Designing an Access Control Strategy for Data

Terms you’ll need to understand:
✓ Delegation of Control
✓ Auditing
✓ A G U DL P
✓ Permissions
✓ Rights

Techniques you’ll need to master:
✓ Designing an access control strategy for directory services
✓ Designing an access control strategy for files and folders
✓ Designing an access control strategy for the Registry
The main purpose of a network is to share resources, which include hardware, software, applications, and information. Your network needs to be designed to allow for this as transparently as possible for those who have authorization. At the same time, your design needs to prevent those who are not authorized from using or even viewing the objects in your directory. Windows Server 2003 provides a structure that assists you in designing your access control strategy. In this chapter, we examine this built-in structure and its relation to access control in the following key areas:

- Designing an access control strategy for directory services
- Designing an access control strategy for files and folders
- Designing an access control strategy for the Registry

**Designing an Access Control Strategy for Directory Services**

The design of each network is unique in regard to access control. Many factors can affect your decisions, such as whether you want to manage the entire network yourself or delegate some responsibility, and how sensitive the information is and how tightly you need to control access to it. Some standards are built in to Windows Server 2003 servers that you can follow. You need to understand access control strategy in regard to the following concepts:

- Creating a delegation strategy
- Analyzing auditing requirements
- Designing an appropriate group strategy for accessing resources
- Designing a permission structure for directory service objects

**Creating a Delegation Strategy**

Your job as a network administrator is to control all aspects of the functionality and data on your network. This can be a monumental task on a large network. For example, your network might include many different geographical locations, making management by one person a difficult task. Also, a manager at a remote location might know better than you what type and level of network management is needed at that location. For these reasons, network administrators sometimes delegate the ability to manage certain aspects of a network to other managers.
In Windows Server 2003, a user does not have to be a network administrator to handle some network management tasks. You can use the structure of the system to delegate the necessary control over only the appropriate objects and attributes for each user that you designate. Windows Server 2003 Active Directory provides the means to control every object’s access to every other object. To create an effective delegation strategy, you need to understand the concept and the use of the following components of Active Directory:

➤ Objects
➤ Organizational units (OUs)
➤ Discretionary access control lists (DACLs)
➤ Delegation of Control Wizard

**Objects**

Basically, everything in Active Directory is an object. This includes users, computers, resources, Group Policies, and even connections. Each of these objects is fully controllable as to what it can do to other objects and what other objects can do to it. You can place objects into containers, such as domains, OUs, and sites to better manage those objects. You can create new objects when needed to represent the physical or logical characteristics of your network. Each object is unique and is represented to your Active Directory with a *security descriptor*. Even if you were to delete an object and re-create an object with the same name, the new object would be totally new to your Active Directory.

**Organizational Units**

An organizational unit (OU) is a container that is used to group objects into logical units. OUs have two primary purposes. First, OUs are used to control the distribution of Group Policies to groups of computers and users. Second, OUs are used to delegate administrative authority. You can delegate to a user the right to manage all of the objects that are in a certain OU. You can then determine which objects you place into the OU.
Discretionary Access Control Lists
As we discussed previously, every object in Active Directory is fully controllable. The discretionary access control lists (DACLs) provide this control. Each object has its own DACL, and each DACL has a set of access control entries (ACEs) that can be set to allow or to deny permissions to another object in Active Directory. These permissions include Full Control, Read, Write, Create All Child Objects, Delete All Child Objects, and many other Special Permissions. You can implicitly deny permissions by simply not allowing them, or you can explicitly deny permissions by selecting Deny. Figure 6.1 shows a DACL.

![Figure 6.1](image)

Figure 6.1 Each object in Active Directory has its own discretionary access control list.

**Alert**
You need to be careful about explicitly denying any permissions because an explicit Deny applied to a user or group overrides any other permissions that user might have had through another group membership.

