



realtimepublishers.comtm

The Administrator Shortcut Guidetm To



Active Directory Security

SCRIPTLOGIC

*Derek Melber, Dave Kearns,
and Beth Sheresh*

Chapter 4: Delegating Administrative Control	68
Data Administration	69
Delegating GPO Administration to Data Administrators	69
Delegating Object Creation Administration to Data Administrators.....	69
Categories and Roles of Data Management Delegation	70
Account Administrator.....	70
Workstation Administrator	70
Server Operators	70
Resource Administrator	70
Security Group Administrator.....	71
Help Desk Operators.....	71
Application-Specific Administrator.....	71
How to Delegate Data Administration.....	71
Service Administration	72
Categories and Roles of Service Management Delegation.....	72
Service Administration Groups and Privileges.....	73
Forest Configuration Operators	73
Domain Configuration Operators	73
Security Policy Administrators.....	73
Service Administration Managers.....	74
Domain Controller Administrators	74
Replication Management Administrators	74
DNS Administrators.....	74
How to Delegate Service Administration	75
Best Practices	75
Delegation Needs to Be Structured and Logical.....	76
Delegate Around Roles.....	76
Delegation Model.....	76
Best Practice Implementation	77
Logging, Monitoring, and Auditing.....	77
Logging.....	77
Monitoring	78
Auditing	79

Delegation Tools.....79

 Delegation of Control Wizard.....80

 Active Directory Users and Computers81

 AD Sites and Services.....81

 ACL Editor.....82

 Ldp.exe.....85

 Dscls.exe85

 Acldiag.exe85

 Dsrevoke.exe.....85

Summary.....86

Copyright Statement

© 2004 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimerepublishers.com and the Realtimerepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimerepublishers.com, please contact us via e-mail at info@realtimerepublishers.com.

Chapter 4: Delegating Administrative Control

Delegation of administrative control might be the sole reason you moved from your old directory service to AD. Many want to move to AD to take advantage of the efficiency, security, scalability, and ROI that delegation provides. The ability to provide detailed task privileges to all areas of the IT staff, as well as to non-IT professionals, is why delegation is so useful.

There are many tasks that can be delegated within AD, but they can all be broken down into two categories: data administration and service administration. Data administrators control the resources that are stored in AD, such as user, group, and computer accounts. They also control member servers and the resources that reside on these computers. The administrative responsibilities that are associated with these tasks are broken down into categories to help organize the delegation that must occur to get all of the tasks done. Once the categories are created and the AD design finalized to include data administration, the delegation of these tasks can be completed. Delegation of data administration is provided within AD by giving data administrative groups permission over the objects that they will control.

Service administration and the delegation of the related tasks differ greatly from data administration. Service administration controls the directory service, ensuring it is configured properly, available, and stable. Service administration is typically delegated by adding user accounts to existing groups that already have privileges to control aspects of AD administration. These groups and additional groups are configured with user rights on domain controllers to give them additional delegated privileges. These delegated tasks are assigned from categories that organize the different AD administration tasks necessary to keep AD running.

You must begin delegating within AD early in the directory implementation. This best practice is one of many that you will be introduced to with regard to delegation of administration in AD. This chapter will also explore additional AD delegation best practices in areas such as logical and structured designs, the use of roles, and a clear understanding of your delegation model.

Once the delegation is implemented, the job is not done. You will still need to monitor and control the delegation for the production environment. This task typically can be broken down into three areas: logging, monitoring, and auditing. Each area is critical to ensuring that security within AD is maintained. Finally, we will take a look at tools that can help you complete your delegation within AD.

Data Administration

Data administration is not only the administration of data—it entails almost every delegation aspect outside of supporting the directory service itself. Data administration includes the following responsibilities:

- Creation of user, group, and computer accounts
- Assignment of user rights to user and group accounts
- Management of group membership
- Management of resources (data, application, and services) on member servers
- Management of client computers

The common thread among all of these responsibilities is controlling privilege access to a resource. In some cases, the resource is a file and in other cases the resource might be an entire server. Regardless, the structure of allowing, or delegating, these responsibilities must be designed, implemented, and maintained.

