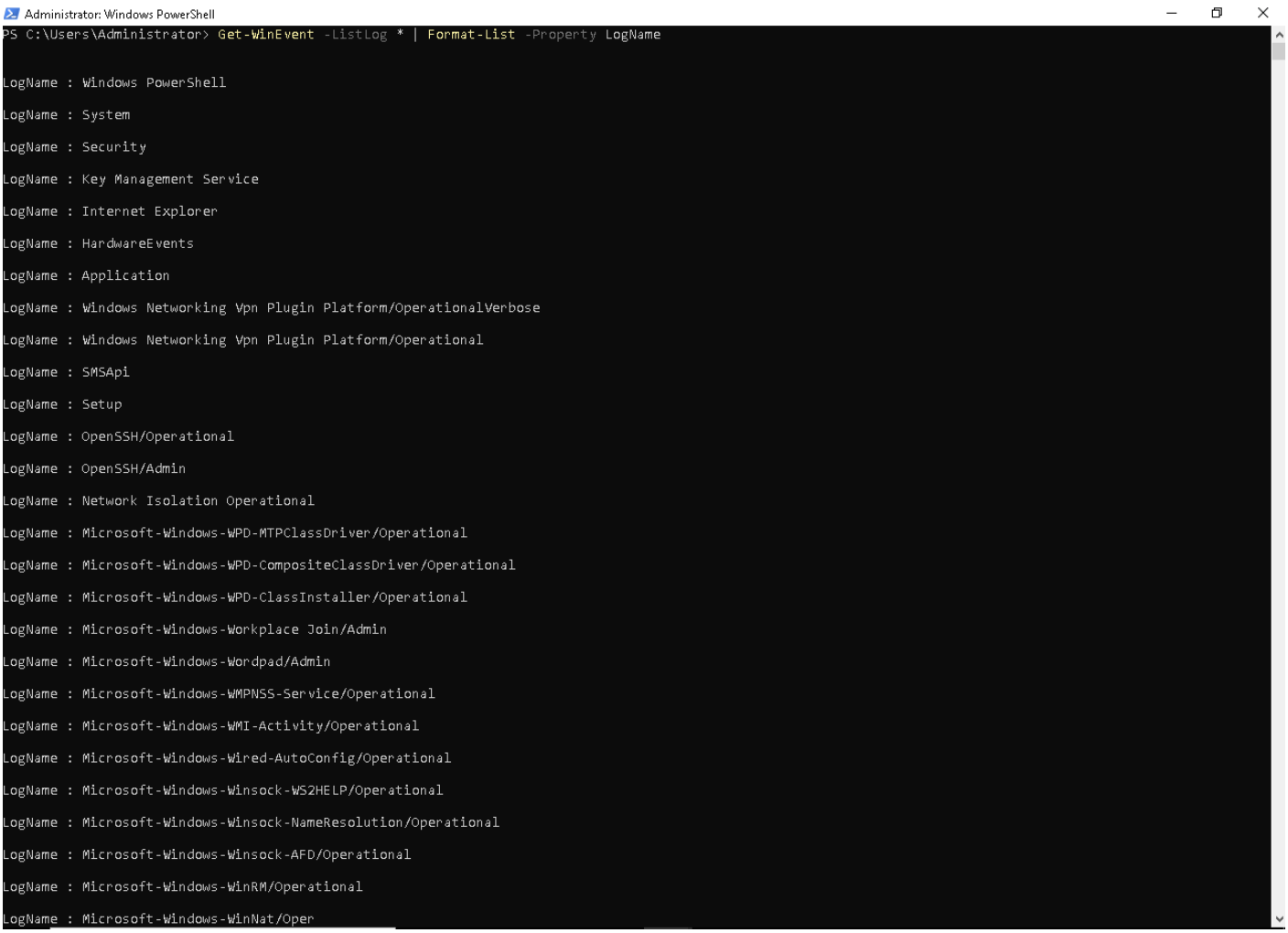
Custom Windows Event Logs - Integration

Custom Windows Event Logs

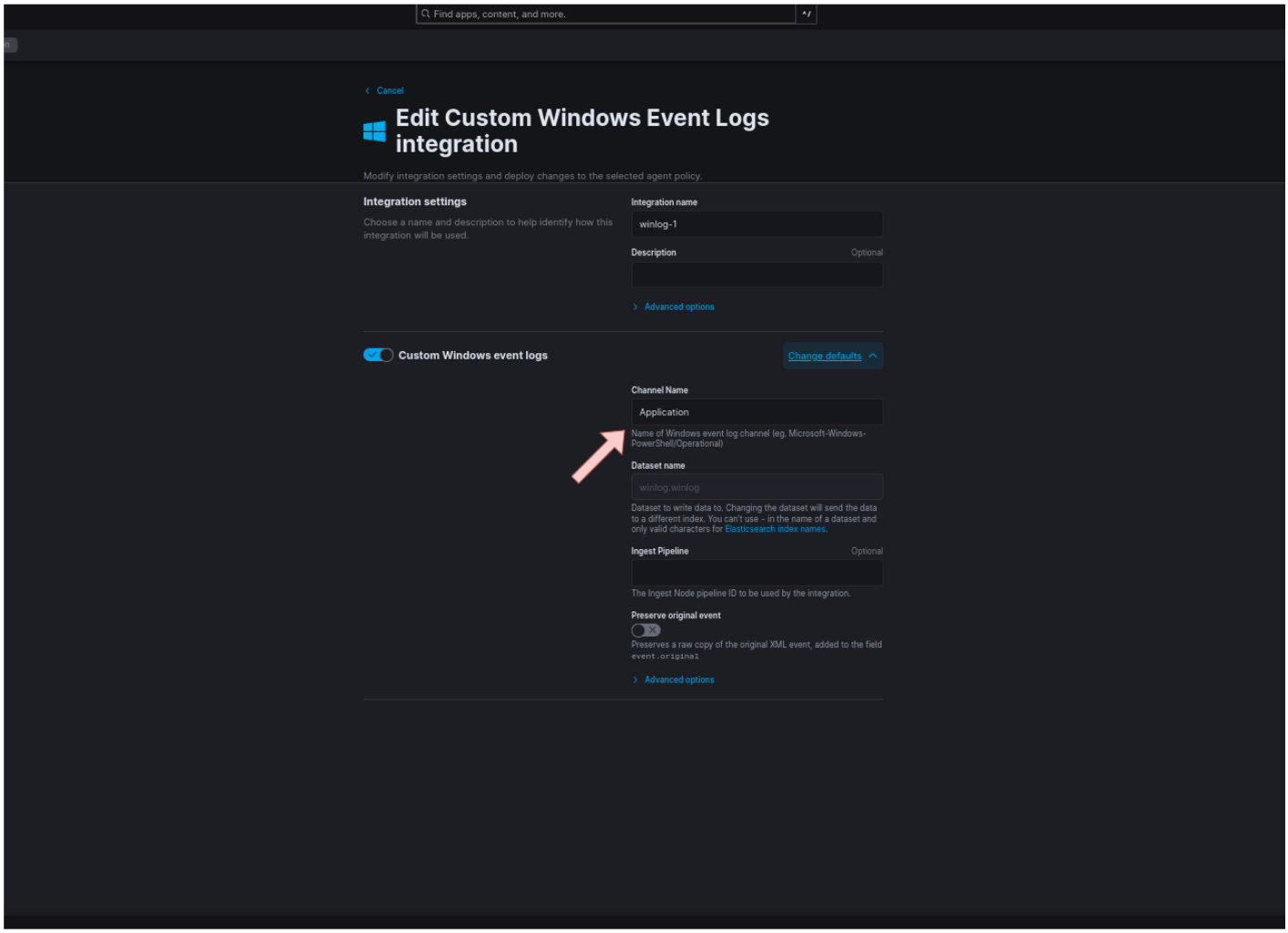
Collect and parse logs from any Windows event log channel with Elastic Agent.

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.



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



Revision #1
Created 22 October 2024 02:16:41 by Eduardo Dominico Llosa
Updated 22 October 2024 06:49:33 by Eduardo Dominico Llosa