Delegation of Control Wizard
As you might have noticed, the DACLs can be complex and confusing in regard to the correct settings to apply for a desired result. For this reason, the Delegation of Control Wizard focuses instead on the desired result. You simply select the tasks that you want the user to be allowed to perform, and the wizard changes the DACLs so that the user has the permissions to perform the selected tasks.
You access the Delegation of Control Wizard by right-clicking a selected container in Active Directory Users and Computers or Active Directory Sites and Services and then clicking Delegate Control. You can then choose the user or group to which you want to delegate control. Next, you choose tasks from a list or you can create a custom task. Figure 6.2 shows the Delegation of Control Wizard. You can only use the wizard to give additional permissions, not to take them away. To take away control, you need to modify the appropriate DACLs manually.

![Delegation of Control Wizard](image)

**Figure 6.2** The Delegation of Control Wizard focuses on the tasks being delegated and sets the DACLs automatically.

You can use the Delegation of Control Wizard to add tasks that a user is delegated to perform, not to take away control. To remove control, you need to modify the DACLs manually.

### Analyzing Auditing Requirements

As mentioned previously, you are responsible for controlling access to all data on your network. Some data is not confidential or sensitive and is simply the information that is exchanged in day-to-day business in an organization. Other data might be more private or even confidential, as we discussed in Chapter 1, “Creating the Conceptual Design for Network Infrastructure Security.” You need to prevent unauthorized access to confidential and private data by assigning permissions only to the appropriate individuals. We discuss strategies for assigning permissions in the section titled “Designing an Access Control Strategy for Files and Folders” later in this chapter. In addition, you need to create an audit policy to ensure that you know and can prove who has accessed the servers, folders, and files that contain the confidential or private data.
Your audit policy can contain entries to record the success and/or failure of gaining access to any file, folder, or server on your network. Although auditing successes might be helpful to prove that a user has breached your security, auditing failures is actually more proactive because you might discover attempts to breach your security before a security breach has actually occurred. All audit results are recorded in the security log of Event Viewer.

You need to understand that you cannot audit everything because it isn’t practical from a resource standpoint. Auditing consumes resources, such as processor and memory, and reviewing audit logs takes time. Therefore, you need to set your audit policy based on your own experience and understanding of the security needs of your own network.

You can set the audit policy for a computer through the Local Security Policy settings on that computer, or you can control multiple computers on your network using Group Policy. You need to be familiar with the following audit policy settings that relate to directory services:

➤ Account logon events
➤ Account management
➤ Directory service access
➤ Logon events
➤ Policy change
➤ Privilege use

**Account Logon Events**
This setting only applies to domain controllers. It audits the computer’s validation of a user account that was logging on from another computer. You need to apply this setting on domain controllers if you suspect that individuals other than valid users are gaining access or attempting to gain access to your network.

**Account Management**
Account management audits each event in which a user account or group is created, renamed, disabled, enabled, deleted, or changed. In addition, it audits user password changes. You can apply this setting to an individual computer or to a group of computers using Group Policy. You need to apply this setting if you suspect that invalid accounts are being created or accounts are being tampered with on your network.
Directory Service Access
This setting combines with the individual setting on an Active Directory object. If you select this setting, the system will examine each object’s system access control list (SACL) to determine what auditing is required. You need to use this setting for specific auditing of a particular object or group of objects.

Logon Events
Logon events apply to the local logon on the computer to which the policy is applied. You need to apply this setting if you feel that a user is inappropriately logging on to a computer and gaining access to data and information.

Policy Change
This setting determines whether you will audit any changes to user rights assignment policies, audit policies, or trust policies. You need to apply this setting if you feel that a delegated administrator is attempting to change or is changing the policies that you have created.

Privilege Use
Privilege use applies to a user exercising a user right. You only need to audit this setting if you feel that a user is exceeding his given rights. In that case, you might want to apply the setting to a specific container using Group Policy or to a specific suspected user. This setting generates a large amount of data because the users are given many rights on a typical network.

Designing an Appropriate Group Strategy for Accessing Resources
As a general rule, you need to avoid assigning permissions to individual users for each of the resources that they use. Instead, assign permissions to groups of users. In the long term, this method saves you time and makes troubleshooting permissions much easier. The type of groups that you can use to assign permissions depends upon whether the user accounts are located on a computer or in the Active Directory of a domain. For domain accounts, your choice of groups also depends on the functional level of the domain.

