Realtime publishers
"Leading the Conversation"

The Essentials Series

Active Directory 2008 Operations

sponsored by
SCRIPTLOGIC

by Greg Shields

Copyright Statement

Understanding Active Directory Auditing in Windows Server 2008

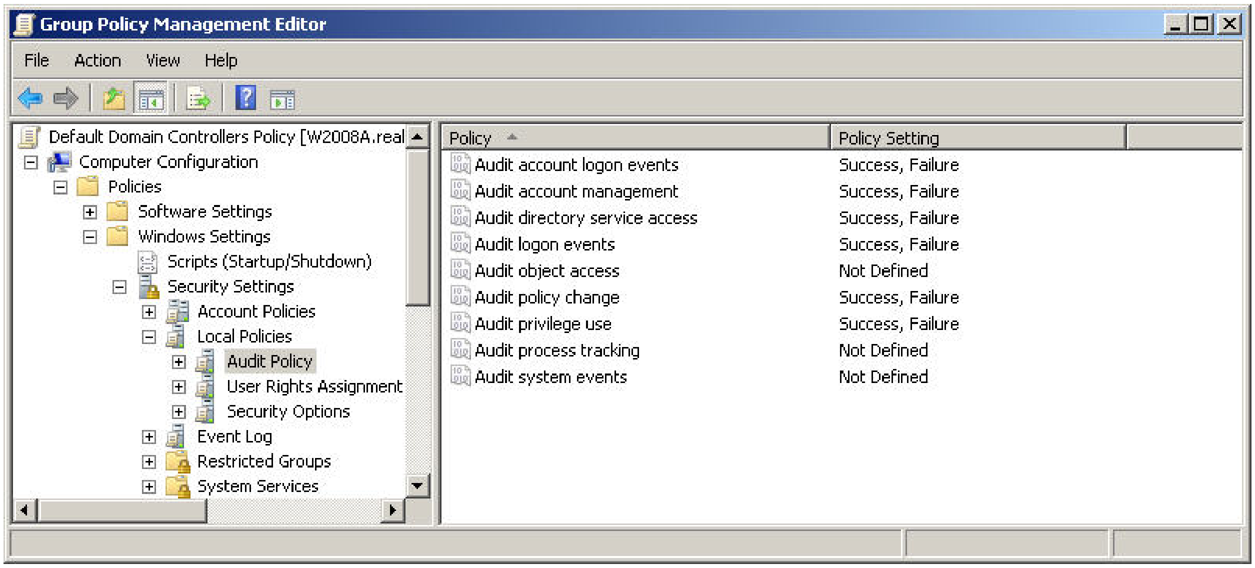
Throughout the history of the Windows operating system (OS), the features available to enable and monitor auditing for Active Directory (AD) have been relatively limited. Nine general categories of auditing have traditionally been available, all of which result in a fairly coarse level of logging to the Windows Event Log. By including only a small number of log categories, the result of enabling logging is a vast amount of excess data that must be managed in order to capture auditable actions of interest. At the same time, auditing requirements brought about by industry and governmental compliance regulations have increased the criticality for effective and consistent logging in many network environments.

With Microsoft’s release of Windows Server 2008, audit logging gains new levels of granularity associated with configurable event categories and subcategories, while a new Windows Event Log improves the process of filtering for and locating events of interest. AD itself gains four new logging subcategories that assist with the monitoring of configuration changes and replication in addition to object accesses.

This white paper will discuss the new audit capabilities specific to AD gained through an upgrade to Windows Server 2008. It will provide specific guidance and step-by-step instructions to assist you, the administrator, with making best use of AD’s new auditing features.

Enabling Auditing in Windows Server 2008

The process to enable auditing in Windows Server 2008 arrives relatively unchanged from its implementation in previous OS versions. Enabling the basic auditing of AD events on domain controllers is most often performed using Group Policy through modification of the native Default Domain Controllers Policy. Enabling auditing in this manner ensures that auditing settings are configured consistently across all domain controllers. Figure 1 shows a configured policy as seen within the Group Policy Management Editor.