Delegating GPO Administration to Data Administrators

Data administrators are responsible for clients and servers, so there is the potential for them to control GPOs, which offer an ideal means of controlling all computers in the domain for security and configuration settings. As we have seen, GPOs provide control that is targeted and final. However, should a data administrator have control over GPOs that are targeted to clients and servers? This question can only be answered by the individual company and IT department. Take caution when considering this decision as you are giving data administrators a great deal of power when you give them control of a GPO.

GPOs can control security permissions on the target computer, group membership on the target computer, security settings, and much more. If a data administrator is delegated control to create, link, and edit GPOs, there is nothing that administrator can't do with or to the target computer. Also, if there are any user accounts in the OUs to which the data administrator has been delegated privilege, the administrator will also have control over these user accounts on the network. Ideally, you will not give any data administrator the ability to create or edit GPOs, instead delegating only the ability to link a GPO to an OU.

Delegating Object Creation Administration to Data Administrators

It is a common delegation to provide data administrators with the ability to create objects, such as user and group accounts. However, it is often overlooked that once this delegated privilege is given to a user, the user has full control over that object because the user owns the object (as with files and folders, the user that creates an AD object becomes the owner of the object). Thus, if you do want users to have full control access over the objects in AD, do not provide them with the ability to create the object. Alternatively, you can implement a process to change object ownership once an object has been created by a user.

Categories and Roles of Data Management Delegation

As you think about the overall design of data management delegation, consider the myriad options that you have available. The following lengthy list highlights data management categories and the delegation responsibilities that might fall under each role:

Account Administrator

- Create user accounts
- Delete user accounts
- Move user accounts
- Reset a user's password
- Unlock user accounts
- Modify user account properties
- Authorize access to user and group accounts
- Link GPOs to user account OUs

Workstation Administrator

- Create computer accounts
- Link GPOs to computer account OUs
- Have membership in local Administrators group
- Have permission to control workstation remotely

Server Operators

- Create computer accounts
- Link GPOs to computer account OUs
- Have membership in local Administrators group
- Have permission to control server remotely

Resource Administrator

- Control access to data
- Control service and service account on server
- Control application on server

Security Group Administrator

- Create security groups
- Modify the membership of security groups
- Delete security groups

Help Desk Operators

- Reset passwords on user accounts
- Unlock user accounts
- Control non-security-related user account properties

Application-Specific Administrator

- Control services and service accounts
- Modify the membership of security groups
- Have membership in local Administrators group

How to Delegate Data Administration

It is ideal to delegate data administration at the OU level, which allows for the greatest control over who is able to delegate and which objects a user can control. As a guideline for the data administration delegation process, the following list suggests steps that will need to be performed for every delegation that occurs within AD related to data administration:

1. Implement OUs based on the specific data administration model that was designed.
2. Move user, group, and computer accounts into the proper OUs.
3. Create groups that will be used for the delegation process. For example, you might create a group named Sales_PW_Reset that will be used to reset passwords for Sales employees.
4. Add the user accounts to the groups that were created for delegation.
5. Configure delegation for all groups based on the data administration design model that you developed. (You can use any number of tools for this procedure, as we will explore later in this chapter.)

After you delegate administrative privileges to users in the environment, you will need to provide them with tools so that they can perform administrative tasks. The preferred tool for administering user and group accounts is the Microsoft Management Console (MMC) Active Directory Users and Computers console. This tool can be installed on client computers by installing the Adminpak, which is on the server installation media as well as under the system files on any domain controller.

Another option is to create Taskpads, which are individual tasks created from the original Active Directory Users and Computers console but have a narrow scope to control what the user has access to. These Taskpads are discussed in more detail in Chapter 2.

Service Administration

Service administrators configure and manage AD and domain controllers, ensuring the directory service is functional and available. They have privileges that can cross domain boundaries, with the forest acting as the security boundary. Service administrators can act as data administrators, but data administrators cannot perform directory service administrative tasks. The overall mission of the service administrator is to make sure AD is running smoothly and efficiently.

With the scope of the service administrator controlling such important aspects of the company and network, there should be very few service administrators for any given task. Some companies have a team of 5 to 10 IT professionals that control service administration tasks, which allows for separation of duties as well as coverage in case an employee leaves or is promoted out of the role.