In most cases, with accounts located on a single computer in a workgroup, you simply place the user account into a Local group that exists only on that computer and give the Local group permissions for the resource. In this way,
the user account gains the permissions by being a member of the Local group. You can remember this method by the letter sequence of *ALP*, which translates to “Accounts go into Local groups and then the Local groups get Permissions.”

Assigning permissions for domain accounts in Active Directory is more complicated. First, the types of groups you can use depend on the functional level of the domain. Second, the strategy that you use in regard to groups depends on what you want to isolate and how you want to manage the groups. With domain accounts, in general, you can remember the sequence of *AGUDLP*, which translates to “Accounts go into Global groups, Global groups go into Universal groups, Universal groups go into Domain Local groups, and the Domain Local groups get the Permissions.” Figure 6.3 illustrates this concept.

![Diagram of group hierarchy]

*Figure 6.3* The acronym *AGUDLP* applies to domain account group permission assignments.

Let’s take a closer look at all of the types of groups that we can use and how and when we use them. You need to be familiar with the following domain group types:

- Global groups
- Domain Local groups
- Universal groups
Global Groups

Global groups are created in Active Directory of one domain but can be placed into Domain Local groups in any domain or into a Universal group. Global groups can contain users from the domain in which they are created. They can also contain other Global groups if the domain is in at least Windows 2000 native mode functional level. This is called nesting Global groups.

Domain Local Groups

Domain Local groups are created in the Active Directory of one domain and control access to a resource that is contained in that domain. Domain Local groups can contain users, but this is not recommended by Microsoft. Instead, Domain Local groups should contain only Global groups from any domain in an Active Directory forest and Universal groups if there are some domains that are in at least Windows 2000 native mode functional level.

Universal Groups

Universal groups can only be created on a domain controller that is in at least Windows 2000 native mode functional level. Universal groups are created in Active Directory but are not specific to any domain. Universal groups can, therefore, contain members from any domain and can be used to give access to a resource in any domain. Users can be members of Universal groups, but this is not recommended by Microsoft. Instead, Universal group membership should be restricted to Global groups and other Universal groups.

Designing a Permission Structure for Directory Service Objects

Windows Server 2003 servers are flexible in regard to the assignment of permissions for Active Directory objects. As we said before, every object is controllable as to what it can do to other objects and what other objects can do to it. Microsoft recommends best practices when assigning permissions to Active Directory objects. These best practices focus on the strengths of the system and are designed to provide the greatest security with the least effort. You need to be familiar with the following best practices for directory service access permissions:

➤ Avoid taking away the default permissions—Leave the default permissions in place and add to them, if necessary. Taking away default permissions can cause unexpected results.
➤ When delegating control, avoid granting Full Control—if you give a user Full Control, she can undo the configuration that you have carefully put into place. Instead, give her the minimum permissions that she needs to perform the tasks that you have assigned her.

➤ Remember the inheritance property and use it to your advantage—if you allow a user to control a container and everything within it, he also has control of anything within the containers that are within it. Each object, therefore, receives an ACE. The processing of all of the ACEs can eventually have a detrimental effect on network performance. Whenever possible, use the Apply Onto option (in Advanced settings of permissions) to control inheritance and to minimize the number of ACEs that apply to child objects.

➤ When possible, assign the same set of permissions to multiple objects—When multiple objects have identical access, the servers need to store only one instance of the ACL and can apply it to the multiple objects. If you change one thing about an ACL, you create a new ACL.

➤ Assign the rights on the broadest level possible without overassigning the rights—for example, use Create All Child Objects or Delete All Child Objects rather than specifying all of the object types.

➤ Delegate permissions to groups rather than to individuals—Use the AGU DL P principle and assign the permissions to a group, and then make the user a member of the group.

