Add Windows Integrations

Introduction

The Windows integration allows you to monitor the Windows OS, services, applications, and more.

- https://docs.microsoft.com/

Use the Windows integration to collect metrics and logs from your machine. Then visualize that data in Kibana, create alerts to notify you if something goes wrong, and reference data when troubleshooting an issue.

For example, if you wanted to know if a Windows service unexpectedly stops running, you could install the Windows integration to send service metrics to Elastic. Then, you could view real-time changes to service status in Kibana's [Metrics Windows] Services dashboard.

Data streams

The Windows integration collects two types of data: logs and metrics.

Logs help you keep a record of events that happen on your machine. Log data streams collected by the Windows integration include forwarded events, PowerShell events, and Sysmon events. Log collection for the Security, Application, and System event logs is handled by the System integration. See more details in the Logs reference.

- https://aquila-elk.kb.us-east-1.aws.found.io:9243/app/integrations/detail/windows-1.15.2/overview#logs-reference

Metrics give you insight into the state of the machine. Metric data streams collected by the Windows integration include service details and performance counter values. See more details in the Metrics reference.

- https://aquila-elk.kb.us-east-1.aws.found.io:9243/app/integrations/detail/windows-1.15.2/overview#metrics-reference

Note: For 7.11, security, application and system logs have been moved to the system package.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Requirements

You need Elasticsearch for storing and searching your data and Kibana for visualizing and managing it. You can use our hosted Elasticsearch Service on Elastic Cloud, which is recommended, or self-manage the Elastic Stack on your own hardware.

Each data stream collects different kinds of metric data, which may require dedicated permissions to be fetched and which may vary across operating systems.

Setup

For step-by-step instructions on how to set up an integration, see the Getting started guide.

- https://www.elastic.co/guide/en/welcome-to-elastic/current/getting-started-observability.html

Note: Because the Windows integration always applies to the local server, the hosts config option is not needed.

Ingesting Windows Events via Splunk

This integration allows you to seamlessly ingest data from a Splunk Enterprise instance. The integration uses the httpjson input in Elastic Agent to run a Splunk search via the Splunk REST API and then extract the raw event from the results. The raw event is then processed via the Elastic Agent. You can customize both the Splunk search query and the interval between searches. For more information see Ingest data from Splunk.

- https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-input-httpjson.html
- https://www.elastic.co/guide/en/observability/current/ingest-splunk.html

Note: This integration requires Windows Events from Splunk to be in XML format. To achieve this, renderXml needs to be set to 1 in your inputs.conf file.

Logs reference

Forwarded

The Windows forwarded data stream provides events from the Windows ForwardedEvents event log. The fields will be the same as the channel specific data streams.

Powershell

The Windows powershell data stream provides events from the Windows Windows PowerShell event log.

System Integration Procedures

Collect events from the following Windows event log channels: (Enable Yes/No)

1. Preserve original event (Enable Yes/No)

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

2. Event ID

- A list of included and excluded (blocked) event IDs. The value is a comma-separated list. The accepted values are single event IDs to include (e.g. 4624), a range of event IDs to include (e.g. 4700-4800), and single event IDs to exclude (e.g. -4735). Limit 22 IDs.

3. Ignore events older than

- If this option is specified, events that are older than the specified amount of time are ignored. Valid time units are "ns", "us" (or "μs"), "ms", "s", "m", "h".

4. Language ID

- The language ID the events will be rendered in. The language will be forced regardless of the system language. A complete list of language IDs can be found https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-lcid/a9eac961-e77d-41a6-90a5-ce1a8b0cdb9c[here]. It defaults to 0, which indicates to use the system language. E.g.: 0x0409 for en-US

5. Tags

6. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

7. Synthetic source (Enable Yes/No)

Powershell (Enable Yes/No)

1. Preserve original event (Enable Yes/No)

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

2. Event ID

- A list of included and excluded (blocked) event IDs. The value is a comma-separated list. The accepted values are single event IDs to include (e.g. 4624), a range of event IDs to include (e.g. 4700-4800), and single event IDs to exclude (e.g. -4735). Limit 22 IDs.

3. Ignore events older than

- If this option is specified, events that are older than the specified amount of time are ignored. Valid time units are "ns", "us" (or "µs"), "ms", "s", "m", "h".