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Not Defined
Audit system events	Not Defined

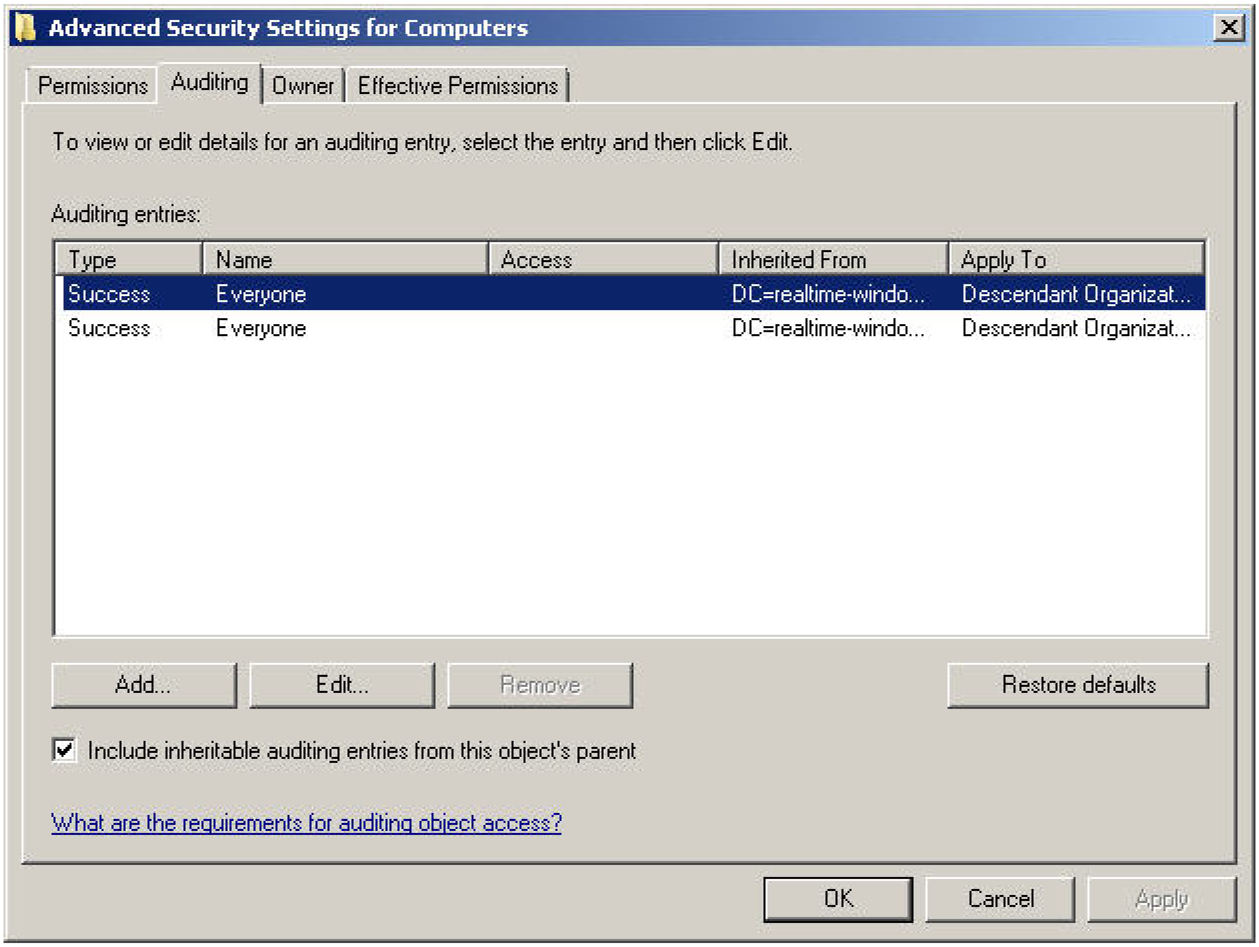
Figure 1: An example of AD auditing as enabled through the Default Domain Controllers Policy.