Categories and Roles of Service Management Delegation

Service management delegation is slightly more complex than data management delegation. Service administration tasks have greater ramifications if performed incorrectly and the AD configurations can be more difficult. The following lengthy list highlights service management categories and the delegation responsibilities that might fall under each role.

- Installation management—This role's tasks include the installation of new domains and domain controllers for the existing AD infrastructure as well as for the overall network
- Schema management—This role's tasks include control over any and all schema changes, modifications, additions, or considerations—involving not only direct changes to the schema but also to applications that extend the schema
- Trust management—This role's tasks include control over all trusts that can be created within or outside of the AD infrastructure (cross-link, Windows external, Kerberos external, and cross-forest trusts are included)
- Operations master roles management—This role's tasks include management of all the operations master roles in the entire forest and the roles in each domain; involves moving and seizing the roles between domain controllers
- Backup and restore management—Specific to the domain controllers and the AD database, this role's tasks include the backup of the system state, Sysvol, and all policies and logon scripts associated with the AD enterprise
- LDAP policy management—If there are any LDAP policies, this role is responsible for the creation and management of the policies and what the policies control
- Replication management—This role's tasks involve all functions related to the replication of AD, GPOs, logon scripts, and Dfs data
- Functional level management—This role's tasks include the control over the functional level at both the domain and forest level and the associated details that control this behavior
- Directory database management—This role's tasks include the optimization, security, location, and recovery of the AD database and the associated files to keep AD up and running

- Security policy management—This role focuses on the two default GPOs at the domain and domain controller OU levels (primarily including the Account Policy settings and the user rights configuration for domain controllers)
- DNS management—With DNS playing such an integral part of AD and the location of resources, an entire role is dedicated to the administration of DNS; this role’s tasks involve the interaction of DNS with AD, security of DNS, and replication of DNS
- Domain controller management—This role’s tasks include the control over installation and configuration of the domain controllers, which involves the management of services, applications, and data that is stored on the domain controllers

Service Administration Groups and Privileges

Service administration is delegated by adding user accounts to administration groups. These groups have default privileges, but they can also be given additional privileges through user rights. The following list provides suggested service administration group models and their privileges:

Forest Configuration Operators

- Creating and deleting child domains
- Creating, deleting, and managing all trust relationships for the forest
- Creating, deleting, and managing cross-reference objects
- Transferring and seizing the forest-wide operations master roles
- Raising the forest functional level

Domain Configuration Operators

- Managing replica domain controllers
- Managing operations master roles
- Managing the default Domain Controllers OU
- Managing the content stored in the System container
- Restoring AD from backup when required

Security Policy Administrators

- Managing Password policy settings
- Managing Account Lockout settings
- Managing Kerberos Policy settings

Service Administration Managers

- Managing service administration user accounts
- Managing service administration security groups

Domain Controller Administrators

- Managing software
- Managing service packs and security updates
- Managing GPO settings, for both security and control
- Managing event logs
- Managing directory service files and Sysvol

Replication Management Administrators

- Managing sites
- Managing subnets
- Managing site links and site-link bridges
- Managing the replication schedule and replication interval on site links
- Managing manual site connections

DNS Administrators

- Installing the DNS Server service on domain controllers
- Managing and configuring DNS recursion methods
- Managing forest-wide zones
- Managing DNS application partitions

How to Delegate Service Administration

Like data administration delegation, service administration delegation needs to be considered early in the AD design process. Although some of the delegation can be achieved by group membership, service administration still requires some OUs for controlling group membership and other delegation tasks. The following is a suggested process for how to delegate your service administration:

1. Create an OU to place the security groups that represent the service administration roles.
2. Create new groups that will be used for each of the service administration roles (where a default administration group does not cover those responsibilities).
3. Add the appropriate security group to all resource ACLs to provide the group with the sufficient access to perform the administrative task (this might include additional permissions given to a group for system files and folders).
4. To allow the service administration group to perform their tasks, configure appropriate user rights on all domain controllers and servers that run directory service applications.
5. Configure delegation for all groups based on the service administration design model and roles that you developed. (You can use any number of tools for this procedure, as we will explore later in this chapter.)
6. Add the appropriate user accounts to the security groups for each role.

