Important Windows Event IDs: Which Events You Should Monitor and Why

September 9, 2020

Blog

Archive

This is an updated blog that was originally published in 2018.

Security breaches often go unnoticed for weeks or months, and some are never uncovered. Investigations usually show evidence of breaches in server event logs but because of the volume of data collected it is like looking for a needle in a haystack. Windows Server logs contain a mass of useful information but finding events that might indicate an operational issue or security breach requires a carefully planned auditing and monitoring strategy.

Ready to learn more? Check out my on-demand webinar, *Windows Events You Should be Tracking: Learn how to Answer the Who, What, When, Where & How*

Windows Advanced Audit Policy and Security Baselines

The Windows Audit Policy defines the specific events you want to log, and what particular behaviors are logged for each of these events. For example, your audit policy may determine that you want to log any remote access to a Windows machine, but that you do not need to audit login attempts from someone on your business premises.

If you don't have any audit policy configured, or if you are still using legacy audit settings, it's time to set up Advanced Audit Policy. First introduced in Windows Server 2008, Advanced Audit Policy provides more granular control over Windows auditing so you can capture what's important and eliminate noise. Legacy and advanced audit policy settings shouldn't be used at the same time, so make sure you plan to retire legacy settings when switching to Advanced Policy Auditing.

If you are not sure what to audit, Microsoft's recommend audit settings in the baseline security templates for Windows Server are an ideal place to start. The Security Compliance Toolkit contains templates for different server roles, like domain controller (DC) and member server, and they can be deployed using Group Policy. The templates contain many other security settings, not just audit policy, so you must test them thoroughly before deploying to production systems. Alternatively, you can just configure the recommend audit settings.

In addition to Microsoft's recommendations, consider auditing anything that might indicate unauthorized activity and that should involve an investigation. For example, if you have a security policy that forbids domain administrators logging in to member servers, then any activity that indicates a breach of the policy should be logged and investigated. Start by prioritizing sensitive servers, like DCs, but don't forget to audit and monitor workstations. Hackers usually start their penetration efforts on devices that users interactively log in to because they are more vulnerable.

Windows Event Forwarding

If you are not using an agent to send server event logs directly to a Security Information and Event Management (SIEM) solution, consider centralizing events on a single collector so that they can be monitored and archived more easily. A collector is configured with subscriptions for servers from which you want to pull event logs.

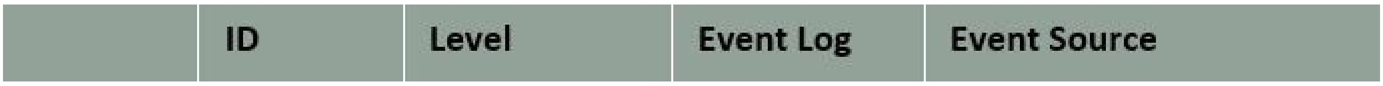
Source computers don't need any special configuration, but Windows Remote Management (WinRM) must be enabled. If you want to collect the Security log from a DC, you will need to give the DC's Network Service account read channel access permission to the Security log.