As you can see, a number of auditing categories are exposed through Group Policy. Each category has the ability to enable auditing for both Success and Failure events. Categories and event types are enabled based on the types of events you are interested in logging to the Windows Security Event Log. Though these categories are not new to Windows Server 2008, there remains some confusion about their use. Let’s take a look at each:

- Audit account logon events—This category generates an event when a user attempts to login or log out of a computer using a domain account.
- Audit account management—This category audits the creation, change, renaming, or deletion of user accounts or groups. It also audits the setting or change of a password.
- Audit directory service access—This category audits the attempt by users to access AD objects. Individual AD objects to be monitored must have their System Access Control List (SACL) configured to be monitored. The process of enabling this will be discussed shortly.
- Audit logon events—This category generates an event when a user attempts to login or log out of a computer using a local computer account.
- Audit object access—This category audits the attempt by a user to access an object, such as files, folders, registry keys, or printers, among others. Individual AD objects to be monitored must have their SACL configured to be monitored.
- Audit policy change—This category generates an event when a user attempts to change a user rights assignment policy, audit policy, or trust policy.
- Audit privilege use—This category audits the attempt by users to exercise the use of their assigned user rights.
- Audit process tracking—This category audits highly detailed tracking information about program activation, process exit, handle duplication, and indirect object access. This level of auditing is often employed by developers and during deep troubleshooting.
- Audit system events—This category generates an event when a user restarts or shuts down a computer or attempts to modify system security or the security log.

Although most of these auditing categories globally enable their type of auditing, two in particular require the configuration of object SACLs to enable auditing. Those two are *Audit directory service access* and *Audit object access*. For these two categories, the individual objects to be audited must also be configured if they are to be audited. For objects such as files, right-clicking the file and selecting Properties brings forward the properties dialog box. Selecting the Security tab, then Advanced, followed by the Auditing tab presents a dialog box used to configure which users and types of accesses should be audited.

The same process is used to audit the configuration of AD objects within Active Directory Users and Computers. To configure the SACL for an AD object, launch Active Directory Users and Computers, then click View | Advanced Features. Doing so enables the Security tab to be seen for individual objects. Right-click an object of interest, and select the Security tab, then click Advanced, and then select the Auditing tab. Figure 2 shows an example of configuring auditing for the Everyone group on the Computers organizational unit (OU).


Advanced Security Settings for Computers
Permissions
Auditing
Owner
Effective Permissions
Add...
Edit...
Remove
Restore defaults
What are the requirements for auditing object access?
OK
Cancel
Apply

To view or edit details for an auditing entry, select the entry and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From	Apply To
Success	Everyone		DC=realtime-windo...	Descendant Organizat...
Success	Everyone		DC=realtime-windo...	Descendant Organizat...

☑ Include inheritable auditing entries from this object's parent

Figure 2: Configuring object-level auditing within Active Directory Users and Computers.

Windows Server 2008's New Auditing Subcategories

The problem with these nine categories in previous versions of the Windows OS was that they didn't provide the level of granularity needed by many administrators. Enabling the *Audit account management* category effectively turned on auditing for all types of account management activities. If you were interested in only auditing for user account management and had no interest in computer account management, you were stuck with wading through the extra data associated with its Event Log entries.

With Windows Server 2008, the original nine categories are broken into 50 audit policy subcategories. These subcategories allow for precise control over the types of events logged into the Security Event Log. Table 1 highlights each of these new subcategories and their relation to the original nine audit policies. As you'll learn, knowing the name of each subcategory and its relation to its category is important for the command-line tool used to enable them.

