Audit Policy

2 out of 3 rated this helpful

Updated: December 17, 2008
Applies To: Windows Server 2008

Establishing an organizational computer system audit policy is an important facet of information security. Configuring Audit policy settings that monitor the creation or modification of objects gives you a way to track potential security problems, helps to ensure user accountability, and provides evidence in the event of a security breach.

There are nine different kinds of events for which you can specify **Audit Policy** settings. If you audit any of these kinds of events, Windows® records the events in the Security log, which you can find in Event Viewer.

- **Account logon events**. Audit this to record each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. Account logon events are generated in the domain controller's Security log when a domain user account is authenticated on a domain controller. These events are separate from logon events, which are generated in the local Security log when a local user is authenticated on a local computer. Account logoff events are not tracked on the domain controller.

- **Account management**. Audit this to record when someone has changed an account name, enabled or disabled an account, created or deleted an account, changed a password, or changed a user group.

- **Directory service access**. Audit this to record when someone accesses an Active Directory® Domain Services object that has its own system access control list (SACL).

- **Logon events**. Audit this to record when someone has logged on or off your computer (either while physically at your computer or by trying to log on over a network).

- **Object access**. Audit this to record when someone has used a file, folder, printer, or other object. Although you can also audit registry keys, we do not recommend auditing them unless you have advanced computer knowledge and know how to use the registry.

- **Policy change**. Audit this to record attempts to change local security policies and to see if someone has changed user rights assignments, auditing policies, or trust policies.

- **Privilege use**. Audit this to record when someone performs a user right.

- **Process tracking**. Audit this to record when events such as program activation or a process exiting occur.

- **System events**. Audit this to record when someone has shut down or restarted the computer, or when a process or program tries to do something that it does not have permission to do. For example, if malicious software tried to change a setting on your computer without your permission, system event auditing would record it.

When you implement **Audit Policy** settings:

- Specify the categories of events that you want to audit. The event categories that you select constitute your audit policy.

- Set the size and behavior of the Security log. You can view the Security log with Event Viewer.

- If you want to audit directory service access or object access, determine which objects you want to audit access of and what type of access you want to audit. For example, if you want to audit all attempts by users to open a particular file, you can configure audit policy settings in the object access event category so that both successful and failed attempts to read a file are recorded.

The Security log records an audit event whenever users perform certain specified actions. For example, the modification of a file or a policy can trigger an event that shows the action that was performed, the associated user account, and the date and time of the action. These events can be both successful and failed attempts to perform actions.

Regular security analyses enable administrators to track and determine whether adequate security measures are in effect for each computer as part of an enterprise risk management program. Such analyses focus on highly specific information about all aspects of a computer that relate to security, which administrators can use to adjust the security levels. More important, this information can help detect any security oversights that may occur in the computer over time. For example, security levels may be temporarily changed to enable immediate resolution of an administration or network issue. However, such changes are often forgotten and never undone. If security levels are not properly reset, a computer may no longer meet the requirements for enterprise security.

Establishing and enabling audit policy settings that record deviations from your enterprise security policy are extremely important for any enterprise network. Audit logs may provide the only indication that a security breach has occurred by recording changes on file permissions, installation of programs, and escalation of privileges. If the breach is discovered some other way, proper audit settings can generate an audit log that may contain important information about the breach, how it occurred, and what systems were affected.

In many cases, failure events are much more informative than success events because failures typically indicate errors. For example, successful logon to a computer by a user would typically be considered normal. However, if someone unsuccessfully tries to log on to a computer multiple times, it may indicate an attacker's attempt to break into the computer with someone else's account credentials. The Event Log item of Group Policy is used to define attributes that relate to the Application, Security, and System logs, such as maximum log size, access rights for each log, and retention settings and methods. Auditing events are stored in the Security event log. For more information about the Event Log, see the Event Log section in this guide.

Before any audit processes are implemented, an organization should determine how to collect, organize, and analyze the data. There is little value in large volumes of audit data if there is no underlying plan to use it. Also consider that audit settings can affect computer performance. The effect of a given combination of settings may be negligible on an end-user computer but quite noticeable on a busy server. Therefore, you should perform some performance tests before you deploy new audit settings in your production environment. A final consideration is the amount of storage space that you can allocate to store the data collected during auditing. Depending on the setting you choose, auditing data can accumulate quickly and can fill up available disk space.

Audit account logon events

This policy setting enables auditing of each instance of user logon or logoff on a different computer than the one that records the event and validates the account. Success audits provide useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged on to which computer.

Failure audits are useful for intrusion detection. However, this configuration of the policy setting also creates the potential for a DoS attack. When the **Audit: Shut down system immediately if unable to log security audits**setting in the **Security Options** section of Group Policy is also enabled, an attacker could generate millions of logon failures in order to fill the Security log and force the computer to shut down.

If you configure the **Audit account logon events** setting to **Success** on a domain controller, an event is logged for each user who is validated against that domain controller, even though the user actually logs on to a workstation or server that is joined to the domain.

