

Day 10 – Elasticsearch Ingest Data

ACQUISIZIONE DEI LOG DI SYSMON E WINDOWS DEFENDER

Elasticsearch Ingest Data

Dalla home della **Web UI** di **Elasticsearch** clicchiamo su 'Add Integrations', e scegliamo 'Custom Windows Logs events' che, come da definizione, ci permette di raccogliere dati dagli event logs di Windows.

Una volta scelta l'integrazione clicco su 'Add Custom Windows Event Logs'

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, play with a sample data set.

[+ Add integrations](#)[Try sample data](#)[Upload a file](#)

Custom Windows Event Logs



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



Lateral Movement Detection

ML package to detect lateral movement based on file transfer activity and Windows RDP events.



Windows

Collect logs and metrics from Windows OS and services with Elastic Agent.

[< Back to integrations](#)

Custom Windows Event Logs

Elastic Agent

[Overview](#)[Settings](#)[Configs](#)

Version
2.1.2

[+ Add Custom Windows Event Logs](#)

Custom Windows event log package

[Details](#)

Elasticsearch Ingest Data

Il **Field Mapping** si riferisce alla mappatura dei campi dei dati che vengono acquisiti da una fonte (ad esempio, Sysmon) e come questi campi vengono strutturati all'interno dell'indice di Elasticsearch.

Quando acquisisci dati da Sysmon (o da qualsiasi altro evento di Windows come Windows Defender), ogni evento contiene numerosi campi (**ad esempio, timestamp**, ID evento, indirizzi IP, ecc.).

Perché Elasticsearch possa indicizzare e cercare efficacemente questi campi, è importante che **ogni campo abbia un tipo di dato assegnato** (come stringa, numero, booleano, ecc.).

Per esempio: il campo @timestamp viene mappato come tipo date perché rappresenta una data.


All'interno della documentazione in molti casi troviamo una descrizione per ogni campo.

Elasticsearch Ingest Data

Diamo il nome e una descrizione all'integrazione e come Channel Name inseriamo il path di Sysmon indicato nelle proprietà dell'Event Viewer.

(vedi slide successiva)

[< Cancel](#)



Add Custom Windows Event Logs integration

Configure an integration for the selected agent policy.

1

Configure integration

Integration settings

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

Integration name

WIN-Sysmon

Description Optional

Collect Sysmon Logs

[Advanced options](#)


☒ Custom Windows event logs [Change defaults ^](#)

Channel Name

Microsoft-Windows-Sysmon/Operational

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 Pipeline Optional

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](#)

The image is a screenshot of the Windows Event Viewer application. The top pane shows a list of 15 events, all with an 'Information' icon and the text 'Information'. The bottom pane is titled 'Event 13, Sysmon' and has two tabs: 'General' and 'Details'. The 'Details' tab is selected, showing the following information: 'Registry value set', 'RuleName: -', 'Event Type: SetVa', 'Log Name:', 'Source:', and 'Event ID:'. The 'Level' column is partially visible at the bottom.

^
v

Elasticsearch Ingest Data

Qui invece selezioniamo l'agent di Windows configurato in precedenza e clicchiamo su 'Save and continue' in basso a destra.

2

Where to add this integration?

New hosts

Existing hosts

Agent policy

Agent policies are used to manage a group of integrations across a set of agents.

Agent policy

Windows-Policy



1 agent is enrolled with the selected agent policies.

