing security and permissions, access control lists (ACLs), User Account Control (UAC), and access control entries (ACEs).

When you are setting up a network, you should always keep in mind that 90 percent of all hacks on a network are internal. This means internal permissions and security (as well as external security) need to be as strong as possible while still allowing users to do their jobs.

Understanding Security Principals

Security principals are Active Directory objects that are assigned *security identifiers (SIDs)*. An SID is a unique identifier that is used to manage any object to which permissions can be assigned. Security principals are assigned permissions to perform certain actions and access certain network resources.

The following basic types of Active Directory objects serve as security principals:

User Accounts User accounts identify individual users on your network by including information such as the user's name and their password. User accounts are the fundamental unit of security administration.

Groups There are two main types of groups: *security groups* and *distribution groups*. Both types can contain user accounts. System administrators use security groups to ease the management of security permissions. They use distribution groups, on the other hand, solely to send email. Distribution groups are not security principals. You'll see the details of groups in the next section.

Computer Accounts *Computer accounts* identify which client computers are members of particular domains. Because these computers participate in the Active Directory database, system administrators can manage security settings that affect the computer. They use computer accounts to determine whether a computer can join a domain and for authentication purposes. As you'll see later in this chapter, system administrators can also place restrictions on certain computer settings to increase security. These settings apply to the computer and, therefore, also apply to any user who is using it (regardless of the permissions granted to the user account).

Note that other objects, such as organizational units (OUs), do not function as security principals. What this means is that you can apply certain settings (such as Group Policy) on all of the objects within an OU; however, you cannot specifically set permissions with respect to the OU. The purpose of OUs is to organize other Active Directory objects logically based on business needs, add a needed level of control for security, and create an easier way to delegate.

You can manage security by performing the following actions with security principals:

- You can assign them permissions to access various network resources.
- You can give them user rights.
- You can track their actions through auditing (covered later in this chapter).

The major types of security principals—user accounts, groups, and computer accounts—form the basis of the Active Directory security architecture. As a system administrator, you will likely spend a portion of your time managing permissions for these objects.

It is important to understand that since a unique SID defines each security principal, deleting a security principal is an irreversible process. For example, if you delete a user account and then later re-create one with the same name, you'll need to reassign permissions and group membership settings for the new account. Once a user account is deleted, its SID is deleted.

Users and groups are two types of fundamental security principals employed for security administration. In the following sections, you'll learn how users and groups interact. You'll also learn about the different types of groups you can create.

Types of Groups

When dealing with groups, you should make the distinction between local security principals and domain security principals, as follows:

Local Users and Groups You use *local users and groups* to assign the permissions necessary to access the local machine. For example, you may assign the permissions you need to reboot a domain controller to a specific domain local group.

Domain Users and Groups *Domain users and groups*, on the other hand, are used throughout the domain. These objects are available on any of the computers within the Active Directory domain and between domains that have a trust relationship.

Here are the two main types of groups used in Active Directory:

Security Groups *Security groups* are considered security principals. They can contain user accounts, computers, or groups. To make administration simpler, system administrators usually grant permissions to groups. This allows you to change permissions easily at the Active Directory level (instead of at the level of the resource on which the permissions are assigned).

You can also place Active Directory Contact objects within security groups, but security permissions will not apply to them.

Distribution Groups Distribution groups are not considered security principals because they do not have SIDs. As mentioned earlier, they are used only for the purpose of sending email messages. You can add users to distribution groups just as you would add them to security groups. You can also place distribution groups within OUs so that they are easier to manage. You will find them useful, for example, if you need to send email messages to an entire department or business unit within Active Directory.

Understanding the differences between security and distribution groups is important in an Active Directory environment. For the most part, system administrators use security groups for the daily administration of permissions. On the other hand, system administrators who are responsible for maintaining email distribution lists generally use distribution groups to group members of departments and business units logically. (A system administrator can also email all of the users within a security group, but to do so, they would have to specify the email addresses for the accounts.)

When you are working in Windows Server 2003, Server 2008, Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 functional-level domains, you can convert security groups to or from distribution groups.

It is vital that you understand group types when you are getting ready to take the Microsoft exams. Microsoft likes to include trick questions about putting permissions on distribution groups. Remember, only security groups can have permissions assigned to them.

Group Scope

In addition to being classified by type, each group is given a specific scope. The scope of a group defines two characteristics. First, it determines the level of security that applies to

a group. Second, it determines which users can be added to the group. *Group scope* is an important concept in network environments because it ultimately defines which resources users are able to access.

The three types of group scope are as follows:

Domain Local The scope of *domain local groups* extends as far as the local domain. When you're using the Active Directory Users and Computers tool, domain local accounts apply to the computer for which you are viewing information. Domain local groups are used to assign permissions to local resources, such as files and printers. They can contain domain locals, global groups, universal groups, and user accounts.

Global The scope of *global groups* is limited to a single domain. Global groups may contain any of the users who are a part of the Active Directory domain in which the global groups reside or other global groups. Global groups are often used for managing domain security permissions based on job functions. For example, if you need to specify permissions for the Engineering department, you could create one or more global groups (such as EngineeringManagers and EngineeringDevelopers). You could then assign security permissions to each group.

Universal *Universal groups* can contain accounts or other universal groups from any domains within an Active Directory forest. Therefore, system administrators use them to manage security across domains. When you are managing multiple domains, it often helps to group global groups within universal groups. For instance, if you have an Engineering global group in the `research.stellacon.com` domain and an Engineering global group in the `asia.stellacon.com` domain, you can create a universal AllEngineers group that contains both of the global groups. Now whenever you must assign security permissions to all engineers within the organization, you need only assign permissions to the AllEngineers universal group.

For domain controllers to process authentication between domains, information about the membership of universal groups is stored in the global catalog (GC). Keep this in mind if you ever plan to place users directly into universal groups and bypass global groups because all of the users will be enumerated in the GC, which will impact size and performance.

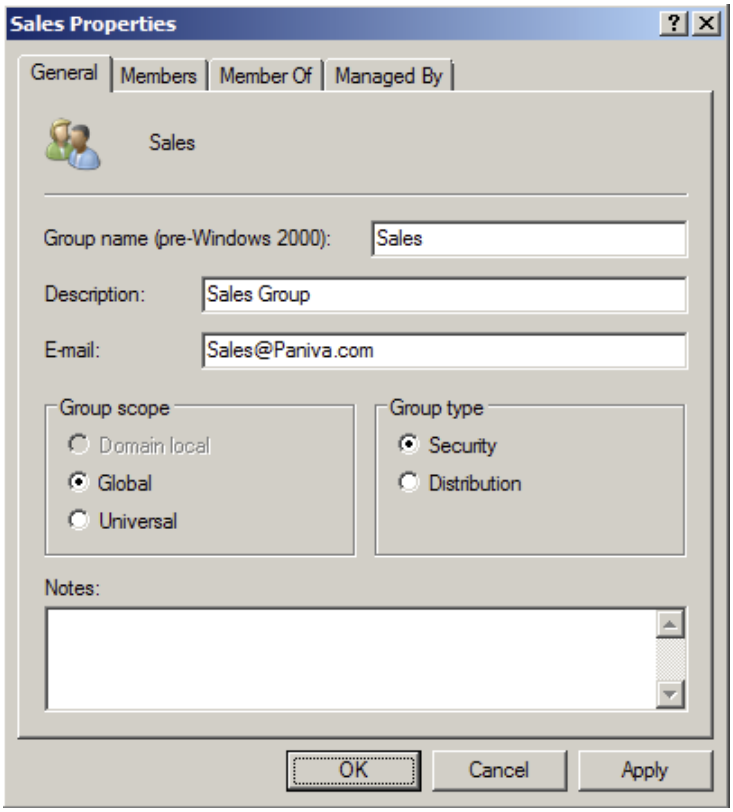
Fortunately, universal group credentials are cached on domain controllers that universal group members use to log on. This process is called *universal group membership caching*. The domain controller obtains the cached data whenever universal group members log on, and then it is retained on the domain controller for eight hours by default. This is especially useful for smaller locations, such as branch offices, that run less expensive domain controllers. Most domain controllers at these locations cannot store a copy of the entire GC, and frequent calls to the nearest GC would require an inordinate amount of network traffic.