Designing an Access Control Strategy for Files and Folders

The information that people use on computers is contained in the files and folders that are available to them. Some of these files and folders are created by the users themselves, whereas others are created for them by someone else. The users on your network have the right to expect that the files and folders that they use are safe based on the security policies of your organization. It’s your responsibility to create a file and folder structure that provides the security that the users expect, while allowing them to access the files and folders that they need. Windows Server 2003 has built-in tools to help you manage the security of files and folders. Your access control strategy should address the following elements of security for files and folders:
➤ Designing a strategy for the encryption and decryption of files and folders
➤ Designing a permission structure for files and folders
➤ Designing security for a backup and recovery strategy
➤ Analyzing auditing requirements

Designing a Strategy for the Encryption and Decryption of Files and Folders

Windows Server 2003 has a built-in encryption mechanism called Encrypting File System (EFS). This mechanism can be used on all volumes that are formatted with NTFS. EFS uses a system of public and private key cryptography and, therefore, requires an enterprise certificate server that is set to autoenroll the certificates, as discussed in Chapter 2, “Creating the Logical Design for Network Infrastructure Security.”

EFS should always be thoroughly tested in a lab or small group before deploying it to a production environment.

A user can encrypt files and folders simply by changing the attribute of the file or folder in the Advanced section of the General tab of its properties, as shown in Figure 6.4. This automatically encrypts the file or folder with a symmetric key and then encrypts the symmetric key (the decryption key) with the user’s public key and a designated Recovery Agent’s public key. With this in place, only the user's private key or the Recovery Agent's private key decrypts the decryption key, which can then be used to decrypt the file. Typically, the designated Recovery Agent is the administrator of the network. In Windows 2000 Server, the original administrative account for a domain was, by default, the Recovery Agent. In Windows Server 2003, there is no default Recovery Agent. You can set the designated Recovery Agent in Group Policy.

Windows Server 2003 has no default Recovery Agent for a domain. You can set a Recovery Agent using Group Policy.
As you can see, this system is quite complex from an administrative standpoint but is transparent to the user. You should consider using EFS on any removable drives or portable computers. It is the only type of defense that remains in place if you lose physical control of a hard drive. Without EFS, an attacker could simply take administrative control of the computer and read the information.

With Windows Server 2003 and Windows XP, you can assign multiple users to the same encrypted file or folder and give them access to it at a remote server. You need to keep in mind that the transmission of the data from the server to the client is not encrypted. To maintain encryption during transmission of the file or folder, you need to use Internet Protocol Security (IPSec), as discussed in Chapter 4, “Creating the Physical Design for Network Infrastructure Security.”

If the user’s key becomes corrupt and fails to decrypt the file or folder, the Recovery Agent can decrypt the file or folder and return the information to the user. The file or folder to be decrypted must be on the same computer as the key used to encrypt it. You can either take the encrypted file to the Recovery Agent’s computer or export the Recovery Agent’s key to a floppy disk and use it on the computer where the file exists. You can also export the Recovery Agent’s key from the network and store it on a floppy disk in a secure location. That way, an attacker cannot possibly gain access to the key over the network.

An attacker could take administrative control over a lost or stolen laptop by simply reinstalling the operating system and making himself the administrator. The attacker would then have access to all files and folders on which no encryption has been used. EFS prevents an attacker from viewing encrypted files and folders, even if he takes administrative control.
Microsoft recommends encrypting a folder, such as the My Documents folder, and then storing the files that you want encrypted in that folder. Any files that are moved or copied to an encrypted folder become encrypted, regardless of whether they are moved from the same volume or from a different volume. However, should you decrypt a file or folder that is already in an encrypted file or folder, that folder remains decrypted until you explicitly encrypt it again. To avoid this confusion, simply encrypt the parent folder and then move the files and folders (that you want to encrypt) into the parent folder.

**Designing a Permission Structure for Files and Folders**

Although your users might all share the same physical volumes to store their data, they still have the expectation that the files and folders are secure. You provide this security using the file systems built in to Windows Server 2003. You can control two types of permissions—shares and NTFS. You need to be familiar with both types, and you need to understand how to combine the two types for expected effective permissions.

As mentioned previously, a user can obtain permissions for an object based on groups of which he is a member. Windows Server 2003 includes a new tool to assist you in determining effective permissions when a user has NTFS permissions from multiple sources. You need to be familiar with the following in regard to permissions structure for files and folders:

- Share permissions for files and folders
- NTFS permissions for folders
- NTFS permissions for files
- Effective permissions

**Share Permissions for Files and Folders**

Share permissions allow a user to gain access to a resource through the network. If a file or folder is not shared, the only access to that file or folder would be from the local computer where the file exists. The following are levels of share permissions:

- **Read**—This is the default permission for any file that is shared in Windows Server 2003. With Read permissions, a user can see a file or folder and can execute the file or open the folder. A user can also
right-click the file or folder and view the properties, but cannot make any changes to the file or folder or to its properties.