Cancel

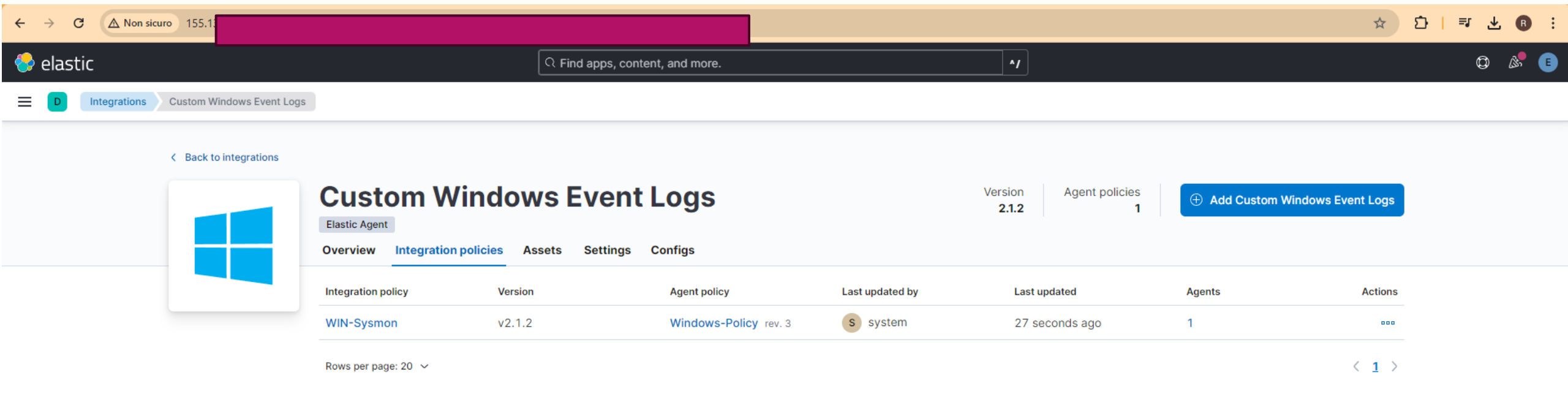
Preview API request



Save and continue

Elasticsearch Ingest Data

Questo è quanto ci risulterà alla fine, ripetiamo il processo per **Windows Defender**. La procedura è identica, cambia ovviamente il file da cui prenderemo il 'Channel Name' (slide successiva).




The screenshot shows the Elastic Agent console interface. At the top, there's a navigation bar with the Elastic logo and a search bar. Below it, the 'Integrations' tab is active, showing a list of integrations. The 'Custom Windows Event Logs' integration is highlighted, and its details are shown below. The details include a 'Back to integrations' link, a 'Custom Windows Event Logs' title, and a table of integration policies. The table has columns for Integration policy, Version, Agent policy, Last updated by, Last updated, Agents, and Actions. There is one row showing the 'WIN-Sysmon' integration policy, version v2.1.2, with agent policy 'Windows-Policy rev. 3', last updated by 'system', and last updated '27 seconds ago'. There is 1 agent associated with this policy. A button 'Add Custom Windows Event Logs' is also visible.

elastic Find apps, content, and more.

Integrations Custom Windows Event Logs

< Back to integrations

 Custom Windows Event Logs

Elastic Agent

Version 2.1.2 Agent policies 1

+ Add Custom Windows Event Logs

Overview Integration policies Assets Settings Configs

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
WIN-Sysmon	v2.1.2	Windows-Policy rev. 3	system	27 seconds ago	1	...

Rows per page: 20

< 1 >

Elasticsearch Ingest Data

Altra differenza importante è che nel caso del Defender ci limiteremo a monitorare 3 tipologie di eventi che sono il 1116, 1117 e 5001, che corrispondono a:

- Event ID 1116: Generalmente associato a notifiche relative al rilevamento di malware da parte di Windows Defender.
- Event ID 1117: Questo evento è solitamente legato a una rimozione di minacce da parte di Windows Defender.
- Event ID 5001: Questo evento è solitamente associato all'avvio o alla sospensione del servizio di protezione in tempo reale di Windows Defender.

Elasticsearch Ingest Data

Per configurarli andiamo sulle opzioni avanzate e li inseriamo nel campo Event ID.
(Se avessimo voluto escludere degli Event ID sarebbe bastato mettere un '-' prima dell'ID.

Ora avremo due integrations.