When you create a new group using the Active Directory Users and Computers tool, you must specify the scope of the group. Figure 7.1 shows the New Object – Group dialog box and the available options for the group scope.

Changing group scope, however, can be helpful when your security administration or business needs change. You can change group scope easily using the Active Directory Users and Computers tool. To do so, access the properties of the group. As shown in Figure 7.2, you can make a group scope change by clicking one of the options.

FIGURE 7.1 The New Object – Group dialog box

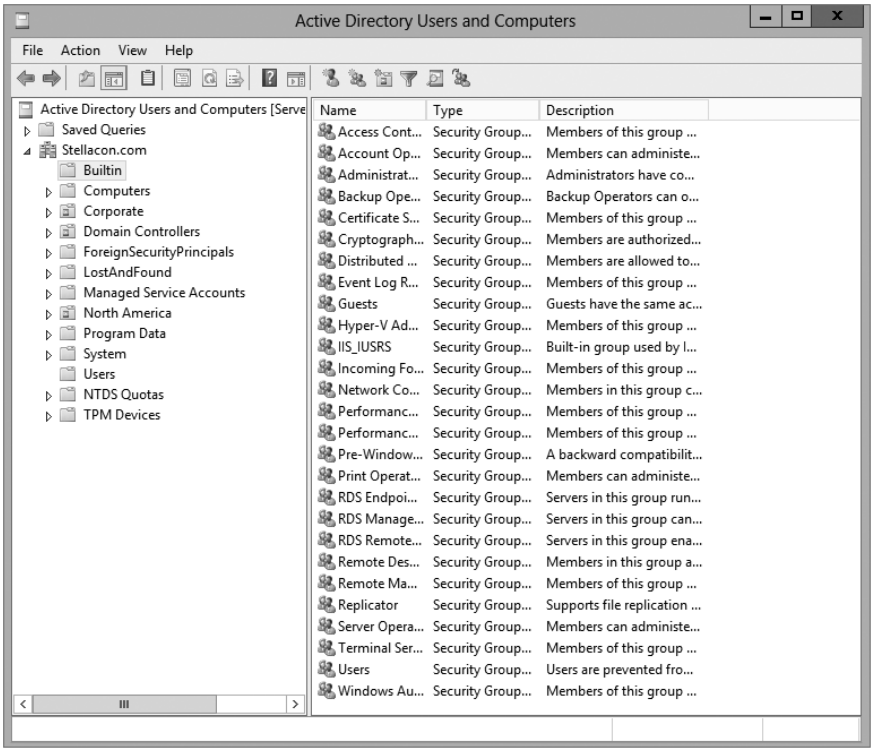
FIGURE 7.2 The Sales Security Group's Properties dialog box



Built-in Domain Local Groups

System administrators use built-in domain local groups to perform administrative functions on the local server. Because these have pre-assigned permissions and privileges, they allow system administrators to assign common management functions easily. Figure 7.3 shows the default built-in groups that are available on a Windows Server 2012 R2 domain controller.

FIGURE 7.3 Default built-in local groups



The list of built-in local groups includes some of the following:

Account Operators These users can create and modify domain user and group accounts. Members of this group are generally responsible for the daily administration of Active Directory.

Administrators By default, members of the Administrators group are given full permissions to perform any functions within the Active Directory domain and on the local computer. This means they can access all files and resources that reside on any server within the domain. As you can see, this is a powerful account.

In general, you should restrict the number of users who are included in this group because most common administration functions do not require this level of access.

Backup Operators One of the problems associated with backing up data in a secure network environment is that you need to provide a way to bypass standard file system security so that you can copy files. Although you could place users in the Administrators group, doing so usually provides more permissions than necessary. Members of the Backup Operators group can bypass standard file system security for the purpose of backup and recovery only. They cannot, however, directly access or open files within the file system.

Generally, backup software applications and data use the permissions assigned to the Backup Operators group.

Certificate Service DCOM Access Members of the Certificate Service DCOM Access group can connect to certificate authority servers in the enterprise.

Cryptographic Operators Members of the Cryptographic Operators group are authorized to perform cryptographic operations. *Cryptography* allows the use of codes to convert data, which then allows a specific recipient to read it using a key.

Guests Typically, you use the Guests group to provide access to resources that generally do not require security. For example, if you have a network share that provides files that should be made available to all network users, you can assign permissions to allow members of the Guests group to access those files.

Print Operators By default, members of the Print Operators group are given permissions to administer all of the printers within a domain. This includes common functions such as changing the priority of print jobs and deleting items from the print queue.

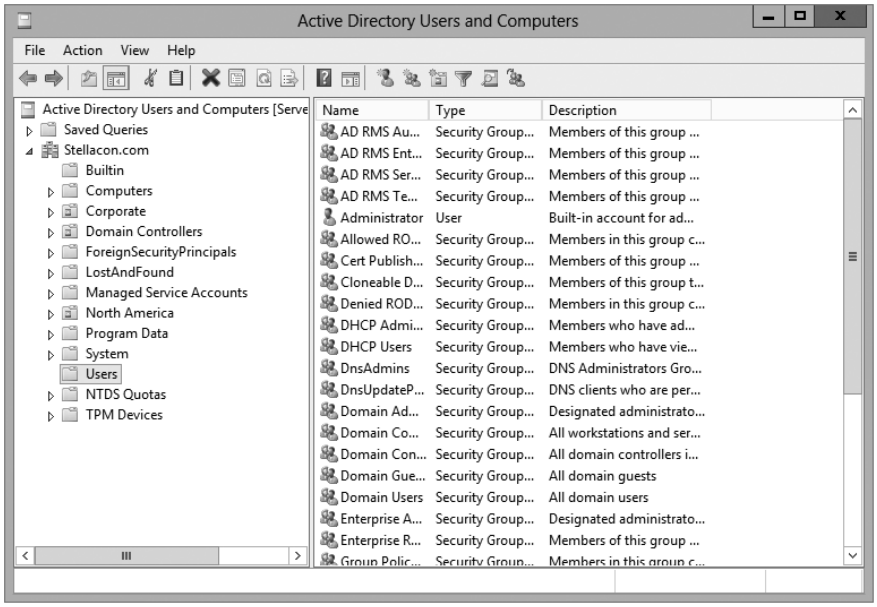
Replicator The Replicator group allows files to be replicated among the computers in a domain. You can add accounts used for replication-related tasks to this group to provide those accounts with the permissions they need to keep files synchronized across multiple computers.