At this point in the process, you need to provide the appropriate tools to the service administrators.

Best Practices

What is a best practice? In this context, we are going to define a best practice as a suggestion or recommendation from a valued, experienced source. A best practice is something that can be quantified, based on experience and analysis. The best practices here are from years of experience with AD, security, and delegation. Any good delegation strategy or best practice must be based on structured and logical thought processes, including a methodology of separating and organizing the different tasks into categories that are easily tracked and understood. Both of these factors will be molded into a model, which can then be implemented. The implementation stage is just as important as the design phase because mistakes here result in security issues down the road. In the following sections, we cover all of these areas of best practice delegation.

Delegation Needs to Be Structured and Logical

When you develop the model for your delegation, it must be structured and logical so that it can be implemented and managed with ease. Best practices that you should follow as you develop your delegation model include:

- Have a good understanding of all aspects of AD management
- Understand the administrative needs of departments, applications, and services that are associated with the Windows network
- Ensure that the delegation model has multiple users controlling each administrative task
- Always work from the least privilege aspect of any task and add permissions and privileges on an as-needed basis

Delegate Around Roles

As you design the delegation model, consider using roles as the core structure for the administration task. Roles categorize the different tasks so that you can either provide full access to each task in a role or partial access to a few of the tasks. We have already broken down the data and service administration delegation options into roles. You can either use these roles or develop your own roles as a basis for your delegation model.

Delegation Model

As a best practice for delegation, you need to develop a delegation model. This model will be the underlying structure for your AD design and how the objects in AD are organized. You will need to consider all of the different aspects of how your company is organized, especially with regard to the IT administration staff. You will need to work this consideration into the delegation model. In the end, the delegation model will provide the foundation for the overall AD structure and specific delegation for data and service administration. A good delegation model will

- Make sure all aspects of data and service administration are covered
- Provide separation of duties and isolation of duties where needed
- Ensure that data and service administration tasks are equally divided among the users performing these tasks
- Ensure that the delegation for all tasks is implemented using the least-privilege concept
- Restrict delegated tasks to only a few individuals

Best Practice Implementation

As you deploy and implement the delegation, there are some best practice considerations that you should keep in mind. Some of these can cause more initial work, but the time that they save in the long run is well worth the initial effort. When you implement delegation, make sure you consider the following:

- Every data and service administration role is covered by a security group
- Do not use security groups that were designed for delegation for any other purpose (this includes ACL permissions, user rights, and GPO filtering not associated with delegation)
- For delegation management of AD objects such as user and group accounts, make sure you delegate at the OU level
- Avoid configuring delegated management at the individual user or group account level
- Delegate with limited access in mind; doing so will require using resources that specify delegation configurations and testing for your environment

Logging, Monitoring, and Auditing

It is foolish to design, implement, and manage delegation without some way of ensuring that the desired delegation is the actual resulting delegation. To do so, you can have different levels of checking on the delegation of AD administration. First, you can establish a log that tracks changes to delegation as well as the use of delegation privileges. Next, you can monitor, either manually or automatically, the activity that occurs as a result of delegation of tasks. Finally, an audit needs to be done to ensure that the documented delegation is the current delegation.

The following sections explore each of these areas to ensure that delegation at all steps in the process is covered and correct. If you are not satisfied with the built-in capabilities of the Windows OS with regard to these tasks, investigate tools from ScriptLogic, Aelita, NetPro, and BindView. These tools provide more robust and efficient solutions.

Logging

You can produce logs of delegation activity with the built-in logging feature of Windows. With this feature, you can track almost every activity that occurs to an object, service, or setting within the OS. Ideally, you will set up logging on the domain controllers to track when data administrators manage the objects contained in AD. If there are any servers that contain resources, you will also need to enable logging on those servers. For service administrators, you will primarily establish the logging only for the domain controllers, because these computers are the only servers that control AD.