Events to Monitor

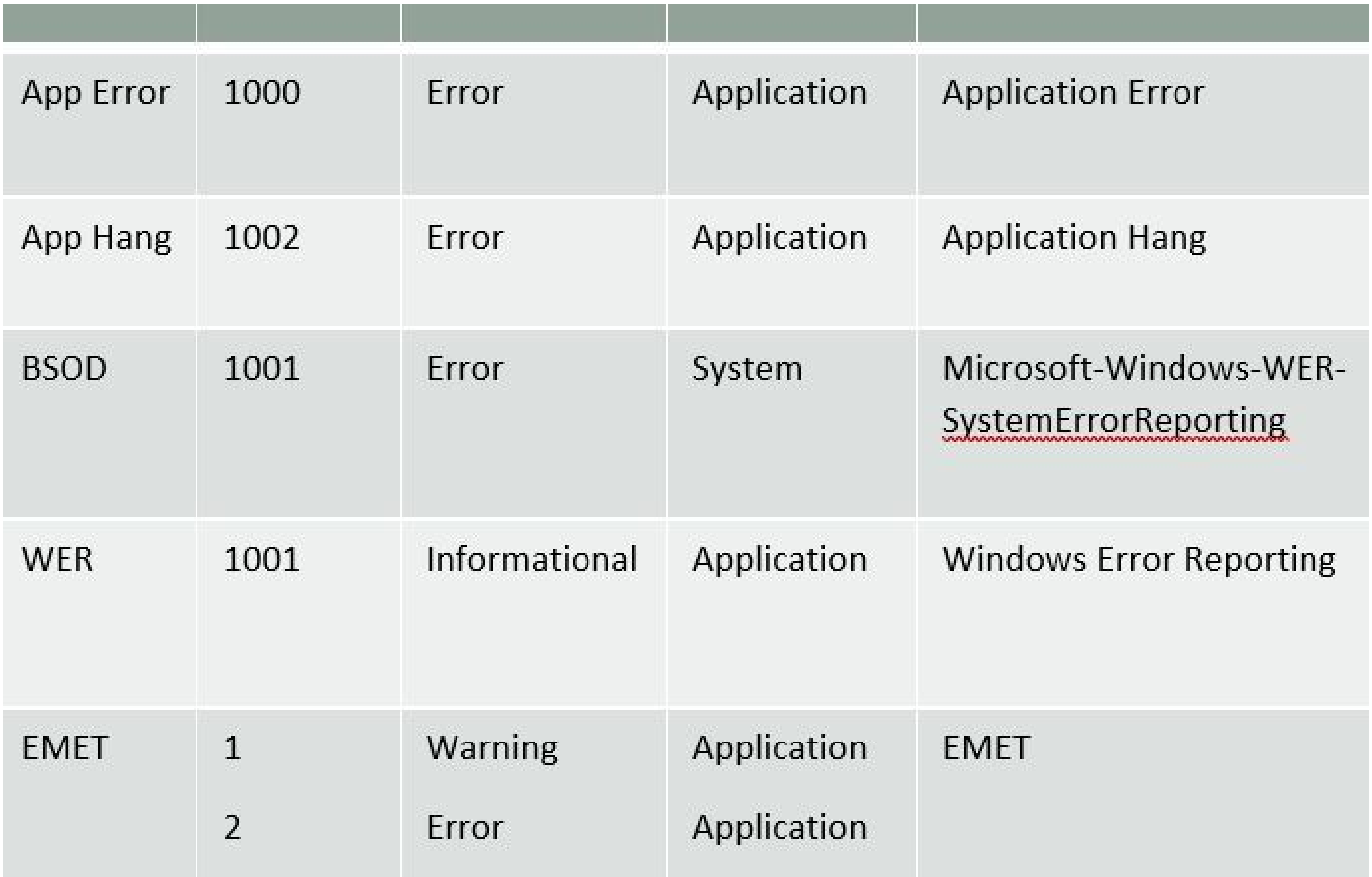
Below, I've listed categories of events that you should consider monitoring. For example, you might collect events that indicate a change in Windows Firewall configuration. Application allow listing is worth enabling in audit mode to log processes and scripts that don't normally run on your systems. Another example is Windows Defender, which is included out-of-the-box in Windows Server 2016 and 2019. Look for events like *Scan failed*, *Malware detected*, and *Failed to update signatures*.

- Application Allow listing
- Application Crashes
- System or Service Failures
- Windows Update Errors
- Windows Firewall
- Clearing Event Logs
- Software and Service Installation
- Account Usage Kernel Driver Signing
- Group Policy Errors
- Windows Defender Activities
- Mobile Device Activities
- External Media Detection
- Printing Services
- Pass the Hash Detection Remote Desktop Logon Detection

Hackers try to hide their presence. Event ID 104 *Event Log was Cleared* and event ID 1102 *Audit Log was Cleared* could indicate such activity. Event ID 4719 *System audit policy was changed* could also show malicious behavior. If an application crashes, it could be that a hacker has tried to force a process to end to hide their actions.



