

Windows event logs

Choose the right channel, filter the time window and preserve the evidence.

Choose the relevant log

System - operating system, drivers and services.

Application - application/provider events.

Security - configured security audit events; access and audit policy affect what is available.

Setup - installation/setup activity.

Forwarded Events - events received by a configured collector.

Applications and Services Logs contains provider-specific Operational channels, including GroupPolicy and TaskScheduler.

Interpret the fields together

Record computer, channel, provider, Event ID, Record ID, level, timestamp and full message. Inspect the XML details and ActivityID when available. An Event ID alone is not a diagnosis and is not globally unique across providers. Event Viewer displays local time; confirm the time zone when correlating systems.

Standard levels

1 Critical · **2** Error · **3** Warning

4 Information · **5** Verbose

0 LogAlways.

Audit Success/Failure are audit keywords, not a replacement for these numeric levels. Informational events can still be essential evidence.

Inspect recent events

```
Get-WinEvent -LogName System -MaxEvents 30
```

Read recent system events.

```
Get-WinEvent -ListLog *
```

Discover log names and their configuration. Permissions affect visibility.

Filter at the source

```
Get-WinEvent -FilterHashtable @{
  LogName="System"; Level=1,2,3
  StartTime=(Get-Date).AddHours(-2)
} -MaxEvents 100
```

One PowerShell command: critical, error and warning events from the last two hours. Add EndTime for a bounded window.

Add ProviderName and Id when investigating a known provider/event combination. Filtering in the query avoids loading an entire log before Where-Object filters it. No matches can mean the window, provider or channel is wrong.

Export the original events

```
wevtutil epl System .\System.evtx
```

Export the System log to a new EVTX file in the current writable folder. Choose a unique filename; no overwrite is requested.

```
Get-WinEvent -Path .\System.evtx
-MaxEvents 30
```

One PowerShell command; join the lines. Inspect a saved EVTX without importing it into the live log.

Preserve context

In Event Viewer, use Filter Current Log or a Custom View, then export the required events. Keep EVTX for original event data; CSV or copied message text is useful for summaries but is not a full substitute. Protect originals and note the collection time and filter.

Investigate before changing logging

Correlate events before and after the symptom across related providers. Log retention, disabled channels or audit settings can explain missing history. Enabling extra logging changes collection and will not recreate old events. Do not clear logs during evidence collection. Redact sensitive information from shared summaries.