➤ **Change**—Change permissions allow all of the permissions of Read, but the user can also change or add to the file or folder and can change the properties of the file or folder, such as the name or other attributes. In addition, the user can also delete the file or folder with Change permissions.

➤ **Full Control**—Full Control permissions allow all of the permissions of Change, and the user can take ownership of the file or folder and, thereby, assign other users permission for the file or folder.

### NTFS Permissions for Folders

The following are NTFS permissions for folders:

➤ **List Folder Contents**—A user with List Folder Contents permissions can view a folder and view the files and folders within the folder, but cannot change the folder or its attributes or even view the attributes of the folder. If he were to right-click the file and click Properties, he would get an Access Denied message.

➤ **Read**—A user with Read permissions for the folder can view the folder, but cannot view the contents of the folder. In addition, he cannot change the folder or its properties. He can view the properties of the folder by right-clicking the folder and clicking Properties.

➤ **Read & Execute**—A user with Read & Execute permissions has all of the same permissions as a user with Read permissions, and he can double-click the folder and view its contents.

➤ **Write**—A user with Write permissions has all of the same permissions as the Read & Execute permissions, and he can add files or folders to the folder. Whether he can delete files or folders from the folder depends on the individual permissions of the files or folders within the folder. He cannot delete the folder itself, but he can change its properties.

➤ **Modify**—A user who has Modify permissions to a folder has all of the permissions of Write, and he can delete the folder.

➤ **Full Control**—A user who has Full Control permissions has all of the permissions of Modify, and he can take ownership of the folder and, thereby, assign other users permission to the folder.
NTFS Permissions for Files

The following are NTFS permissions for files:

➤ **Read**—A user who has only Read permissions for a file can view the file, but cannot change, delete, or execute the file.

➤ **Read & Execute**—A user who has Read & Execute permissions can view the file and double-click the file to execute it. He cannot change or delete the file.

➤ **Write**—A user who has Write permissions can view the file and execute it, and can change the file and its properties. He cannot delete the file.

➤ **Modify**—A user who has Modify permissions has all of the same permissions as Write, and he can delete the file.

➤ **Full Control**—A user who has Full Control permissions has all of the same permissions of Modify, and he can take ownership of the file and, thereby, assign permissions to other users.

In addition to the standard NTFS permissions for files and folders, you can also select Special Permission in the Advanced security properties of the file or folder. Special permissions allow you to tailor the specific actions that a user is allowed to perform on a file or folder.

Effective Permissions

If a file or folder exists on an NTFS volume and is also shared through the network, the share permissions might be different than the NTFS permissions for the file or folder. In addition, if a user has permissions to the file from membership in multiple groups, the permissions might differ by group. The effective permissions are, therefore, a combination of all of the separate permissions. You need to remember this three-step method of determining the effective permissions for a resource:

1. Combine all of the share permissions.
2. Combine all of the NTFS permissions.
3. The effective permissions are the combination that is the most restrictive.

A combination that includes NTFS Deny permissions always overrides and results in permissions being denied. A combination that includes share Deny permissions results in permissions being denied unless the user is logging on locally to the resource, in which case the share permissions would not apply.
Windows Server 2003 contains a new tool called the Effective Permissions tool. This tool automatically combines the NTFS permissions for a resource. You only need to select the resource and then select the user on which you want to determine the effective permissions. This tool only combines the NTFS permissions and does not take share permissions into account. It is only accurate if the combined share permissions are of the same restriction or less restrictive than the share permissions. Figure 6.5 illustrates the Effective Permissions tool.

![Figure 6.5](image)

You can use the Effective Permissions tool to determine the effective NTFS permissions.

## Designing Security for a Backup and Recovery Strategy

An organized schedule of backups is an essential element in any network design. Windows Server 2003 has a built-in backup utility that can assist you in creating normal, incremental, and differential backups. You can also use third-party backup tools to provide more flexibility for backups.