Server Operators A common administrative task is managing server configuration. Members of the Server Operators group are granted the permissions they need to manage services, shares, and other system settings.

Users The Users built-in domain local group is used to administer security for most network accounts. Usually, you don't give this group many permissions, and you use it to apply security settings for most employees within an organization.

Windows Server 2012 R2 also includes many different default groups, which you can find in the `Users` folder. As shown in Figure 7.4, these groups are of varying scopes, including domain local, global, and universal groups. You'll see the details of these groups in the next section.

FIGURE 7.4 Contents of the default `Users` folder



Three important user accounts are created during the promotion of a domain controller, described here:

Administrator Account The Administrator account is assigned the password a system administrator provides during the promotion process, and it has full permissions to perform all actions within the domain.

Guest Account The Guest account is disabled by default. The purpose of the *Guest account* is to provide anonymous access to users who do not have an individual logon and password to use within the domain. Although the Guest account might be useful in some situations, it is generally recommended that this account be disabled to increase security.

Krbtgt, or Key Distribution Center Service, Account Only the operating system uses the *krbtgt*, or *Key Distribution Center Service*, *account* for Kerberos authentication while it is using `DCPromo.exe`. This account is disabled by default. Unlike other user accounts, the krbtgt account cannot be used to log on to the domain, and therefore it does not need to be enabled. Since only the operating system uses this account, you do not need to worry about hackers gaining access by using this account.

Predefined Global Groups

As mentioned earlier in this chapter, you use global groups to manage permissions at the domain level. Members of each of these groups can perform specific tasks related to managing Active Directory.

The following predefined global groups are installed in the `Users` folder:

Cert Publishers Certificates are used to increase security by allowing for strong authentication methods. User accounts are placed within the *Cert Publishers group* if they must publish security certificates. Generally, Active Directory security services use these accounts.

Domain Computers All of the computers that are members of the domain are generally members of the *Domain Computers group*. This includes any workstations or servers that have joined the domain, but it does not include the domain controllers.

Domain Admins Members of the *Domain Admins group* have full permissions to manage all of the Active Directory objects for this domain. This is a powerful account; therefore, you should restrict its membership only to those users who require full permissions.

Domain Controllers All of the domain controllers for a given domain are generally included within the *Domain Controllers group*.

Domain Guests Generally, by default, members of the *Domain Guests group* are given minimal permissions with respect to resources. System administrators may place user accounts in this group if they require only basic access or temporary permissions within the domain.

Domain Users The *Domain Users group* usually contains all of the user accounts for the given domain. This group is generally given basic permissions to resources that do not require higher levels of security. A common example is a public file share.

Enterprise Admins Members of the *Enterprise Admins group* are given full permissions to perform actions within the entire forest. This includes functions such as managing trust relationships and adding new domains to trees and forests.

Group Policy Creator Owners Members of the *Group Policy Creator Owners group* are able to create and modify Group Policy settings for objects within the domain. This allows them to enable security settings on OUs (and the objects they contain).

Schema Admins Members of the *Schema Admins group* are given permissions to modify the Active Directory schema. As a member of Schema Admins, you can create additional fields of information for user accounts. This is a powerful function because any changes to the schema will be propagated to all the domains and domain controllers within an Active Directory forest. Furthermore, you cannot undo changes to the schema (although you can disable some).

In addition to these groups, you can create new ones for specific services and applications that are installed on the server. Specifically, services that run on domain controllers and servers will be created as security groups with domain local scope. For example, if a domain controller is running the DNS service, the DnsAdmins and DnsUpdateProxy groups become available. In addition, there are two read-only domain controller (RODC) local groups: the Allowed RODC Password Replication and the Denied RODC Password Replication groups. Similarly, if you install the DHCP service, it automatically creates the

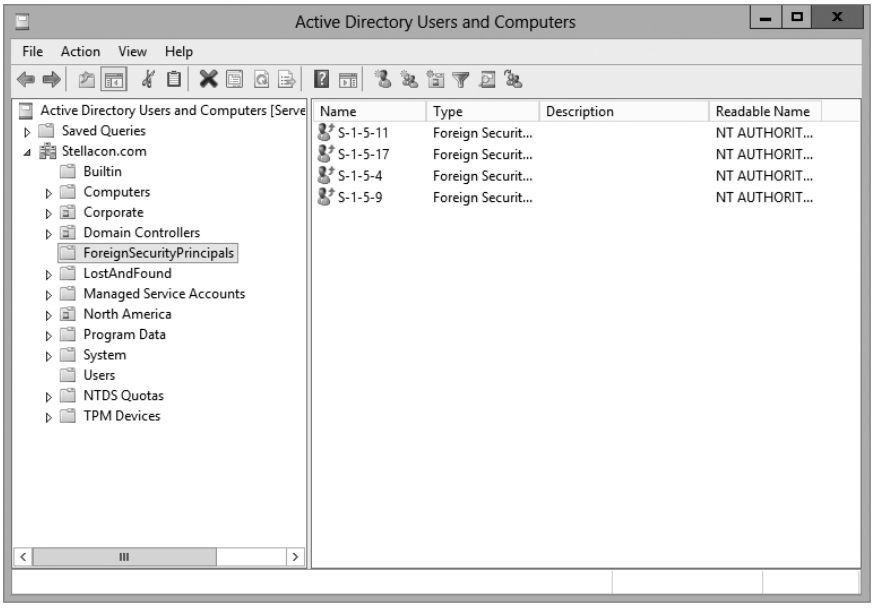
DHCP Users and DHCP Administrators groups. The purpose of these groups depends on the functionality of the applications being installed.

Foreign Security Principals

In environments that have more than one domain, you may need to grant permissions to users who reside in multiple domains. Generally, you manage this using Active Directory trees and forests. However, in some cases, you may want to provide resources to users who belong to domains that are not part of the forest.

Active Directory uses the concept of *foreign security principals* to allow permissions to be assigned to users who are not part of an Active Directory forest. This process is automatic and does not require the intervention of system administrators. You can then add the foreign security principals to domain local groups for which, in turn, you can grant permissions for resources within the domain. You can view a list of foreign security principals by using the Active Directory Users and Computers tool. Figure 7.5 shows the contents of the `ForeignSecurityPrincipals` folder.

FIGURE 7.5 The `ForeignSecurityPrincipals` folder

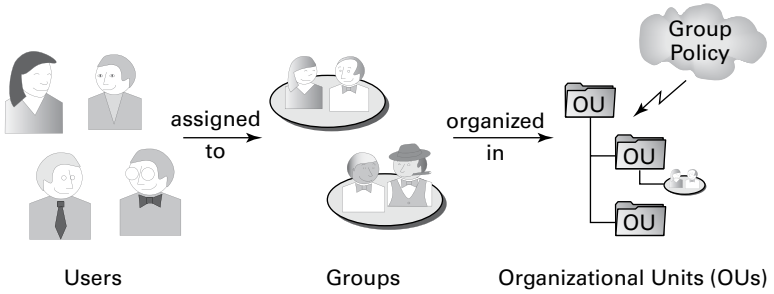


Managing Security and Permissions

Now that you understand the basic issues, terms, and Active Directory objects that pertain to security, it's time to look at how you can apply this information to secure your network resources. The general practice for managing security is to assign users to groups and then grant permissions and logon parameters to the groups so that they can access certain resources.

