netwrix

Windows Audit Policy Best Practices

What is audit policy in Windows?

Windows audit policy defines what types of events are written to the Security logs of your Windows servers. Establishing an effective audit policy helps you spot potential security problems, ensure user accountability and provide evidence in the event of a security breach.

The recommended audit policy settings provided here are intended as a baseline for system administrators starting to define AD audit policies. You should be sure to consider the cybersecurity risks and compliance requirements of your organization. In addition, test and refine your policies before implementing them in your production environment.

How to implement audit policy

There are two methods of setting up your audit policy:

- **Basic security audit policy** in Windows (also referred as local Windows security settings) allows you to set auditing by on a per-event-type basis. Basic policies can be found under Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Audit Policy.

- **Advanced security audit policy** address same issues, as basic audit policies, but let you to set up auditing granularly within each event category. These settings are found in Computer Configuration -> Policies -> Windows Security Settings -> Advanced Audit Policy Configuration -> System Audit Policies. They appear to overlap (not override) basic security audit policies.

Microsoft advises organizations not to use both the basic audit policy settings and the advanced settings simultaneously for same category, because when advanced audit policy is configured, it will always override basic audit policies, which in result can cause “unexpected results in audit reporting”.

You can view the Security log with the Event Viewer.

Before changing any settings, you should:

- Determine which types of events you want to audit from the list below, and specify the settings for each one. The settings you specify constitute your audit policy. Note that some event types are audited by default.
- Decide how you will collect, store and analyze the data. There is little value in amassing large volumes of audit data if there is no underlying plan to manage and use it.
- Specify the maximum size and other attributes of the Security log using the Event Logging policy settings. An important consideration is the amount of storage space that you can allocate to storing the data collected by auditing. Depending on the setting you choose, audit data can quickly fill up available disk space.
- Remember that audit settings can affect computer performance. Therefore, you should perform performance tests before you deploy new audit settings in your production environment.
- If you want to audit directory service access or object access, configure the **Audit directory service access** and **Audit object access** policy settings.

Types of events you can audit

Here are the basic security audit policy categories:

- **Audit account logon events.** User logon auditing is the only way to detect all unauthorized attempts to log in to a domain. It is vital to audit logon events — both successful and failed — to detect intrusion attempts. Logoff events are not tracked on domain controllers.
- **Audit account management.** Carefully monitoring all user account changes helps minimize the risk of business disruption and system unavailability.
- **Audit directory service access.** Monitor this only when you need to see when someone accesses an AD object that has its own system access control list (for example, an OU).
- **Audit logon events.** Seeing successful and failed attempts to log on or off a local computer is useful for intruder detection and post-incident forensics.
- **Audit object access.** Audit this only when you need to see when someone used privileges to access, copy, distribute, modify or delete files on file servers.

- **Audit policy change.** Improper changes to a GPO can greatly damage the security of your environment. Monitor all GPO modifications to reduce the risk of data exposure.

- **Audit privilege use.** Turn this policy on when you want to track each instance of user privileges being used. It is recommended to setup **this function granularly in Sensitive Privilege Use of the advanced audit policies.**

- **Audit process tracking.** Auditing process-related events, such as process creation, process termination, handle duplication and indirect object access, can be useful for incident investigations.

- **Audit system events.** Configuring the system audit policy to log startups, shutdowns and restarts of the computer, and attempts by a process or program to do something that it does not have permission to do, is valuable because all such events are very significant. For example, if malicious software tries to change a setting on your computer without your permission, system event auditing would record that action.

Recommended Windows Auditing Settings

Here are the basic security audit policy categories:

Account Logon

- Audit Credential Validation: Success and Failure

Account Management

- Audit Computer Account Management: Success and Failure

- Audit Other Account Management Events: Success and Failure

- Audit Security Group Management: Success and Failure

- Audit User Account Management: Success and Failure

DS Access (Directory Service Access)

- Audit Directory Service Access: Success and Failure on DC

- Audit Directory Service Changes: Success and Failure on DC

Logon/Logoff

- Audit Account Lockout: Success
- Audit Logoff: Success
- Audit Logon: Success and Failure
- Audit Special Logon: Success and Failure

Object Access

- Enable these settings only if you have a specific use for the data that will be logged, because they can cause a large volume of entries to be generated in your Security logs.

Policy Change

- Audit Audit Policy Change: Success and Failure
- Audit Authentication Policy Change: Success and Failure

Privilege Use

- Enable these settings only if you have a specific use for the data that will be logged, because they can cause a large volume of entries to be generated in your Security logs.

Process Tracking

- Audit Process Creation: Success

Enable these settings only if you have a specific use for the information that will be logged, because they can cause a large volume of entries to be generated in your Security logs.

System

- Audit Security State Change: Success and Failure
- Audit Other System Events: Success and Failure
- Audit System Integrity: Success and Failure

Secure your Active Directory from end to end with Netwrix solutions

- Uncover security risks in Active Directory and prioritize your mitigation efforts
- Harden security configurations across your IT infrastructure
- Promptly detect and contain even advanced threats, such as DCSync and Golden Ticket attacks
- Respond to known threats instantly with automated response options
- Minimize business disruptions with fast Active Directory recovery

Request One-to-One Demo

About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 11,500 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers. Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S. For more information, visit www.netwrix.com.

Next Steps

See Netwrix products — Explore the full Netwrix portfolio: netwrix.com/products

Get a live demo — Take a personalized product tour with a Netwrix expert: netwrix.com/livedemo

Request a quote — Receive pricing information: netwrix.com/buy

CORPORATE HEADQUARTER:	PHONES:
300 Spectrum Center Drive Suite 200 Irvine, CA 92618	1-949-407-5125 Toll-free (USA): 888-638-9749
565 Metro Place S, Suite 400 Dublin, OH 43017	1-201-490-8840
5 New Street Square London EC4A 3TW	+44 (0) 203 588 3023

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:

netwrix.com/social