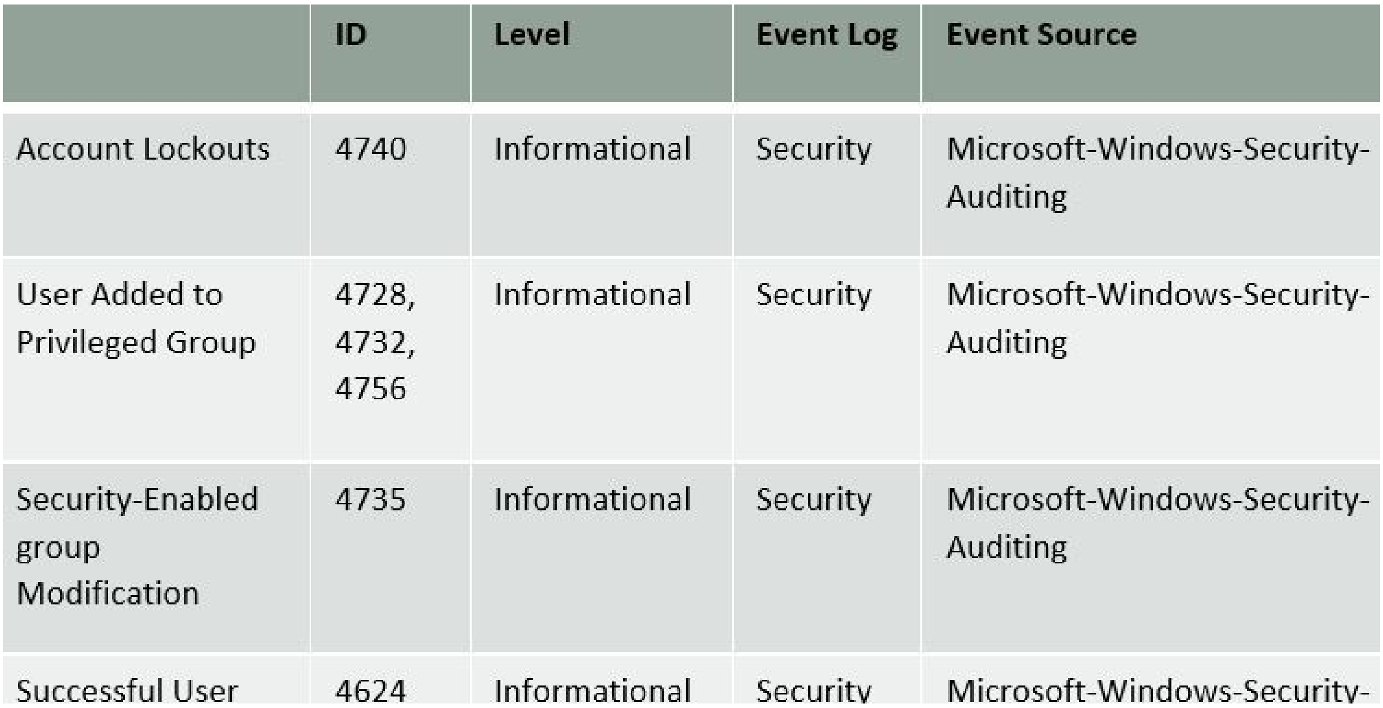
	ID	Level	Event Log	Event Source



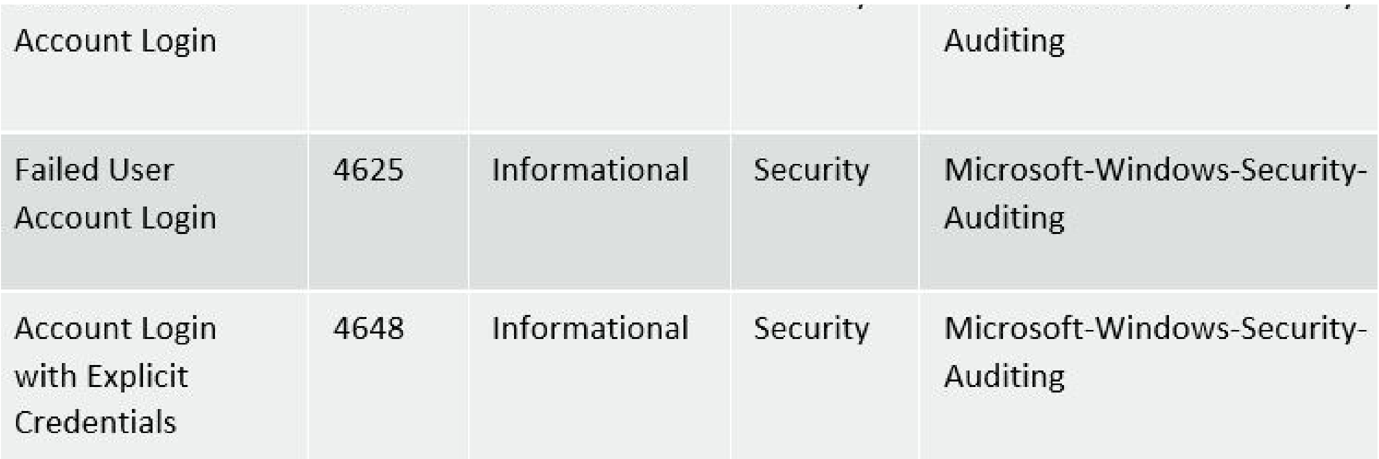
App Error	1000	Error	Application	Application Error
App Hang	1002	Error	Application	Application Hang
BSOD	1001	Error	System	Microsoft-Windows-WER-SystemErrorReporting
WER	1001	Informational	Application	Windows Error Reporting
EMET	1 2	Warning Error	Application Application	EMET

Table 1: Application crashes

Table 2 shows events that might indicate suspicious logon activity. Pass-the-Hash (PtH) is a popular form of attack that allows hackers to gain access to an account without needing to know the password. Look out for NTLM Logon Type 3 event IDs 4624 (failure) and 4625 (success).