For management ease and to implement a hierarchical structure, you can place groups within OUs. You can also assign Group Policy settings to all of the objects contained within an OU. By using this method, you can combine the benefits of a hierarchical structure (through OUs) with the use of security principals. Figure 7.6 provides a diagram of this process.

FIGURE 7.6 An overview of security management



The primary tool you use to manage security permissions for users, groups, and computers is the Active Directory Users and Computers tool. Using this tool, you can create and manage Active Directory objects and organize them based on your business needs. Common tasks for many system administrators might include the following:

- Resetting a user's password (for example, in cases where they forget their password)
- Creating new user accounts (when, for instance, a new employee joins the company)
- Modifying group memberships based on changes in job requirements and functions
- Disabling user accounts (when, for example, users will be out of the office for long periods of time and will not require network resource access)

Once you've properly grouped your users, you need to set the actual permissions that affect the objects within Active Directory. The actual permissions available vary based on the type of object. Table 7.1 provides an example of some of the permissions that you can apply to various Active Directory objects and an explanation of what each permission does.

TABLE 7.1 Permissions of Active Directory objects

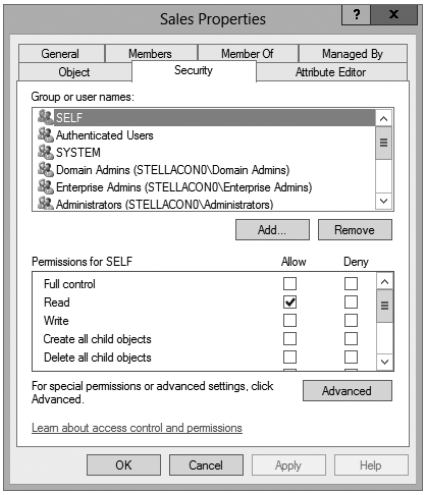
Permission	Explanation
Control Access	Changes security permissions on the object
Create Child	Creates objects within an OU (such as other OUs)
Delete Child	Deletes child objects within an OU

Delete Tree	Deletes an OU and the objects within it
List Contents	Views objects within an OU
List Object	Views a list of the objects within an OU
Read	Views properties of an object (such as a username)
Write	Modifies properties of an object

Using ACLs and ACEs

Each object in Active Directory has an *access control list (ACL)*. The ACL is a list of user accounts and groups that are allowed to access the resource. For each ACL, there is an access control entry (ACE) that defines what a user or a group can actually do with the resource. Deny permissions are always listed first. This means that if users have Deny permissions through user or group membership, they will not be allowed to access the object, even if they have explicit Allow permissions through other user or group permissions. Figure 7.7 shows an ACL for the Sales OU.

FIGURE 7.7 The ACL for an OU named Sales



The Security tab is enabled only if you selected the Advanced Features option from the View menu in the Active Directory Users and Computers tool.

Configuring User Account Control

One issue that many users have run into is as follows: When they log into their standard Windows user account and they need to make a change on their local machines or run a program that requires a higher level of security, they can't complete the task. This is where User Account Controls can help.

User Account Control (UAC) allows your domain users to log into their machines using their standard Windows user account and then execute processes that may require additional user group access.

Some applications may require additional security permissions to run successfully. These types of programs are normally referred to as *legacy applications*. Some applications, however, such as installing new software or making configuration changes, require more permissions than what is available to a standard user account. This is where UAC can help.

When an executable or program needs to function properly with more than just standard user rights, UAC can give that user's token additional user groups. This token allows the executable or program to function properly by giving the standard user account the rights to complete the task.

To configure the UAC, an administrator can go into the system's Control Panel and then User Accounts. Inside the User Accounts snap-in, choose Change User Account Control Settings.

Delegating Control of Users and Groups

A common administrative function related to the use of Active Directory involves managing users and groups. You can use OUs to group objects logically so that you can easily manage them. Once you have placed the appropriate Active Directory objects within OUs, you are ready to delegate control of these objects.

Delegation is the process by which a higher-level security administrator assigns permissions to other users. For example, if Admin A is a member of the Domain Admins group, they are able to delegate control of any OU within the domain to Admin B. You can access the Delegation Of Control Wizard through the Active Directory Users and Computers tool. You can use it to perform common delegation tasks quickly and easily. The wizard walks you through the steps of selecting the objects for which you want to perform delegation, what permission you want to allow, and which users will have those permissions.

Exercise 7.1 walks through the steps required to delegate control of OUs.

EXERCISE 7.1

Delegating Control of Active Directory Objects

1. Open the Active Directory Users and Computers tool.
2. Create a new user within the Engineering OU using the following information (use the default settings for any fields not specified):

First Name: **Robert**

Last Name: **Admin**

User Logon Name: **radmin**

Password: **P@ssw0rd**

3. Right-click the Sales OU and select Delegate Control. This starts the Delegation Of Control Wizard. Click Next.
4. To add users and groups to which you want to delegate control, click the Add button. In the Add dialog box, enter **Robert Admin** for the name of the user to add. Note that you can specify multiple users or groups using this option.
5. Click OK to add the account to the delegation list, which is shown in the Users Or Groups page. Click Next to continue.
6. On the Tasks To Delegate page, you must specify which actions you want to allow the selected user to perform within this OU. Select the Delegate The Following Common Tasks option and place a check mark next to the following options:

   Create, Delete, And Manage User Accounts

   Reset User Passwords And Force Password Change At Next Logon

   Read All User Information

   Create, Delete And Manage Groups

   Modify The Membership Of A Group
7. Click Next to continue. The wizard provides you with a summary of the selections that you have made on the Completing The Delegation Of Control Wizard page. To complete the process, click Finish to have the wizard commit the changes.

   Now when the user Robert Admin logs on (using *radmin* as his logon name), he will be able to perform common administrative functions for all the objects contained within the Sales OU.
8. When you have finished, close the Active Directory Users and Computers tool.

Understanding Dynamic Access Control

One of the advantages of Windows Server 2012 R2 is the ability to apply data governance to your file server. This will help control who has access to information and auditing. You get these advantages through the use of Dynamic Access Control (DAC). DAC allows you to identify data by using data classifications (both automatic and manual) and then to control access to these files based on these classifications.

DAC also gives administrators the ability to control file access by using a central access policy. This central access policy will also allow an administrator to set up audit access to files for reporting and forensic investigation.

DAC allows an administrator to set up Active Directory Rights Management Service (AD RMS) encryption for Microsoft Office documents. For example, you can set up encryption for any documents that contain financial information.

DAC gives an administrator the flexibility to configure file access and auditing to domain-based file servers. To do this, DAC controls claims in the authentication token, resource properties, and conditional expressions within permission and auditing entries.

Administrators have the ability to give users access to files and folders based on Active Directory attributes. For example, a user named Dana is given access to the file server share because in the user's Active Directory (department attribute) properties, the value contains the value Sales.

For DAC to function properly, an administrator must enable Windows 8 computers and Windows Server 2012/2012 R2 file servers to support claims and compound authentication.