The logging settings that need to be enabled to track delegation and the use of delegated privileges include:

- Account management—Tracks account management events that occur on the local SAM of servers and within AD
- Directory service access—Tracks when a user, group, or computer accesses an AD object; the object must also have auditing configured on the System Audit Control List (SACL), which is unique per object
- Object access—Tracks when a user, group, or computer accesses a resource; the resource must also have auditing configured on the SACL, which is unique per resource object (objects can include files, folders, registry keys, printers, and AD objects)
- Policy change—Tracks changes to user rights, audit policy, or trusts
- Privilege use—Tracks when a user performs a task that uses a user right on the computer
- System events—Tracks when the client is restarted or events that affect system security or the Security Log

To ensure consistent and persistent configuration of the logging settings, it is best to use GPOs to deploy these settings. For domain controllers, use a GPO linked to the Domain Controllers OU. For all other computers, create a new GPO, link it to the appropriate OU containing the computer accounts, then configure the audit policy settings in the GPO.

The logs generated from these settings are tracked in the Security Log of the Event Viewer. The security logs are kept in the log until they are archived or overwritten by newer events. Each OS configures the size of the security log differently, but it is a good idea to increase the size of this log to more than 10MB for domain controllers to ensure that all of the information is captured between archiving of the log. If there is a lot of traffic on the domain controller or there are numerous resources being tracked, it might be a good idea to increase the security log size to 50MB or more to ensure that no events are lost.

Monitoring

Once you have the logging and tracking established, you need to be made aware of when a critical event occurs. Even if the event is not logged, you still want to be made aware of the event occurring. Unfortunately, Microsoft does not have any such tool built-in to the Windows OS and really don't have many options that provide such monitoring. The Microsoft Operations Management (MOM) product provides some good monitoring over the OS; however, you might want to look at other tools that can provide you with more advanced monitoring capabilities over AD and the delegation that you have established over tasks.

When you evaluate your need for monitoring, you will need to consider the following features that some tools, none built-in, provide:

- Real-time monitoring
- Real-time alerting via email, phone calls, or pager messages
- Centralized management and storage of monitored events
- Documentation tracking of what was changed, when it was changed, and who changed it

Auditing

Once the logs have been established and there is a monitoring tool in place, auditing needs to be performed to make sure that nothing is missed. Also, auditing provides a process in which the events that are logged can be reviewed to find trends of security attacks or vulnerabilities. The first step to auditing is to create an audit trail. We have already discussed this step in the logging section earlier.

Employing a centralized tool is very beneficial when it comes to auditing. It can take days to track down the events from all of the domain controllers and servers in the organization. Tools such as EventCombMT from Microsoft can help, but this tool does not provide the efficient interface and query mechanisms that are really needed to ensure that a good audit can be performed on the event logs. Be sure to investigate tools from ScriptLogic, Aelita, NetPro, and BindView to help solve these issues.

Make sure that you also include the delegation audit. This audit includes the reporting of the delegation of administration on OUs and the membership in groups that you need to know in order to provide a good audit on delegation in AD. For these additional control checks, you will need to obtain a tool that allows you to efficiently list and organize ACLs of AD objects. You will then need to quickly access the membership of groups, especially those that were created specifically for delegation. Finally, you will need to audit the service administration default groups, which provide control over AD-related functions.

Delegation Tools

There are plenty of tools that can be used to help develop and report on the delegation of administration for AD and the objects in AD. It cannot be stressed enough how important it is to have the design of the delegation well thought out and implemented first. A poor delegation model is very difficult to administer regardless of the delegation tool.

Although there are plenty of tools that are available to help implement your delegation model in AD, we will explore the Delegation of Control Wizard, which is a free, built-in tool that is part of the Active Directory Users and Computers console. This tool offers many of the standard delegation tasks already configured for you to just click for an easy implementation. However, with many configurations required for a large organization and the need to report on the delegation that is in place, other tools are also needed to ensure successful delegation. The different tools that can be used to delegate administration in AD include:

- Delegation of Control Wizard
- ACL Editor
- Ldp.exe
- Dsacls.exe
- Acldiag.exe
- Dsrevoke.exe

We will discuss each tool and talk about their benefits and weaknesses. I must also stress that this is not an exhaustive list of tools that can be used for delegation of administration in AD. The tools not listed might provide a better solution because they offer GUI-based solutions, which can help with the overall implementation and reporting of the delegation in such a complex environment.