Audit Category Name	Associated Audit Subcategories
System events	• Security state change • IPSec driver • Security system extension • System integrity • Other system events
Login events	• Logon • Logoff • Account Lockout • IPSec main mode • IPSec quick mode • IPSec extended mode • Special login • Other logon/logoff events
Object access	• File system • Registry • Kernel object • SAM • Certification services • Application generated • Handle manipulation • File share • Filtering platform packet drop • Filtering platform connection • Other object access events
Privilege use	• Sensitive privilege use • Non-sensitive privilege use
Process tracking	• Process creation • Process termination • DPAPI activity • RPC events
Policy change	• Audit policy change • Authentication policy change • Authorization policy change • MPSSVC rule-level policy change • Filtering platform policy change • Other policy change events
Account management	• User account management • Computer account management • Security group management • Distribution group management • Application group management • Other account management event

Directory service access	- Directory service access - Directory service changes - Directory service replication - Detailed directory service replication
Account logon events	- Kerberos service ticket operations - Credential validation - Kerberos authentication service - Other account logon events

Table 1: A list of the new audit subcategories and their relation to the original nine audit categories.

> You can find detailed information about the Event IDs and descriptions associated with each of the new subcategories at http://support.microsoft.com/default.aspx/kb/947226/en-us.

Configuring Audit Subcategories

Unlike with the nine categories, the implementation of these new subcategories is not done through Group Policy. Nor are they enabled through Local Security Policy. Rather, the only mechanism currently available for enabling specific subcategories is through the command-line tool auditpol.exe.

The auditpol command is used to enable and disable individual subcategories on individual machines. As auditpol does not leverage Group Policy for its assignment, it must be configured individually on each machine. Auditpol is equipped with a number of switches that are used to set and verify policy assignment. For example, to configure success auditing for the account management category with all subcategories, use the command

```
Auditpol /set /category:”account management”
```

It is also possible to use auditpol to set specific subcategories, one per command. Do so by using the /subcategory switch. To enable both success and failure auditing on only the *Computer account management* and *User account management* subcategories of the account management category, use the following two commands:

```
Auditpol /set /subcategory:”user account management”
/success:enable /failure:enable

Auditpol /set /subcategory:”computer account management”
/success:enable /failure:enable
```

The process of verifying set policies is also done through the same command-line tool. Listing 1 highlights an example of using the /get switch to verify the configuration after running the two pervious commands.

```
C:\Users\Administrator>auditpol /get /category:"account management"

System audit policy
Category/Subcategory           Setting
Account Management
 Computer Account Management       Success and Failure
 Security Group Management        No Auditing
 Distribution Group Management      No Auditing
 Application Group Management      No Auditing
 Other Account Management Events     No Auditing
 User Account Management         Success and Failure

C:\Users\Administrator>
```

Listing 1: The result of using the /get switch to verify correct audit subcategory configuration.