Using Group Policy for Security

Through the use of Group Policy settings, system administrators can assign thousands of different settings and options for users, groups, and OUs. Specifically, in relation to security, you can use many different options to control how important features, such as password policies, user rights, and account lockout settings, can be configured.

The general process for making these settings is to create a Group Policy object (GPO) with the settings that you want and then link it to an OU or other Active Directory object.

Table 7.2 lists many Group Policy settings, which are relevant to creating a secure Active Directory environment. Note that this list is not comprehensive—many other options are available through Windows Server 2012 R2 administrative tools.

TABLE 7.2 Group Policy settings used for security purposes

Setting section	Setting name	Purpose
Account Policies ➢ Password Policy	Enforce Password History	Specifies how many passwords will be remembered. This option prevents users from reusing the same passwords whenever they're changed.
Account Policies ➢ Password Policy	Minimum Password Length	Prevents users from using short, weak passwords by specifying the minimum number of characters that the password must include.

Account Policies ➢ Account Lockout Policy	Account Lockout Threshold	Specifies how many bad password attempts can be entered before the account gets locked out.
Account Policies ➢ Account Lockout Policy	Account Lockout Duration	Specifies how long an account will remain locked out after too many bad password attempts have been entered. By setting this option to a reasonable value (such as 30 minutes), you can reduce administrative overhead while still maintaining fairly strong security.
Account Policies ➢ Account Lockout Policy	Reset Account Lockout Counter After	Specifies how long the Account Lockout Threshold counter will hold failed logon attempts before resetting to 0.
Local Policies ➢ Security Options	Accounts: Rename Administrator Account	Often, when trying to gain unauthorized access to a computer, individuals attempt to guess the administrator password. One method for increasing security is to rename this account so that no password allows entry using this logon.
Local Policies ➢ Security Options	Domain Controller: Allow Server Operators To Schedule Tasks	This option specifies whether members of the built-in Server Operators group are allowed to schedule tasks on the server.
Local Policies ➢ Security Options	Interactive Logon: Do Not Display Last User Name	Increases security by not displaying the name of the last user who logged onto the system.
Local Policies ➢ Security Options	Shutdown: Allow System To Be Shut Down Without Having To Log On	Allows system administrators to perform remote shutdown operations without logging on to the server.

Implementing an Audit Policy

One of the most important aspects of controlling security in networked environments is ensuring that only authorized users are able to access specific resources. Although system administrators often spend much time managing security permissions, it is almost always possible for a security problem to occur.

Sometimes, the best way to find possible security breaches is actually to record the actions that specific users take. Then, in the case of a security breach (the unauthorized shutdown of a server, for example), system administrators can examine the log to find the cause of the problem.

The Windows Server 2012 R2 operating system and Active Directory offer you the ability to audit a wide range of actions. In the following sections, you'll see how to implement auditing for Active Directory.

Overview of Auditing

The act of *auditing* relates to recording specific actions. From a security standpoint, auditing is used to detect any possible misuse of network resources. Although auditing does not necessarily prevent resources from being misused, it does help determine when security violations have occurred (or were attempted). Furthermore, just the fact that others know that you have implemented auditing may prevent them from attempting to circumvent security.

You need to complete several steps in order to implement auditing using Windows Server 2012 R2:

1. Configure the size and storage settings for the audit logs.
2. Enable categories of events to audit.
3. Specify which objects and actions should be recorded in the audit log.

Note that there are trade-offs to implementing auditing. First, recording auditing information can consume system resources. This can decrease overall system performance and use up valuable disk space. Second, auditing many events can make the audit log impractical to view. If too much detail is provided, system administrators are unlikely to scrutinize all of the recorded events. For these reasons, you should always be sure to find a balance between the level of auditing details provided and the performance-management implications of these settings.

Implementing Auditing

Auditing is not an all-or-none type of process. As is the case with security in general, system administrators must choose specifically which objects and actions they want to audit.

The main categories for auditing include the following:

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

In this list of categories, four of the categories are related to Active Directory. Let's discuss these auditing categories in a bit more detail.

Audit Account Logon Events You enable this auditing event if you want to audit when a user authenticates with a domain controller and logs onto the domain. This event is logged in the security log on the domain controller.

Audit Account Management This auditing event is used when you want to watch what changes are being made to Active Directory accounts. For example, when another administrator creates or deletes a user account, it would be an audited event.

Audit Directory Service Access This auditing event occurs whenever a user or administrator accesses Active Directory objects. Let's say that an administrator opens Active Directory and clicks a user account; even if nothing is changed on that account, an event is logged.

Audit Logon Events Account logon events are created for domain account activity. For example, you have a user who logs on to a server so that they can access files; the act of logging onto the server creates this audit event.

Audit Object Access Audit object access allows you to audit objects within your network such as folders, files, and printers. If you suspect someone is trying to hack into an object (for example, the `finance` folder), this is the type of auditing that you would use. You still would need to enable auditing on the actual object (for example, the `finance` folder).

Audit Policy Change Audit policy change allows you to audit changes to user rights assignment policies, audit policies, or trust policies. This auditing allows you to see whether anyone changes any of the other audit policies.

Audit Privilege Use Setting the audit privilege use allows an administrator to audit each instance of a user exercising a user right. For example, if a user changes the system time on a machine, this is a user right. Logging on locally is another common user right.

To audit access to objects stored within Active Directory, you must enable the Audit Directory Service Access option. Then you must specify which objects and actions should be tracked.

Exercise 7.2 walks through the steps you must take to implement auditing of Active Directory objects on domain controllers.

EXERCISE 7.2

Enabling Auditing of Active Directory Objects

1. Open the Local Security Policy tool (located in the Administrative Tools program group).
2. Expand Local Policies ➢ Audit Policy.
3. Double-click the setting for Audit Directory Service Access.
4. In the Audit Directory Service Access Properties dialog box, place check marks next to Success and Failure. Click OK to save the settings.
5. Close the Local Security Policy tool.

Using the *Auditpol.exe* Command

There may be a time when you need to look at your actual auditing policies set on a user or a system. This is where an administrator can use the `Auditpol.exe` command. *Auditpol* allows administrators the ability not only to view an audit policy but also to set, configure, modify, restore, and even remove an audit policy. Auditpol is a command-line utility, and there are multiple switches that can be used with Auditpol. The following is the syntax used with Auditpol; Table 7.3 describes some of the switches:

```
Auditpol command [<sub-command><options>]
```

Here's an example:

```
Auditpol /get /user:wpanek /category:"Detailed Tracking" /r
```

TABLE 7.3 Auditpol commands

Command	Description
`/backup`	Allows an administrator to save the audit policy to a file
`/clear`	Allows an administrator to clear an audit policy
`/get`	Gives administrators the ability to view the current audit policy
`/list`	Allows you to view selectable policy elements
`/remove`	Removes all per-user audit policy settings and disables all system audit policy settings
`/restore`	Allows an administrator to restore an audit policy from a file that was previously created by using `auditpol /backup`
`/set`	Gives an administrator the ability to set an audit policy
`/?`	Displays help

Features of Windows Server 2012 R2 Auditing

Microsoft continues to increase the level of detail in the security auditing logs. Microsoft has also simplified the deployment and management of auditing policies. The following list includes some of the features:

Global Object Access Auditing Administrators using Windows Server 2012 R2 and Windows 8 now have the ability to define computer-wide system access control lists (SACLs). Administrators can define SACLs for either the file system or the registry. After the specified SACL is defined, the SACL is then applied automatically to every object

of that type. This can be helpful to administrators for verifying that all critical files, folders, and registry settings on a computer are protected. This is also helpful for identifying when an issue occurs with a system resource.