Advanced options

Providers

Optional

+ Add row

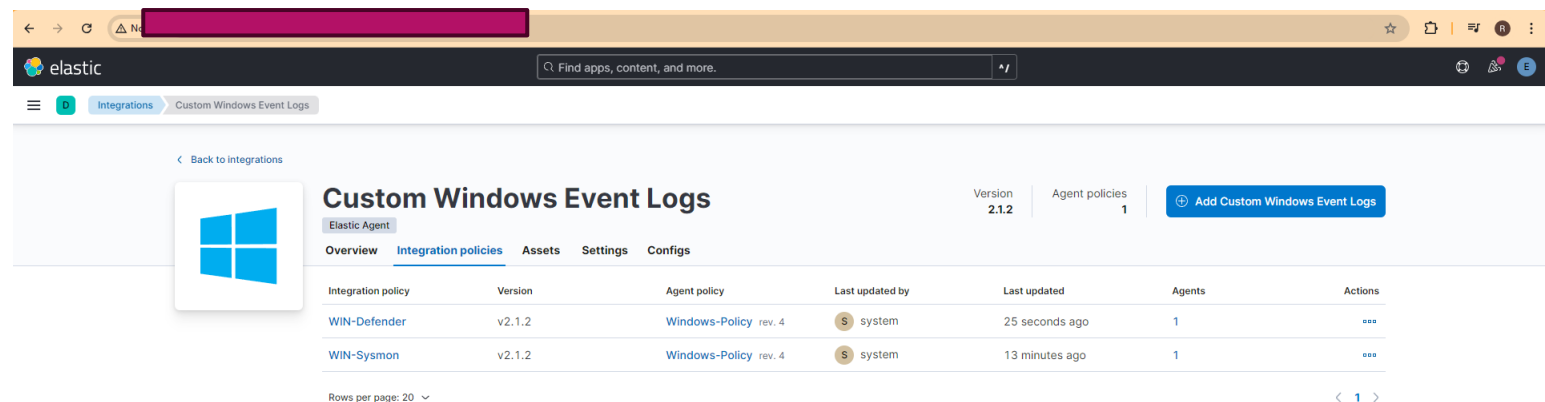
A list of providers (source names) to include.

Event ID

Optional

1116,1117,5001|

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 clauses, lower in some situations. See integration documentation for more details.



The screenshot shows the Elastic Agent configuration interface for Custom Windows Event Logs. The page title is "Custom Windows Event Logs" and it includes a "Back to integrations" link. The configuration is for the "Elastic Agent" and shows "Version 2.1.2" and "Agent policies 1". There is a button to "Add Custom Windows Event Logs". The main table lists the integration policies:

Integration policy	Version	Agent policy	Last updated by	Last updated	Agents	Actions
WIN-Defender	v2.1.2	Windows-Policy rev. 4	system	25 seconds ago	1	...
WIN-Sysmon	v2.1.2	Windows-Policy rev. 4	system	13 minutes ago	1	...

At the bottom, it shows "Rows per page: 20" and a pagination link "< 1 >".

Elasticsearch Ingest Data

Attualmente, non vedo alcuna attività dall'agent di **Windows** poiché il firewall di **Elasticsearch** non consente connessioni in entrata sulla porta 9200. Procederemo ad aggiungere una nuova regola senza specificare l'IP, poiché questa configurazione sarà utile per altri agent.


accept TCP 9200 0.0.0.0/0

WIN-johndoe

[Agent details](#) [Logs](#) [Diagnostics](#)

Overview

CPU ⓘ	N/A ⓘ
Memory ⓘ	N/A ⓘ
Status	Healthy
Last activity	15 seconds ago
Last checkin message	Running
Agent ID	62496ecd-b7b7-45d0-9011-696033bdfe47
Agent policy	Windows-Policy rev. 4
Agent version	8.15.1
Host name	WIN-johndoe
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	windows
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

 [View more agent metrics](#)

Elasticsearch Ingest Data

Ora come vediamo l'agent è attivo.
Quando andremo nel Discover riusciremo
ad effettuare le query per cercare gli
eventi id associati a **Sysmon** e **Defender**
come fa screen nelle slide successive.

[View all agents](#)

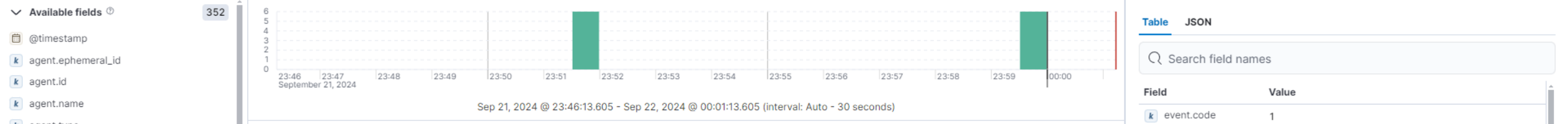
WIN-johndoe

[Agent details](#) [Logs](#) [Diagnostics](#)

Overview

CPU ⓘ	21.68 %
Memory ⓘ	165 MB
Status	Healthy
Last activity	32 seconds ago
Last checkin message	Running
Agent ID	62496ecd-b7b7-45d0-9011-696033bdf47
Agent policy	Windows-Policy rev. 4
Agent version	8.15.1
Host name	WIN-johndoe
Logging level	info
Privilege mode	Running as root
Agent release	stable
Platform	windows
Monitor logs	Enabled
Monitor metrics	Enabled
Tags	-