Windows Server 2003 has a new tool that assists you in recovering data on your servers. This new tool is referred to as *Volume Shadow Copy service*. You need to be familiar with the Volume Shadow Copy service and its potential effect on the productivity of your users.

Although volume shadow copies are not a replacement for performing regular backups on a system, they are an effective enhancement to the security of data. Volume shadow copies are multiple versions of files on a file server that are automatically stored based on a schedule that you set. They are categorized by time. You can enable the Volume Shadow Copies features in the properties of an NTFS volume, as shown in Figure 6.6. They are not full copies of each
file version, but rather just the changes from the previous version. This system is used to conserve hard disk space while providing a backup of each version. You can set the schedule for the copies, but Microsoft recommends that you set it for no more than once per hour.

![Local Disk (C) Properties](image)

**Figure 6.6** You can enable the system to keep multiple shadow copies of a file sorted by time created.

If a user accidentally modifies a file in such a way as to lose some of the information in the file, he can use volume shadow copies to obtain a previous version of the file. This can save the user a tremendous amount of time and, thereby, increase productivity.

**Volume Shadow Copies to the Rescue**

Let's pretend that you are a user who has been working on a PowerPoint presentation for weeks, and your presentation now includes more than 500 slides. You want to send a “mini version” of your presentation to another user for her opinion, so you delete 475 slides, intending to save the remainder of the slides as a new file. However, you accidentally click Save instead of Save As and you have now lost your original file and 475 slides!

Without volume shadow copies, your options would be quite limited at this point. You could either ask the network administrator to restore the file from backup tape, or you could begin recreating the 475 slides that you deleted.

With volume shadow copies (and a little training), you simply right-click the file that you still have and then select the Previous Versions tab of the file’s properties. You then select the version of the file that you had a couple of hours ago before you made your mistake. Your file would return and life would go back to normal. It's as simple as that.
Analyzing Auditing Requirements

You need to be selective when auditing anything on a computer. Remember that auditing consumes resources. Furthermore, if you audit too much, the review of the security logs consumes a tremendous amount of human resources. Having said that, you can audit specific files and folders to determine who is accessing or changing information in them. Remember that all auditing is local; therefore, you have to set the auditing policy on the computer on which you want the auditing to occur. This can be accomplished through the Local Security Policy settings on the computer or through Group Policy, as shown in Figure 6.7.

![Figure 6.7](image)

**Figure 6.7** You can set the audit policy for a computer through the Local Security Policy settings of the computer itself or through Group Policy.

You need to be familiar with the following settings in regard to auditing files and folders:

- Auditing object access
- Setting auditing entries on the resource

**Auditing Object Access**

This setting combines with the individual audit setting on the SACL of the file, folder, Registry key, or other resource on which you have applied audit settings. If you select this setting, the system examines the SACLs of all resources to determine whether auditing is required.
**Setting Auditing Entries on the Resource**

After you have set the audit policy to Audit Object Access, you can then set the resources themselves to be audited. You can determine which users or groups you will audit for each resource. In this way, you can create an audit report that gives you the information that you need without having so much information so as to become unusable.

You can set the audit entries in the Advanced options of the Security tab for the object to be audited, as shown in Figure 6.8. This creates a SACL that the system automatically tracks and uses to create the entries for you in the security log of Event Viewer. If you choose, you can audit an entire hierarchy of folders by allowing the audit entries to propagate from the parent object to the child objects.

![Figure 6.8](image)

**Figure 6.8**  You can set audit entries in the Advanced options of the Security tab.

## Designing an Access Control Strategy for the Registry

By default, only administrators have permissions to view or change the Registry. You can assign permissions to each of the *keys* in the Registry to allow certain users to make changes to the keys. You can also use the system to audit the Registry to determine which users have made changes or even attempted to make changes to the Registry. Your access control strategy for the Registry should include the following:
➤ Designing a permission structure for Registry objects
➤ Analyzing auditing requirements

Designing a Permission Structure for Registry Objects

In Windows Server 2003, all system information is centrally located in the Registry. The information is stored in containers called keys. The two main keys are HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE. One incorrect edit to the information contained in these keys can potentially disable the operating system. For this reason, only administrators should have access to the Registry on most computers. Users indirectly make changes to the Registry when they use GUI tools, such as Control Panel or Display Settings. These changes are much safer than changes made directly to the Registry.