"Reason For Access" Reporting When an administrator is performing auditing in Windows Server 2012 R2 and Windows 8, they can now see the reason why an operation was successful or unsuccessful. Previously, they lacked the ability to see the reason why an operation succeeded or failed.

Advanced Audit Policy Settings In Windows Server 2012 R2, there are many new Advanced Audit Policy settings that can be used in place of the nine basic auditing settings. These advanced audit settings also help eliminate the unnecessary auditing activities that can make audit logs difficult to manage and decipher.

Expression-Based Audit Policies Administrators have the ability, because of Dynamic Access Control, to create targeted audit policies by using expressions based on user, computer, and resource claims. For example, an administrator has the ability to create an audit policy that tracks all Read and Write operations for files that are considered high-business impact. Expression-based audit policies can be directly created on a file or folder or created through the use of a Group Policy.

Removable Storage Device Auditing Administrators have the ability to monitor attempts to use a removable storage device on your network. If an administrator decides to implement this policy, an audit event is created every time one of your users attempts to copy, move, or save a network resource onto a removable storage device.

Configuring Windows Firewall Options

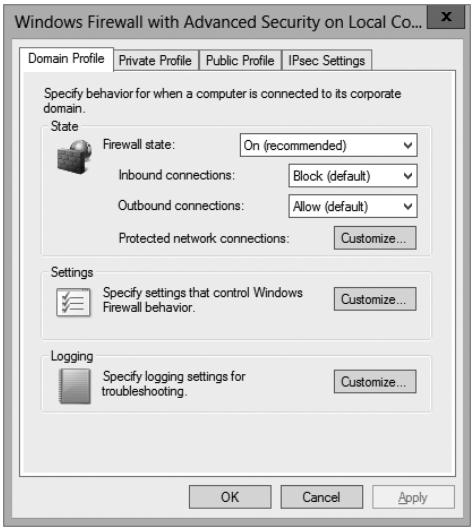
Another security aspect to look into is Windows Firewall. Before I can start talking about firewall options, you must first understand what a firewall does. A *firewall* is a software or hardware device that checks the information that is received from an outside (Internet) or external network and uses that information to determine whether the packet should be accepted or declined.

Depending on the firewall, you have the ability to check all potential remote users against Active Directory to verify that the remote user has an authorized domain account. This process is called *Active Directory account integration*.

Microsoft Windows Server 2012 R2 has a built-in firewall. The following are some of the configuration options included in the Windows Firewall Settings dialog box:

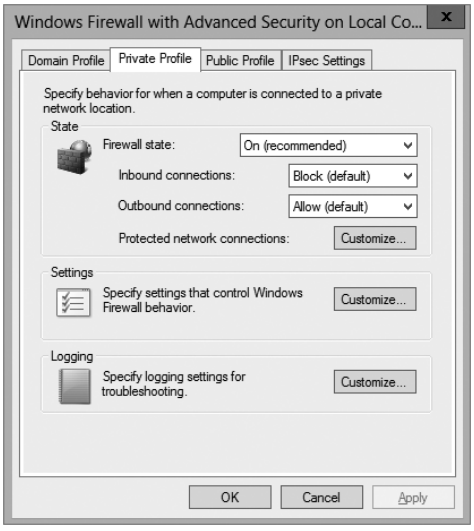
Domain Profile Tab On the Domain Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State option on this tab, it's for turning the firewall on or off for the domain only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.8). Administrators also have the ability to control the Windows Firewall behavior along with setting up logging.

FIGURE 7.8 Domain Profile tab of Windows Firewall Settings



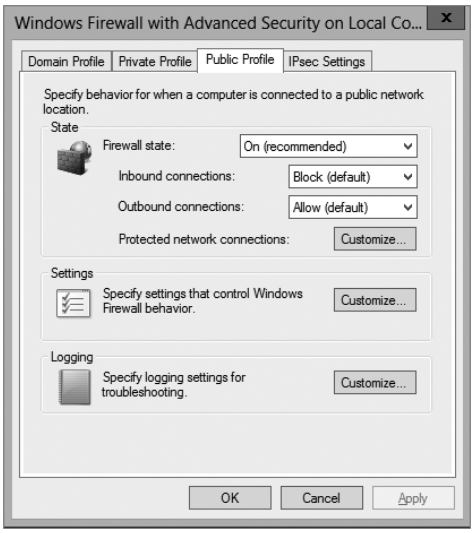
Private Profile Tab On the Private Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State in this tab, it's for turning the firewall on or off for the Private Profile only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.9). Administrators also have the ability to control the Windows Firewall Private Profile behavior along with setting up logging.

FIGURE 7.9 Private Profile tab of Windows Firewall Settings



Public Profile On the Public Profile tab, you have the ability to turn the firewall on or off by using the Firewall State drop-down menu. When setting the Firewall State in this tab, it's for turning the firewall on or off for the Public Profile only. When turning the firewall on, you also have the ability to block inbound and outbound connections (see Figure 7.10). Administrators also have the ability to control the Windows Firewall Public Profile behavior along with setting up logging.

FIGURE 7.10 Public Profile tab of Windows Firewall



IPsec Settings Tab The IPsec Setting tab allows you to set up the IPsec defaults, IPsec exemptions, and IPsec tunnel authorization. The IPsec defaults button allows you to specify settings used by IPsec to establish secured connections. The IPsec exemptions allow you to set up ICMP exemptions from IPsec. Finally, you can set up IPsec tunnel authorization, which allows you to specify the users and computers that are authorized to establish an IPsec tunnel (see Figure 7.11).

Windows Server 2012 R2 takes firewalls a step further than just the normal firewall settings in Control Panel. An MMC snap-in called *Windows Firewall with Advanced Security* (see Figure 7.12) can block all incoming and outgoing connections based on its configuration.

One of the major advantages to using the Windows Firewall with Advanced Security snap-in is the ability to set firewall configurations on remote computers using group policies. Another advantage to using this MMC is the ability to set up firewalls using IPsec security. Windows Firewall with Advanced Security snap-in allows an administrator to set more in-depth rules for Microsoft Active Directory users and groups, source and destination Internet Protocol (IP) addresses, IP port numbers, ICMP settings, IPsec settings, specific types of interfaces, and services.

