

Custom Windows Event Logs - Integration

Custom Windows Event Logs

Collect and parse logs from any Windows event log channel with Elastic Agent.

The custom Windows event log package allows you to ingest events from any [Windows event log](#) channel. You can get a list of available event log channels by running `Get-WinEvent -ListLog * | Format-List -Property LogName` in PowerShell on Windows Vista or newer. If `Get-WinEvent` is not available, `Get-EventLog *` may be used.

By executing this command in the powershell(administrator), it will list the log names that is being used.

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-WinEvent -ListLog * | Format-List -Property LogName

LogName : Windows PowerShell
LogName : System
LogName : Security
LogName : Key Management Service
LogName : Internet Explorer
LogName : HardwareEvents
LogName : Application
LogName : Windows Networking Vpn Plugin Platform/OperationalVerbose
LogName : Windows Networking Vpn Plugin Platform/Operational
LogName : SMSApi
LogName : Setup
LogName : OpenSSH/Operational
LogName : OpenSSH/Admin
LogName : Network Isolation Operational
LogName : Microsoft-Windows-WPD-MTPClassDriver/Operational
LogName : Microsoft-Windows-WPD-CompositeClassDriver/Operational
LogName : Microsoft-Windows-WPD-ClassInstaller/Operational
LogName : Microsoft-Windows-Workplace Join/Admin
LogName : Microsoft-Windows-Wordpad/Admin
LogName : Microsoft-Windows-WMPNSS-Service/Operational
LogName : Microsoft-Windows-WMI-Activity/Operational
LogName : Microsoft-Windows-Wired-AutoConfig/Operational
LogName : Microsoft-Windows-Winsock-WS2HELP/Operational
LogName : Microsoft-Windows-Winsock-NameResolution/Operational
LogName : Microsoft-Windows-Winsock-AFD/Operational
LogName : Microsoft-Windows-WinRM/Operational
LogName : Microsoft-Windows-WinNat/Oper
```

Add a channel name in the Channel Name text field (e.g Application).

Find apps, content, and more.

1/

Cancel

Windows

Edit Custom Windows Event Logs

integration

Modify integration settings and deploy changes to the selected agent policy.

Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

winlog-1

DescriptionOptional

Advanced options

Custom Windows event logs

Change defaults

Channel Name

Application

Name of Windows event log channel (eg. Microsoft-Windows-PowerShell/Operational)

Dataset name

winlog.winlog

Dataset to write data to. Changing the dataset will send the data to a different index. You can't use - in the name of a dataset and only valid characters for Elasticsearch index names.

Ingest PipelineOptional

The Ingest Node pipeline ID to be used by the integration.

Preserve original event

Preserves a raw copy of the original XML event, added to the field event.original

Advanced options

Revision #1

Created 22 October 2024 02:16:41 by Eduardo Dominico Llosa

Updated 22 October 2024 06:49:33 by Eduardo Dominico Llosa