Delegation of Control Wizard

The Delegation of Control Wizard is built-in to the Active Directory Users and Computers console, where most of the administration of AD objects takes place. The wizard is designed to walk you through the decisions to configure the permissions on the objects in AD. Of course, the wizard is also designed to help configure the large number of permissions on objects in AD. The wizard will begin by asking questions about

- User or group to receive the delegation task
- Administrative task to be delegated
- Specific object type and property control (if standard administrative task is not selected)

When the wizard is finished asking questions, it configures the ACL on the object in which the wizard was initiated as well as down through the AD structure following the rules of inheritance that are configured for the objects being affected.

Although I have only mentioned that the Delegation of Control Wizard is available in the Active Directory Users and Computers console, it is also available to configure delegation to objects located in the AD Sites and Services console. In each AD tool, the Delegation of Control Wizard provides a default list of administrative tasks that configure the permissions on the objects automatically. These default administrative tasks differ slightly between Win2K Server and WS2K3 domain controllers, due to the updated list that the WS2K3 domain controllers provide. The following list summarizes the WS2K3 domain controller offerings of default administrative tasks in each AD tool:

Active Directory Users and Computers

- 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
- Generate Resultant Set of Policy (Planning)
- Generate Resultant Set of Policy (Logging)
- Create, delete, and manage inetOrgPerson accounts
- Reset inetOrgPerson passwords and force password change at next logon
- Read all inetOrgPerson information
- Join a computer to the domain (Domain node)
- Manage Group Policy links
- Create, delete, and manage WMI Filters

AD Sites and Services


- Manage Group Policy links

To use the Delegation of Control Wizard to delegate the resetting of passwords on an OU, you would follow these steps:

1. Right-click the OU and select Delegate Control, then click Next.
2. On the Users or Groups page, click Add.
3. On the Select Users, Computers, or Groups page, in the *Enter the object names to select* box, type the name of the user or security group to which you want to delegate tasks.
4. Click OK, then click Next.
5. On the Tasks to Delegate page, select the *Reset user passwords and force password change at next logon* check box.
6. Click Next, then click Finish.

This process will configure the needed permissions on the user accounts in the OU so that the configured users can reset the password and check the box to force the password to be changed when the user logs on again.

If an administrative task is not listed, yet you want to delegate that task to a user or group, you can create a custom task in the wizard. This task can be very daunting because there are literally hundreds of detailed permissions that can be set on any one object in AD. Rather than create a custom task, you can modify the underlying file that configures the default list of administrative tasks. This file, `Delegwiz.inf`, can be customized to include any set of permissions to make up an administrative task.

 For more information about how to complete this customization, refer to the Microsoft article “HOW TO: Customize the Task List in the Delegation Wizard” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;308404>.

As you can see, the Delegation of Control Wizard is easy to use and extremely efficient. However, there is one flaw with the tool. The tool can only “add” delegation permissions, it can’t remove permissions. We will look at other tools—such as ScriptLogic’s Active Administrator (AA)—that can report on and remove the delegated permissions if you have configured too much to a user or group.

ACL Editor

The ACL Editor is the rawest tool for establishing the delegation on an object in AD. The editor allows you to view, modify, and add the security configurations of objects in AD, just like you can for files and folders. The Delegation of Control Wizard is a GUI-based tool that performs this same task.

A benefit of the ACL Editor is the additional detailed configurations that can be made to the security description of the object. The permission that controls access to an object is just one of many settings associated with the overall security of an object. You can also configure the following security-related settings by using the ACL Editor:

- Security auditing—The SACL establishes which users or groups will be tracked in the Security Log when accessing the object. Figure 4.1 shows the SACL interface for a typical object in AD. The ability to track access to an AD object is essential to the overall delegation model, because it is the only way to track when a user fails or succeeds at modifying the objects in AD.