4. Language ID

- The language ID the events will be rendered in. The language will be forced regardless of the system language. A complete list of language IDs can be found https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-lcid/a9eac961-e77d-41a6-90a5-ce1a8b0cdb9c[here]. It defaults to 0, which indicates to use the system language. E.g.: 0x0409 for en-US

5. Tags

6. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

7. Synthetic source (Enable Yes/No)

Powershell Operational (Enable Yes/No)

1. Preserve original event (Enable Yes/No)

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

2. Event ID

- A list of included and excluded (blocked) event IDs. The value is a comma-separated list. The accepted values are single event IDs to include (e.g. 4624), a range of event IDs to include (e.g. 4700-4800), and single event IDs to exclude (e.g. -4735). Limit 22 IDs.

3. Ignore events older than

- If this option is specified, events that are older than the specified amount of time are ignored. Valid time units are "ns", "us" (or "µs"), "ms", "s", "m", "h".

4. Language ID

- The language ID the events will be rendered in. The language will be forced regardless of the system language. A complete list of language IDs can be found https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-lcid/a9eac961-e77d-41a6-90a5-ce1a8b0cdb9c[here]. It defaults to 0, which indicates to use the system language. E.g.: 0x0409 for en-US

5. Tags

6. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

7. Synthetic source (Enable Yes/No)

Sysmon Operational (Enable Yes/No)

1. Preserve original event (Enable Yes/No)

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

2. Event ID

- A list of included and excluded (blocked) event IDs. The value is a comma-separated list. The accepted values are single event IDs to include (e.g. 4624), a range of event IDs to include (e.g. 4700-4800), and single event IDs to exclude (e.g. -4735). Limit 22 IDs.

3. Ignore events older than

- If this option is specified, events that are older than the specified amount of time are ignored. Valid time units are "ns", "us" (or "μs"), "ms", "s", "m", "h".

4. Language ID

- The language ID the events will be rendered in. The language will be forced regardless of the system language. A complete list of language IDs can be found https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-lcid/a9eac961-e77d-41a6-90a5-ce1a8b0cdb9c[here]. It defaults to 0, which indicates to use the system language. E.g.: 0x0409 for en-US

5. Tags

6. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

7. Synthetic source (Enable Yes/No)

Collect Windows perfmon and service metrics (Enable Yes/No)

1. Perfmon Group Measurements By Instance (Enable Yes/No)

- Enabling this option will send all measurements with a matching perfmon instance as part of a single event

2. Perfmon Ignore Non Existent Counters (Enable Yes/No)

- Enabling this option will make sure to ignore any errors caused by counters that do not exist

3. Perfmon Queries

- Will list the perfmon queries to execute, each query will have an object option, an optional instance contiguration and the actual counters

4. Period

5. Synthetic source (Enable Yes/No)

Windows service metrics (Enable Yes/No)

1. Period

2. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

3. Synthetic source (Enable Yes/No)

Collect logs from third-party REST API (experimental) (Enable Yes/No)

1. URL of Splunk Enterprise Server

- i.e. scheme://host:port, path is automatic

2. Splunk REST API Username

3. Splunk Authorization Token

- Bearer Token or Session Key, e.g. "Bearer eyJFd3e46..." or "Splunk 192fd3e...". Cannot be used with username and password.

4. SSL Configuration

- i.e. certificate_authorities, supported_protocols, verification_mode etc.
-

Windows ForwardedEvents via Splunk Enterprise REST API (Enable Yes/No)

1. Interval to query Splunk Enterprise REST API

- Go Duration syntax (eg. 10s)

2. Preserve original event (Enable Yes/No)

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

3. Splunk search string

4. Tags

5. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

6. Synthetic source (Enable Yes/No)
7.

Windows Powershell Events via Splunk Enterprise REST API (Enable Yes/No)

1. Interval to query Splunk Enterprise REST API

- Go Duration syntax (eg. 10s)

2. Preserve original event (Enable Yes/No)

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

3. Splunk search string

4. Tags

5. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

6. Synthetic source (Enable Yes/No)

Windows Powershell Operational Events via Splunk Enterprise REST API (Enable Yes/No)

1. Interval to query Splunk Enterprise REST API

- Go Duration syntax (eg. 10s)

2. Preserve original event (Enable Yes/No)

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

3. Splunk search string

4. Tags

5. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

6. Synthetic source (Enable Yes/No)

Windows Sysmon Operational Events via Splunk Enterprise REST API (Enable Yes/No)

1. Interval to query Splunk Enterprise REST API

- Go Duration syntax (eg. 10s)

2. Preserve original event (Enable Yes/No)

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

3. Splunk search string

4. Tags

5. Processors

- Processors are used to reduce the number of fields in the exported event or to enhance the event with metadata. This executes in the agent before the logs are parsed. See Processors for details.

6. Synthetic source (Enable Yes/No)

Revision #2
Created 23 April 2024 10:12:55
Updated 19 June 2024 06:54:01