Some applications and some hardware require a Registry edit to function properly. You might want to allow certain users to make the changes to the Registry so that you don’t have to make them every time. If you choose to allow a user to make changes to the Registry, you need to ensure that he has the training and the knowledge to make the changes correctly.

You can assign permissions on each key of the Registry in much the same way that you assign permissions to files or folders. To do so, access the Registry using the regedit32.exe or regedit.exe tool, right-click the key that you want to change, and click Permissions. The Permissions dialog box opens, as shown in Figure 6.9. You can then add a user and give him the permissions required to make the change. As always, you should only give him the minimum level of permissions required to make the appropriate changes. You can also use Group Policy to assign permissions to multiple users and computers at the same time.

You should rarely need to give a user Full Control permissions on a Registry key.

Analyzing Auditing Requirements

You only need to audit the Registry if you feel that someone is making changes to it without your approval. If troubleshooting a problem seems to indicate that a change was made to the Registry that could not have been
made by another tool and could not have been made by accident, auditing the Registry is in order. In this case, you should audit the specific key where the change was made. You can set the auditing for the key in the Advanced section of the permissions for the key, as shown in Figure 6.10. In this case, you might want to audit the Everyone group for access to the Registry key because the list should not be large and because you want to ensure that everyone is included in the audit.

Figure 6.9  You can set permissions for each key in the Registry.

Figure 6.10  You can set audit entries in Advanced Security Settings for each key in the Registry.
Exam Prep Questions

Answer the questions for the following case study based on the information provided in the case study.

Case 1: HACA Inc.

HACA Inc. is a large retail outlet with 75 chain stores located throughout the United States. HACA has recent concerns over the local security of the networks in each of its stores. Currently, the only administration performed on any of the computers is remote administration from the corporate offices in Birmingham, Alabama. HACA is considering allowing some managers to perform some administration because they are closer to the situation and know more about the local needs of the store. As part of this change, the company wants to review all policies in regard to permissions and auditing of all network resources. The managers might also be asked to review the security logs on a set schedule. HACA has hired you as an independent consultant.

Question 1

Which delegation tool should HACA use to focus on the task to be delegated and let the system set the DACLs?

- A. Active Directory Users and Computers
- B. regedit.exe
- C. Delegation of Control Wizard
- D. Advanced permissions

Answer C is correct. The Delegation of Control Wizard focuses on the task itself and sets the DACLs to the appropriate setting. Active Directory Users and Computers is not a delegation tool; therefore, answer A is incorrect. regedit.exe is a tool you can use to edit the Registry; therefore, answer B is incorrect. Advanced permissions would focus on the DACLs themselves; therefore, answer D is incorrect.
Question 2

Which tools can you use to control the audit policy on computers on your network? (Choose two.)

- A. Local Security
- B. Group Policy
- C. Advanced permission settings
- D. Event Viewer

Answers A and B are correct. All auditing is local and should be set on the local computer, but this can be accomplished through the Local Security tool on the computer or through Group Policy. Advanced permission settings control the creation of the SACL used to audit the objects themselves, not the audit policy; therefore, answer C is incorrect. Event Viewer is a tool that you can use to view the security log for the results of a security audit; therefore, answer D is incorrect.

Question 3

Which audit setting tracks local logons on a computer?

- A. Logon events
- B. Directory service access
- C. Account logon events
- D. Privilege use

Answer A is correct. Logon events tracks local logons on a computer to which it is applied. Directory service access tracks the viewing and changing of specific Active Directory objects to which SACLs are applied; therefore, answer B is incorrect. Account logon events is applied on domain controllers to track their authorization of users who log on from other computers on the network; therefore, answer C is incorrect. Privilege use tracks the actions of a user exercising a user right; therefore, answer D is incorrect.
Question 4

Which of the following are Microsoft recommendations for directory service access permissions? (Choose two.)

- A. Remove the default permissions when assigning specific permissions.
- B. Use the settings with the broadest permissions possible without overassigning.
- C. When possible, assign the same set of permissions to multiple objects.
- D. Assign Full Control permissions whenever possible.