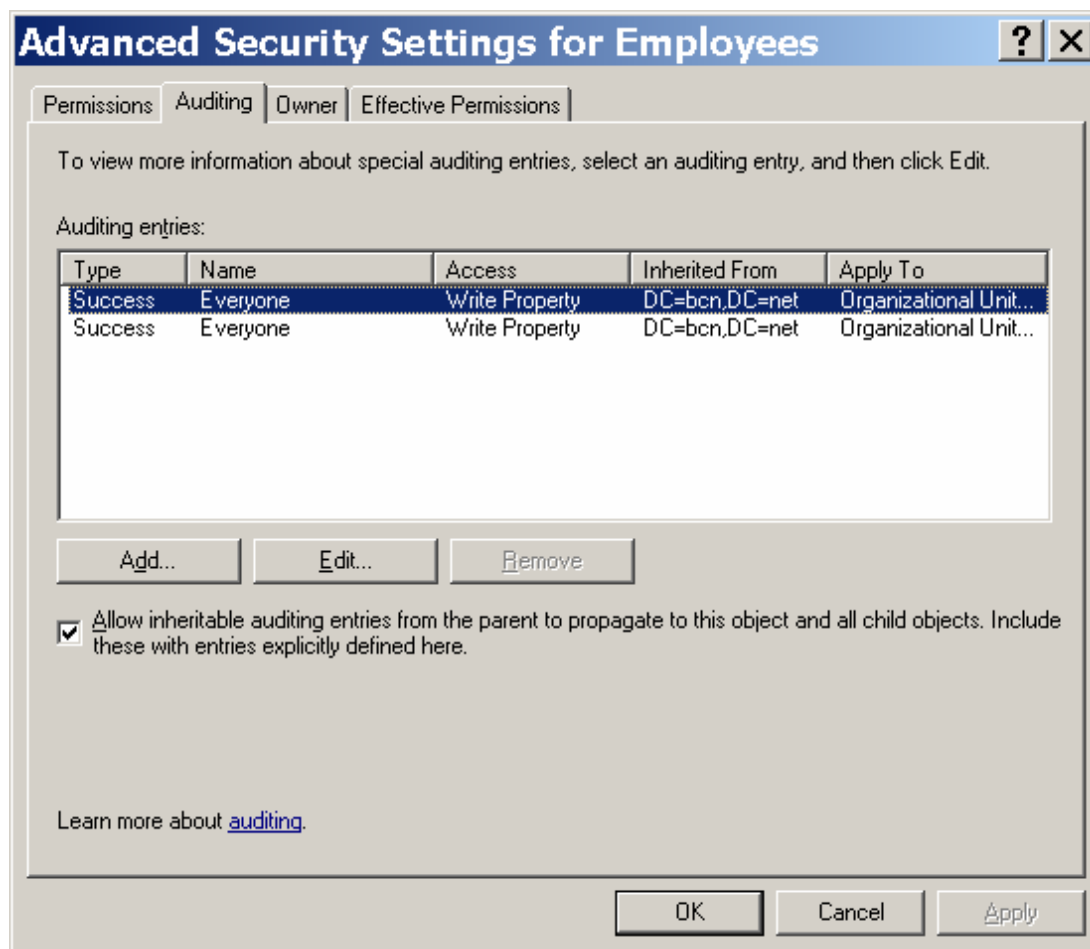



Figure 4.1: SACL settings configure auditing for objects in AD.

- Object ownership—The owner of an object can perform any task on that object. Therefore, the owner of AD objects is a critical part of overall security of that object and other objects that can be affected by the owner of an object. The user or group that creates an object becomes the owner of the object; thus, this configuration might need to be evaluated periodically to ensure that the optimum security configurations for object ownership are maintained over time.

The ACL Editor can be accessed from either the default administrative tools (Active Directory Users and Computers and AD Sites and Services) or from ADSI Edit, which is a GUI-based tool that allows you to see the objects located in AD.

 ADSI Edit is a free tool that comes on the Windows installation CD-ROM. You can find the tool, `adsiedit.msc`, under the Support Tools directory. Ideally, you will install the entire suite of support tools, which will make the ADSI Edit tool available from the Start menu.

If you are using Active Directory Users and Computers to access the ACL Editor, you might find that it is not available by default. If such is the case, to access the ACL Editor, you will first need to enable the Security tab on the objects that exist in AD. To enable the ACL Editor, click View on the toolbar in the Active Directory Users and Computers console, then select the Advanced Features menu option. The Security tab (which shows the ACL Editor) will be accessible for the objects in AD. To access the ACL Editor, follow these steps, right-click an object in the Active Directory Users and Computers console, select the Properties menu option, then select the Security tab on the Properties sheet for the object you are viewing.