[View more agent metrics](#)



Documents (12) **Field statistics**

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tour Dismiss

@timestamp	Document
<input type="checkbox"/> Sep 21, 2024 @ 23:59:43.334	winlog.event_id 1 @timestamp Sep 21, 2024 @ 23:59:43.334 agent.ephemeral_id af304138-8c28-4379-88de-a68c3379
<input checked="" type="checkbox"/> Sep 21, 2024 @ 23:59:42.5	
<input checked="" type="checkbox"/> Sep 21, 2024 @ 23:59:42.5	
<input checked="" type="checkbox"/> Sep 21, 2024 @ 23:59:42.5	
<input checked="" type="checkbox"/> Sep 21, 2024 @ 23:59:41.5	

Rows per page: 100

Actions: View single document View surrounding documents

Search field names

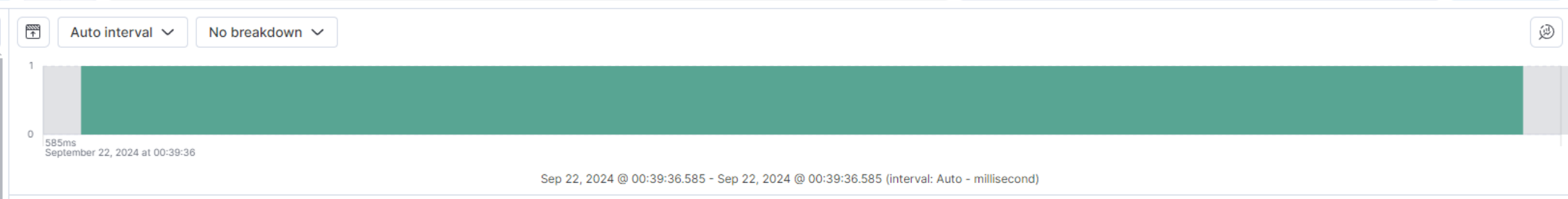
Field	Value
event.code	1
event.created	Sep 21, 2024 @ 23:59:57.498
event.dataset	winlog.winlog
event.ingested	Sep 22, 2024 @ 00:00:07.000
event.kind	event
event.provider	Microsoft-Windows-Sysmon
host.architecture	x86_64
host.hostname	win-johndoe
host.id	1fbfb8c7-de5a-4e45-aa2d-fd86bb31c5b5
host.ip	[fe80::5400:5ff:fe19:7718, 155.138.133.204]
host.mac	56-00-05-19-77-18
host.name	win-johndoe
host.os.build	20348.2655
host.os.family	windows
host.os.kernel	10.0.20348.2652 (WinBuild.160101.0800)
host.os.name	Windows Server 2022 Standard
host.os.platform	windows

Search field names 0

Available fields 355

- @timestamp
- agent.ephemeral_id
- agent.id
- agent.name
- agent.type
- agent.version
- cloud.availability_zone
- cloud.instance.id
- cloud.instance.name
- cloud.machine.type
- cloud.provider
- cloud.region
- cloud.service.name
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- ecs.version
- elastic_agent.id
- elastic_agent.snapshot
- elastic_agent.version
- event.action
- event.agent_id_status
- event.category
- event.code
- event.created

Add a field



Documents (1) Field statistics

Get the best look at your search results

Add relevant fields, reorder and sort columns, resize rows, and more in the document table.

Take the tour Dismiss

@timestamp	Document
Sep 22, 2024 @ 00:39:36.585	<pre>winlog.event_id 5001 @timestamp Sep 22, 2024 @ 00:39:36.585 agent.ephemeral_id 9d40a9ae-c181-4978-a1d2-1d187ab88278 agent.id 62496ecd-b7b7-45d0-9011-696033bdfc47 agent.name WIN-johndoe agent.type filebeat agent.version 8.15.1 cloud.availability_zone (empty) cloud.instance.id (empty) cloud.instance.name (empty) cloud.provider hetzner cloud.region (empty) cloud.service.name Cloud data_stream.dataset winlog.winlog data_stream.namespace default data_stream.type logs ecs.version 8.0.0 elastic_agent.id 62496ecd-b7b7-45d0-9011-696033bdfc47</pre>