By default, **Auditaccount logon events** is set to **Success**.

Audit account management

This policy setting enables auditing of each account management event on a computer. Examples of account management events include the following:

- User account or group is created, changed, or deleted.
- User account is renamed, disabled, or enabled.
- Password is set or changed.

Success audits should be enabled on all computers in your enterprise. When an organization responds to security incidents, it is critical that they be able to track who created, changed, or deleted an account. Failure audits generate an event when any account management action fails.

Audit directory service access

This policy setting enables auditing of user access of an Active Directory object that has an associated SACL. A SACL is list of users and groups for which actions on an object are to be audited on a Windows–based network.

Success audits generate an event when a user successfully accesses an Active Directory object that has a SACL that indicates that the user should be audited for the requested action. Failure audits generate an event for each unsuccessful attempt. (Both types of events are created before the user is notified that the request succeeded or failed.) If you enable this policy setting and configure SACLs on directory objects, a large volume of entries can be generated in the Security logs on domain controllers. You should enable these settings only if you actually intend to use the information that is created.

Audit logon events

This policy setting enables auditing of each instance of user logon, logoff, or network connection to the computer that records the event. If you log successful account logon events on a domain controller, workstation logon attempts do not generate logon events. Only interactive and network logon attempts to the domain controller itself generate logon events on the domain controller. To summarize, "account logon events" are generated where the account exists, either on the domain controller if the account is a domain account or on the local computer if the account is a local computer account, and "logon events" are generated on the computer where the user is logging on or off.

Success audits provide useful information for accounting purposes and for post-incident forensics so that you can determine who successfully logged on to which computer. Failure audits are useful for intrusion detection. However, the configuration of failure events also creates a potential DoS condition. When the **Audit: Shut down system immediately if unable to log security audits** setting in the **Security Options** section of Group Policy is also enabled, an attacker could generate millions of logon failures in order to fill the Security log, and force the server to shut down.

Audit object access

This policy setting enables auditing of the event generated by a user who accesses an object—for example, a file, folder, registry key, or printer—that has a SACL that specifies a requirement for auditing.

Success audits generate an event when a user successfully accesses an object that has a SACL. Failure audits generate an event for each unsuccessful attempt (some failure events are to be expected during normal computer operations). For example, many applications (such as Microsoft Office Word) always attempt to open files with both read and write privileges. If the applications are unable to do so, they then try to open the files with read-only privileges. If you enable failure auditing and the appropriate SACL on the file, a failure event is recorded when such an event occurs.

You can audit access to objects that are stored in the Internet Information Services (IIS) metabase. To enable metabase object auditing, you must enable **Audit object access** on the target computer and then set SACLs on the specific metabase objects whose access you want to audit.

If you configure the **Audit object access** policy setting and configure SACLs on objects, a large volume of entries can be generated in the Security logs on computers in your organization. Therefore, you should only enable these settings if you actually intend to use the information that is logged.

Audit policy change

This policy setting enables auditing of every incidence of a change to user rights assignment policies, Windows Firewall policies, Audit policies, or trust policies.

Success audits are useful for accounting purposes and can help you determine who successfully modified policies in the domain or on individual computers. Failure audits generate an event when a change to user rights assignment policies, Audit policies, or trust policies fails.

If you enable the **Audit policy change** setting in Windows Vista and Windows Server 2008, logging of configuration changes for the Windows Firewall component is also enabled.

Audit privilege use

This policy setting enables auditing of each instance of a user who exercises a user right.

Success audits generate an event when the exercise of a user right succeeds. Failure audits generate an event for an unsuccessful exercise. If you enable this policy setting, the volume of events that is generated can be very large and cumbersome. You should enable this setting only if you plan to use the information that is generated.

Audit events are not generated for the use of the following user rights, even if success audits or failure audits are specified for the **Audit privilege use** policy setting:

- Bypass traverse checking
- Debug programs
- Create a token object
- Replace process level token
- Generate security audits
- Backup files and directories
- Restore files and directories

Audit process tracking

This policy setting enables auditing of detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

Success audits generate an event when the process being tracked succeeds. Failure audits generate an event when the process fails.

If you enable **Audit process tracking** in Windows Vista and Windows Server 2008, Windows also logs information about the operating mode and status of the Windows Firewall component.

When enabled, the **Audit process tracking** setting generates a large number of events. This policy setting is typically configured to **No Auditing**. However, the information that this policy setting generates can be very beneficial during an incident response because it provides a detailed log of the processes that were started and when they were started.

Audit system events

This policy setting enables auditing of the restart or shutdown of users' computers, or events that affect either computer security or the Security log.

Success audits generate an event when an event runs successfully. Failure audits generate an event when an event is unsuccessful.

Because few additional events are recorded if both failure and success audits are enabled for system events, and because all such events are very significant, you should configure this policy setting to **Enabled** on all computers in your organization.