ManageEngine

The 8 most critical Windows security event IDs

Table of Contents

The Windows Security Log

The Windows Security Log, which you can find under **Event Viewer,** records critical user actions such as logons and logoffs, account management, object access, and more.

Microsoft describes the Windows Security Log as "your best and last defense," and rightly so. The Security Log helps detect potential security problems, ensures user accountability, and serves as evidence during security breaches.

What makes a Windows security event critical?

Among the multitude of Windows security events, the few that can be deemed critical can be broadly classified into two groups:

1. Events whose single occurrence indicates malicious activity. For example, a normal end-user account getting unexpectedly added to a sensitive security group.

2. Events whose successive occurrence above an accepted baseline indicates malicious activity. For example, an abnormally large number of failed logons.

The eight most critical Windows security event IDs

Serial Number	Category	Event ID and description	Reasons to monitor (by no means exhaustive)
(1) & (2)	**Logon and logoff**	**4624** (Successful logon)	• To detect abnormal and possibly unauthorized insider activity, like a logon from an inactive or restricted account, users logging on outside of normal working hours, concurrent logons to many resources, etc. • To get information on user behavior like user attendance, user working hours, etc.
		4625 (Failed logon)	• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons. • To arrive at a benchmark for the account lockout threshold policy setting.
(3), (4), and (5)	**Account management**	**4728** (Member added to security-enabled global group)	• To ensure group membership for privileged users, who hold the “keys to the kingdom,” is scrutinized regularly. This is especially true for security group membership additions. • To detect privilege abuse by users who are responsible for unauthorized additions. • To detect accidental additions.
		4732 (Member added to security-enabled local group)	
		4756 (Member added to security-enabled universal group)	

(6)	**Event log**	**1102** (Log cleared) (Alternatively the event log service can also be disabled which results in the logs not getting recorded. This is done by the system audit policy, in which case event **4719** gets recorded.)	• To spot users with malicious intent, such as those responsible for tampering with event logs.
(7)	**Account management**	**4740** (User account locked out)	• To detect possible brute-force, dictionary, and other password guess attacks, which are characterized by a sudden spike in failed logons. • To mitigate the impact of legitimate users getting locked out and being unable to carry out their work.
(8)	**Object access**	**4663** (Attempt made to access object)	• To detect unauthorized attempts to access files and folders.

Securing Active Directory

First and foremost, you need to configure your audit policy so that Windows can record the relevant events in the Security Log. Next, you need to aggregate and analyze the collected logs, then translate those findings into actionable information, like reports and alerts. Using native tools and PowerShell scripts to complete these tasks demands expertise and a lot of time. To get the job done quickly and efficiently, a third-party tool is truly indispensable.

With in-depth reports, real-time alerts, and graphical displays, ADAudit Plus simplifies the continuous monitoring of logons and logoffs, group membership changes, event log clearance, account lockouts, file servers, and much more across your Active Directory, member servers, and workstations.

Note

While much care has been taken to prepare this document, we give no warranties whatsoever with respect to this document, including but not limited to the accuracy of any information contained therein.