FIGURE 7.11 IPsec Settings tab of Windows Firewall Settings

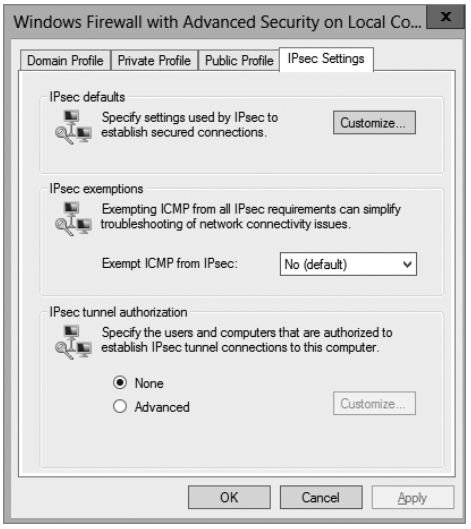
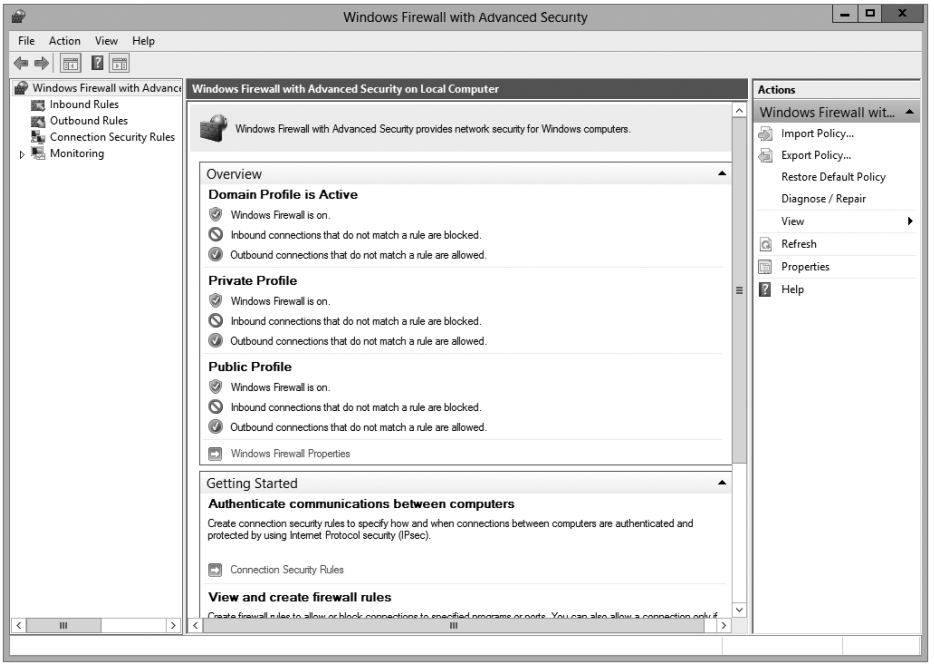


FIGURE 7.12 Windows Firewall with Advanced Security snap-in



You can configure more advanced settings by configuring Windows Firewall with Advanced Security. To access Windows Firewall with Advanced Security, press the Windows key and choose Control Panel ➢ Large Icons View ➢ Windows Firewall, and click the Advanced Settings link.

The scope pane to the left shows that you can set up specific inbound and outbound rules, connection security rules, and monitoring rules. The central area shows an overview of the firewall's status as well as the current profile settings. Let's take a look at these in more detail.

Inbound and Outbound Rules

Inbound and outbound rules consist of many preconfigured rules that can be enabled or disabled. Obviously, inbound rules (see Figure 7.13) monitor inbound traffic, and outbound rules monitor outbound traffic. By default, many are disabled. Double-clicking a rule will bring up its Properties dialog box, as shown in Figure 7.14.

You can filter the rules to make them easier to view. Filtering can be performed based on the profile the rule affects or whether the rule is enabled or disabled or based on the rule group.

If you can't find a rule that is appropriate to your needs, you can create a new rule by right-clicking Inbound Rules or Outbound Rules in the scope pane and then selecting New Rule. The New Inbound (or Outbound) Rule Wizard will launch, and you will be asked whether you want to create a rule based on a particular program, protocol or port, predefined category, or custom settings.

FIGURE 7.13 Inbound rules

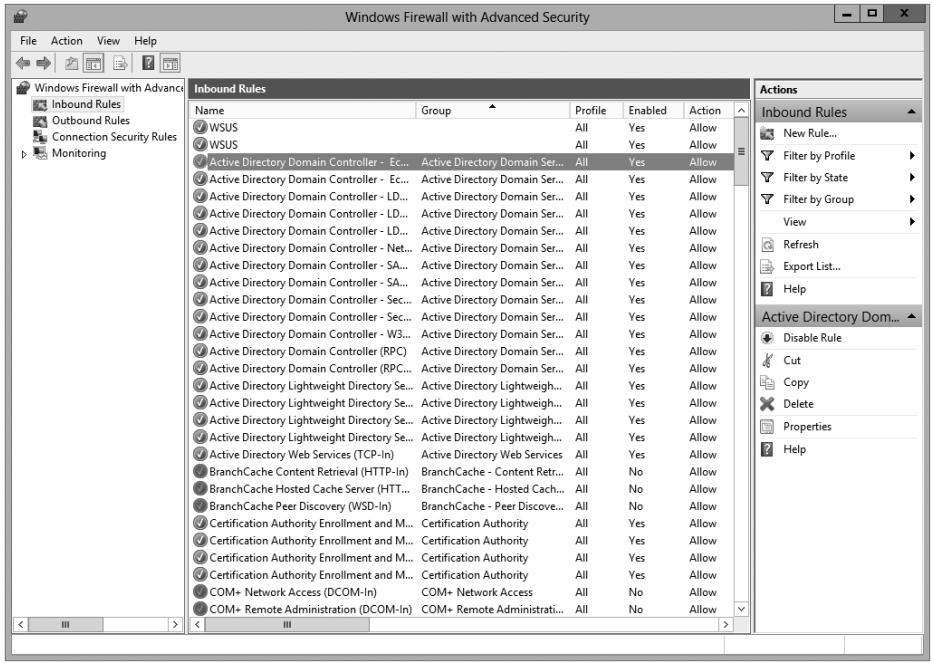


FIGURE 7.14 An inbound rule's Properties dialog box for WSUS

When setting up rules, you can also set up firewall exceptions. These exceptions allow you to work around a particular rule that you may be setting up. Firewall exceptions can be handy when an authenticated user or service needs to get around a firewall setting. These exceptions can be also set under the advanced firewall settings under the Connection Security Rules link.

Exercise 7.3 will walk you through the steps needed to create a new inbound rule that will allow only encrypted TCP traffic. In this exercise, you will have the ability to create a custom rule and then specify which authorized users and computers can connect using this rule.

EXERCISE 7.3

Configuring Windows Firewall

1. Press the Windows key and select Control Panel ➢ Large Icon View ➢ Windows Firewall.
2. Click Advanced Settings on the left side.
3. Right-click Inbound Rules and select New Rule.
4. Choose a rule type. For this exercise, choose Custom so that you can see all of the options available to you; then click Next.
5. Choose the programs or services that are affected by this rule. For this exercise, choose All Programs; then click Next.

6. Choose the protocol type as well as the local and remote port numbers that are affected by this rule. For this exercise, choose TCP and make sure All Ports is selected for both Local Port and Remote Port. Click Next to continue.
7. Choose the local and remote IP addresses that are affected by this rule. Choose Any IP Address for both local and remote; then click Next.
8. Specify whether this rule will allow the connection, allow the connection only if it is secure, or block the connection. Select the option Allow The Connection If It Is Secure; then click Next.
9. Specify whether connections should be allowed only from certain users. You can experiment with these options if you want. Then click Next to continue.
10. Specify whether connections should be allowed only from certain computers. Again, you can experiment with these options if you want. Then click Next to continue.
11. Choose those profiles that will be affected by this rule. Select one or more profiles; then click Next to continue.
12. Give your profile a name and description; then click Finish. Your custom rule will appear in the list of Inbound Rules, and the rule will be enabled.
13. Double-click your newly created rule. Notice that you can change the options you previously configured.
14. Disable the rule by right-clicking the rule and choosing Disable Rule.
15. Close Windows Firewall.