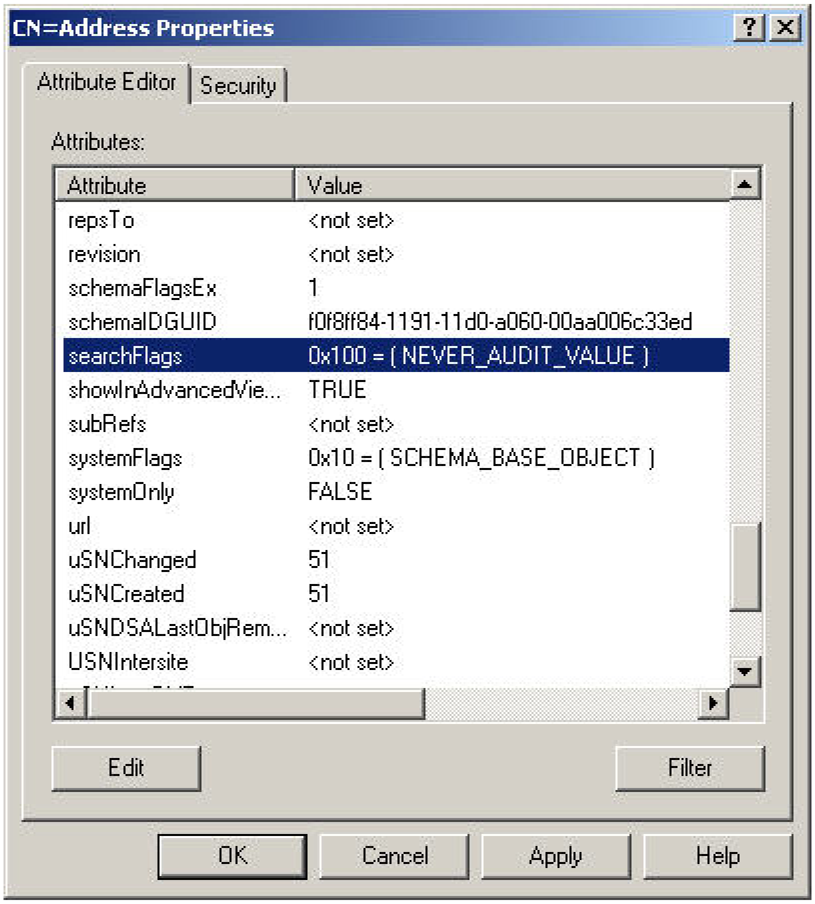
Auditing for AD Changes

As you can see in Table 1, AD auditing gains four new subcategories that provide further granularization of audit data. One subcategory that is of particular use in AD environments is Directory Service Changes. This new audit subcategory enables a new type of auditing associated with the configuration of individual AD objects. In environments that must support regulatory compliance, this new audit subcategory enables critical information about the configuration of AD itself. Once enabled, as an administrator attempts to make a change to an AD configuration, that change is logged to the Security Event Log. What makes this new subcategory particularly powerful is that information about what was changed along with the old and new values are now stored in the log entry itself.

For each change, two events are logged. The first event shows the attribute’s “old” value related to the configuration change. The second event shows the attribute’s “new” value. Because of this split, determining what happened requires a bit of sleuthing to match the two entries together. Four possible Event IDs can be logged:

- 5136 - Modify—An attribute for an existing object has been modified
- 5137 – Create—A new object has been created
- 5138 – Undelete—An object has been undeleted
- 5139 – Move—An object has been moved

It is possible to control which objects are audited through the same SACL modification process as was used earlier. Also possible with this subcategory alone is the disabling of certain attributes directly within the AD schema. You can do so by launching ADSI Edit and navigating to the Schema naming context. In the resulting tree is a list of each attribute in your AD. Double-click an attribute you do not want to be audited. On the Attribute Editor tab of the resulting window, change the value of the searchFlags attribute to 256. As Figure 3 shows, this sets the value for the attribute to NEVER_AUDIT_VALUE.



Attribute	Value
repsTo	<not set>
revision	<not set>
schemaFlagsEx	1
schemaIDGUID	f0f8ff84-1191-11d0-a060-00aa006c33ed
searchFlags	0x100 = (NEVER_AUDIT_VALUE)
showInAdvancedVie...	TRUE
subRefs	<not set>
systemFlags	0x10 = (SCHEMA_BASE_OBJECT)
systemOnly	FALSE
url	<not set>
uSNChanged	51
uSNCreated	51
uSNDSALastObjRem...	<not set>
USNIntersite	<not set>

Figure 3: Configuring an AD attribute's changes to not be audited.

Targeted Auditing Data Is Better Auditing Data

Auditing has historically been a challenging process in the Windows OS, in many ways due to its previous limitations on auditing categories. As you can see, those limitations have been lifted somewhat through the incorporation of greater granularity and higher-quality information. The ability to watch for and report on AD configuration changes enables IT to better fulfill the needs of regulatory compliance in monitoring the actions of users and administrators on the network.