	ID	Level	Event Log	Event Source
Account Lockouts	4740	Informational	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Informational	Security	Microsoft-Windows-Security-Auditing
Security-Enabled group Modification	4735	Informational	Security	Microsoft-Windows-Security-Auditing
Successful User	4624	Informational	Security	Microsoft-Windows-Security-



Account Login				Auditing
Failed User Account Login	4625	Informational	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Informational	Security	Microsoft-Windows-Security-Auditing

Table 2: Account usage

Using Tasks on Custom Views to Generate Alerts

If you are not able to use a SIEM, you can generate alerts by attaching tasks to custom views in Event Viewer. A custom view uses a filter to display only the events you want to see. Attaching a task to a custom view lets you run a program or script whenever a new event is received in the custom view. For example, you could run a PowerShell script that sends an email if a domain administrator logs in to a member server.

Security Information and Event Management

While Microsoft provides some basic event monitoring and alerting features in Windows Server, with today's ever-changing threat landscape, the best way to monitor systems is using a SIEM solution. Microsoft's SIEM product, Azure Sentinel, can monitor Windows Server and cloud-native systems like Office 365 and Amazon AWS. Using threat knowledge from Microsoft, machine learning, and artificial intelligence (AI), you will be better protected than when relying on the limited capabilities of the built-in Windows toolset. Other popular SIEM solutions include Splunk Enterprise Security and IBM QRadar.

How Endpoint Privilege Management Can Help

While, every organization can expect to be breached at some point, prevention is always preferable to curing/remediation. Use of privileged accounts, such as privileged Active Directory (AD) accounts by support staff, or local administrator rights by employees on workstations, increases the risk of compromise. As the annual

Microsoft Vulnerabilities Reports have highlighted, removing admin rights and enforcing least privilege are perhaps the most powerful and effective way to reduce risk across Windows environments. Privileged Access Management (PAM) solutions can address the native Windows privilege management gaps. Third-party PAM solutions, such as BeyondTrust Endpoint Privilege Management, can stop and mitigate many external (malware, hacker) and insider attacks, while also providing threat analytics and detection capabilities that can help pinpoint an attack that is underway. BeyondTrust's solution enables organizations to remove unnecessary privileges, while still providing employees with the access to systems needed for completing tasks related to their roles.

BeyondTrust Endpoint Privilege Management can help your organization control and monitor privileged activity by:

- **Granularly controlling privileged access amount (just enough access and duration (just-in-time access), to ensure true least privilege is enforced.**
- **Tracking and preventing lateral movement:** Utilize rules to track and prevent anomalous user activity based on user roles and targeted resource
- **Maintaining awareness:** Monitor UAC events, application rules, requested elevations, denied applications, and more.
- **Ensuring accountability:** Leverage session monitoring for rules-based activity recording, including screenshots and searchable keystroke logs.
- **Understanding and communicating risk:** Leverage an interactive, role-based reporting and analytics console, backed by a centralized data warehouse for ongoing audits of user privilege management software activities.

To learn more about how BeyondTrust solutions can help your organization monitor events and control privileged activity in your Windows environment, check out my on-demand webinar, *Windows Events You Should be Tracking: Learn how to Answer the Who, What, When, Where & How*.

Privileged Access Management (PAM): Buyer's Guide & Checklist

Whitepapers

Russell Smith,

IT Consultant & Security MVP

Russell Smith specializes in the management and security of Microsoft-based IT systems. In addition to blogging about Windows and Active Directory for the Petri IT Knowledgebase, Russell is a Contributing Editor at CDW’s Biztech Magazine.

Russell has more than 15 years of experience in IT, has written a book on Windows security, co-authored one for Microsoft’s Official Academic Course (MOAC) series and has delivered several courses for Pluralsight.

Stay Up To Date

Get the latest news, ideas, and tactics from BeyondTrust. You may unsubscribe at any time.

Business Email

Submit

I agree to receive product related communications from BeyondTrust as detailed in the Privacy Policy, and I may manage my preferences or withdraw my consent at any time.

Up next

From September 8, 2020:
September 2020 Patch Tuesday

From September 15, 2020:
Privileged Remote Access Version 20.2 Delivers Workflow, Vault, & New Vendor Onboarding Enhancements

You May Also Be Interested In:

Microsoft Vulnerabilities Report 2023

Whitepapers

Cybersecurity Survival Guide

Whitepapers

Advancing Zero Trust with Privileged Access Management (PAM)

Whitepapers