Now let's take a look at setting up Connection Security Rules through Windows Firewall with Advanced Security.

Configuring Windows Firewall with a GPO

If you wanted to configure Windows Firewall on all of your client machines, you have two options. You can either configure each machine manually or set up a GPO to configure the Windows Firewall. To set up the Windows Firewall using a GPO, configure the Computer section ➢ Windows Settings ➢ Security ➢ Windows Firewall With Advanced Security.

One of the advantages of using a GPO when configuring the Windows firewall is that you can configure multiple profiles and multiple firewall settings using the Group Policy.

Another even bigger advantage is being able to configure thousands of computers by setting just one GPO. It saves an IT administrator from going around the company from machine to machine to set up the firewall.

Import/Export Policies

One advantage of configuring Windows Firewall is the ability to export and import policy settings. For example, I set up a policy for 35 machines; I created the policy on one of the 35 machines and then exported the policy. I then imported the policy to the other

34 machines so that I did not have to re-create the policy over and over again. To export a policy, right-click Windows Firewall With Advanced Security and choose Export Policy. Choose Import Policy on the other machines to import the policy.

IPsec Policy Settings in Windows Firewall

When configuring options for Windows Firewall with Advanced Security, you have the ability to configure some IPsec policies. The three options are as follows:

IPsec Defaults Specify settings used by IPsec to establish secure connections.

IPsec Exemptions Exempting ICMP from all IPsec requirements can simplify troubleshooting of network connectivity issues.

IPsec Tunnel Authorization Specify the computers or users authorized to establish IPsec tunnel connections to this computer.

Monitoring

The Monitoring section shows detailed information about the firewall configurations for the Domain Profile, Private Profile, and Public Profile settings. These network location profiles determine which settings are enforced for private networks, public networks, and networks connected to a domain.

Real World Scenario

Firewalls

When I'm consulting, it always makes me laugh when I see small to midsize companies using Microsoft Windows Firewall and no other protection.

Microsoft Windows Firewall should be your *last* line of defense, not your only one. You need to make sure that you have good hardware firewalls that separate your network from the world.

Also watch Windows Firewall when it comes to printing. I have run into many situations where a printer that needs to talk to the operating system has issues when Windows Firewall is enabled. If this happens, make sure that the printer is allowed in the Allowed Programs section.

Summary

In this chapter, you examined server security and saw why it's one of the most important aspects of Windows Server 2012 R2. As a system administrator, Windows security is something that every administrator should be using but many don't know how it works properly.

I explained how to set up groups and group security as well as how to set up the permissions for those groups. I also covered auditing. I showed you how to set up and monitor auditing to see who has successfully, or unsuccessfully, accessed resources, machines, Active Directory, and all aspects of network security.

I finished the chapter by looking into Windows Firewall. I showed you how to configure the firewall and add exclusions and rules. I also showed you how to view and monitor the firewall results.

Exam Essentials

Understand group types and group scope. The two major types of groups are security and distribution groups, and they have different purposes. Groups can be local, global, or universal. Domain local groups are used to assign permissions to local resources, such as files and printers. The scope of global groups is limited to a single domain. Universal groups can contain users from any domains within an Active Directory forest.

Understand the purpose and permissions of built-in groups. The Active Directory environment includes several built-in local and global groups that are designed to simplify common system administration tasks. For instance, members of the Administrators group are given full permissions to perform any functions within the Active Directory domain and on the local computer.

Understand how to use Group Policy to manage security-related policies. Through the use of Group Policy settings, you can configure password and account-related options. You can also specify to which users, groups, and OUs many of the settings apply.

Understand how to use auditing. Through the use of auditing, an administrator can see who has been successfully and unsuccessfully accessing resources and Active Directory.

Understand Windows Firewall. Windows Server 2012 R2 includes Windows Firewall. Windows Firewall gives you secure access to a machine by allowing or denying which applications or users can access a system.

Review Questions

1. You are the network administrator for your organization. A new company policy has been released wherein if a user enters their password incorrectly three times within five minutes, they are locked out for 30 minutes. What three actions do you need to set to comply with this policy? (Choose all that apply.)
   - **A.** Set Account Lockout Duration to five minutes.
   - **B.** Set Account Lockout Duration to 30 minutes.
   - **C.** Set the Account Lockout Threshold setting to three invalid logon attempts.
   - **D.** Set the Account Lockout Threshold setting to 30 minutes.
   - **E.** Set the Reset Account Lockout Counter setting to five minutes.
   - **F.** Set the Reset Account Lockout Counter setting to three times.

2. You create a GPO and link it to the Sales OU. You want to monitor users in the Sales OU who connect to the file server. What type of auditing do you enable?
   - **A.** Audit Object Access
   - **B.** Audit Logon Events
   - **C.** Audit System Events
   - **D.** Audit Process Tracking

3. Alexis is a system administrator for an Active Directory environment that contains four domains. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:
   - Audit changes to User objects that are contained within a specific OU.
   - Allow a special user account called Audit to view and modify all security-related information about objects in that OU.

   Which of the following steps should Alexis take to meet these requirements? (Choose all that apply.)
   - **A.** Convert all volumes on which Active Directory information resides to NTFS.
   - **B.** Enable auditing with the Active Directory Users and Computers tool.
   - **C.** Create a new Active Directory domain and create restrictive permissions for the suspected users within this domain.
   - **D.** Reconfigure trust settings using the Active Directory Domains and Trusts tool.
   - **E.** Specify auditing options for the OU using the Active Directory Users and Computers tool.
   - **F.** Use the Delegation of Control Wizard to grant appropriate permissions to view and modify objects within the OU to the Audit user account.

4. Crystal is a system administrator for an Active Directory environment that is running in Native mode. Recently, several managers have reported suspicions about user activities and have asked her to increase security in the environment. Specifically, the requirements are as follows:

   - The accessing of certain sensitive files must be logged.
   - Modifications to certain sensitive files must be logged.
   - System administrators must be able to provide information about which users accessed sensitive files and when they were accessed.
   - All logon attempts for specific shared machines must be recorded.

   Which of the following steps should Crystal take to meet these requirements? (Choose all that apply.)

   A. Enable auditing with the Computer Management tool.
   B. Enable auditing with the Active Directory Users and Computers tool.
   C. Enable auditing with the Active Directory Domains and Trusts tool.
   D. Enable auditing with the Event Viewer tool.
   E. View the audit log using the Event Viewer tool.
   F. View auditing information using the Computer Management tool.
   G. Enable failure and success auditing settings for specific files stored on NTFS volumes.
   H. Enable failure and success auditing settings for logon events on specific computer accounts.

5. You create a GPO and link it to the Sales OU. You want to monitor users in the Sales OU who connect to the file server. What type of auditing do you enable?

   A. Audit Object Access
   B. Audit Logon Events
   C. Audit System Events
   D. Audit Process Tracking