The majority of administrative tasks that you will need to delegate won't show up on the initial Security tab, because the standard permission shown on this tab are more geared toward typical access of the object—not delegation of administration to the object. To access the permissions that relate to the administrative tasks associated with delegation, follow these steps once you are on the Security tab of the object.

1. Click Advanced, then find or create an entry for the user or group to which you are delegating administrative authority.
2. With the correct user or group entry selected, click Edit.
3. Configure the appropriate detailed permissions to allow the desired administrative task to be performed.
4. Click OK on each of the open ACL editor sheets to accept the settings and close the windows.

You will find that the options for configuring delegated administration are almost overwhelming using this method. The following list provides guidelines that will help you configure the delegation more efficiently using the ACL Editor:

- Configure the scope of inheritance on permissions—When you are working with the detailed permissions in the ACL Editor, configure the Apply onto setting, which will narrow the permissions inheritance. There are four main categories that you can choose from:
 - This object only—This setting will stunt the inheritance, only configuring the permission on the object itself
 - This object and all child objects—This setting will set the permissions on the current object and will allow the standard inheritance of permissions to flow down to the child objects located in the object
 - Child objects only—This setting will not set the permissions on the object itself but will affect the child objects located in the object to which the permissions are being set
 - <Specific object class> objects—This setting allows for a very narrow and specific scope of where the permissions will apply; this configuration targets the permissions to only the objects that are configured

- Use a guide—There are too many permissions with too much detailed control to think that you can configure all of the correct permissions without some form of reference. Rely on the work of others to help and guide you through specifying your own permissions. Refer to the Microsoft document Best Practices for Delegating AD Administration at <http://www.microsoft.com/downloads/details.aspx?FamilyID=631747a3-79e1-48fa-9730-dae7c0a1d6d3&displaylang=en> for detailed listings of permissions for each administrative task.

Ldp.exe

The Ldp.exe tool allows you to access the raw data and objects located in AD. The tool uses the Lightweight Directory Access Protocol (LDAP) operations to view, manage, and create objects in AD. Like the ADSI Edit tool, this tool is part of the Support Tools located on the installation media.

The tool requires you to connect to a domain controller, then bind to the AD database, and finally view the contents of the database. After you have used the tool one time, you will see that it is rather simple. However, first use of the tool can be a bit confusing. Refer to the Microsoft article “Using Ldp.exe to Find Data in the Active Directory” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;224543> for all of the steps and details on accessing and modifying objects using Ldp.exe.

Dsacls.exe

Dsacls.exe can take much of the manual labor out of reporting the existing delegation on any object in AD. The other tools that have been reviewed can update and view the existing permissions on any object in AD, but using them to get a complete list of all permissions that are configured on the objects can be very time consuming. Dsacls.exe is a command-line tool that reports and modifies permissions more efficiently than any of the other tools mentioned. This tool is also available from the Support Tools on the installation media.

Acldiag.exe

Acldiag.exe is another command-line utility that reports on the permissions of AD objects, helping track the delegation that has been configured on the objects. Acldiag.exe will also delineate between inherited and explicit permissions, helping track where delegation might have been configured on individual objects, instead of at higher levels such as OUs or the domain. Acldiag.exe is part of the Support Tools suite, like the other tools mentioned.

Dsrevoke.exe

Dsrevoke.exe is a new tool for Win2K and WS2K3 domain controllers and is designed to work in conjunction with the Delegation of Control Wizard. As we have already discussed, the wizard is not capable of removing any permissions, only adding them to an object. The Dsrevoke.exe tool is a free tool from Microsoft that was designed to remove delegated administrative authority.

Summary

With the complexity of AD administration, you will need to provide other administrators and non-IT professionals with the ability to help manage all of the tasks required to keep AD running. Some tasks are for controlling the core objects in AD and other tasks ensure that the directory is secure, stable, and available. In addition to following the suggested best practices, it is important to remember that delegation needs to be maintained and audited to ensure a secure AD environment.

This guide has walked you through the implementation of security for the information contained in and the resources protected by AD. Although this task is complex, by following the suggested best practices, you can attain and maintain a secure AD environment.