Answers B and C are correct. Using settings with broader permissions makes it easier for the system to process the permissions. Using the same settings for multiple objects creates less DACLS and makes it easier on the system as a result. You should avoid removing the default permissions as this could have unexpected results; therefore, answer A is incorrect. You should avoid assigning Full Control because it allows the person with delegated permissions to change your permission configurations; therefore, answer D is incorrect.

Question 5

Which type of group is named for the resource and must be contained in the same domain as the resource?

- A. Global
- B. Domain Local
- C. Universal
- D. Nested

Answer B is correct. A Domain Local group is created to give access to a resource. It is, therefore, named for the resource and must be contained in the same domain as the resource. Global groups are created to contain users and other Global groups. They are generally named for the function of the user and must be contained in the same domain as their members; therefore, answer A is incorrect. Universal groups are created in the Active Directory of a domain that is in at least Windows 2000 native mode. They are generally named for the overall function of the members to be contained in them; therefore, answer C is incorrect. Nested is not a type of group. A group is said to be nested if it is contained within another group; therefore, answer D is incorrect.
Question 6

Which permission are only NTFS permissions and not share permissions? (Choose two.)

- A. List Folder Contents
- B. Change
- C. Read & Execute
- D. Full Control

Answers A and C are correct. NTFS permissions include List Folder Contents, Read, Read & Execute, Write, Modify, Full Control, and Special Permissions. Change is a type of share permission; therefore, answer B is incorrect. Full Control permissions allow a user to take ownership and are common to shares and NTFS; therefore, answer D is incorrect.

Question 7

Which NTFS permissions allow a user to change a file or folder but do not allow a user to delete the file or folder?

- A. Modify
- B. Write
- C. Change
- D. Read & Execute

Answer B is correct. Write permissions to a file or folder allow a user to change the file or folder but do not allow him to delete it. Modify permissions are NTFS permissions that allow a user to delete a file or folder; therefore, answer A is incorrect. Change permissions are share permissions that allow a user to delete a file or folder; therefore, answer C is incorrect. Read & Execute are NTFS permissions that do not allow a user to change a file or folder; therefore, answer D is incorrect.
Question 8

Which two of the following are part of the three steps to determine effective permissions?

- A. Determine the most restrictive of all permissions.
- B. Combine the NTFS permissions.
- C. Determine the least restrictive of all permissions.
- D. Combine the share permissions.

Answers B and D are correct. You should first combine the share permissions and determine a result. Next, you should combine the NTFS permissions and determine a result. The effective permissions will then be the most restrictive of the two results. Determining the most restrictive of all of the permissions is not one of the steps; therefore, answer A is incorrect. Determining the least restrictive of all of the permissions is not one of the steps; therefore, answer C is incorrect.

Question 9

Which of the following is true about volume shadow copies?

- A. They are full copies of a file that are stored multiple times.
- B. They are automatically copied every 5 minutes.
- C. They replace the need to back up your servers.
- D. They can only be created on NTFS volumes.

Answer D is correct. Volume shadow copies can only be created on NTFS volumes. Volume shadow copies consist of a file and the “shadows” representing only the changes to the file, not full copies of the file; therefore, answer A is incorrect. Volume shadow copies are created on a schedule set by the administrator. The default schedule is twice per day at 7:00 a.m. and 12:00 p.m.; therefore, answer B is incorrect. Volume shadow copies do not replace the need to back up servers; therefore, answer C is incorrect.
Question 10

Which of the following are true regarding the Registry? (Choose two.)

- A. The only way to change the Registry is with the Registry Editor tool.
- B. Users cannot usually make any changes to the Registry.
- C. You should audit the Registry only when you feel that it has been attacked.
- D. By default, only the administrator of a computer has the right to make changes directly to the Registry settings of that computer.

Answers C and D are correct. You only need to audit the Registry when you feel that it has been attacked because auditing consumes system resources and reviewing the audits takes time. The administrator of a computer is, by default, the only account that has the right to make changes to the Registry of that computer. The Registry can be changed indirectly by users with the GUI tools; therefore, answers A and B are incorrect.