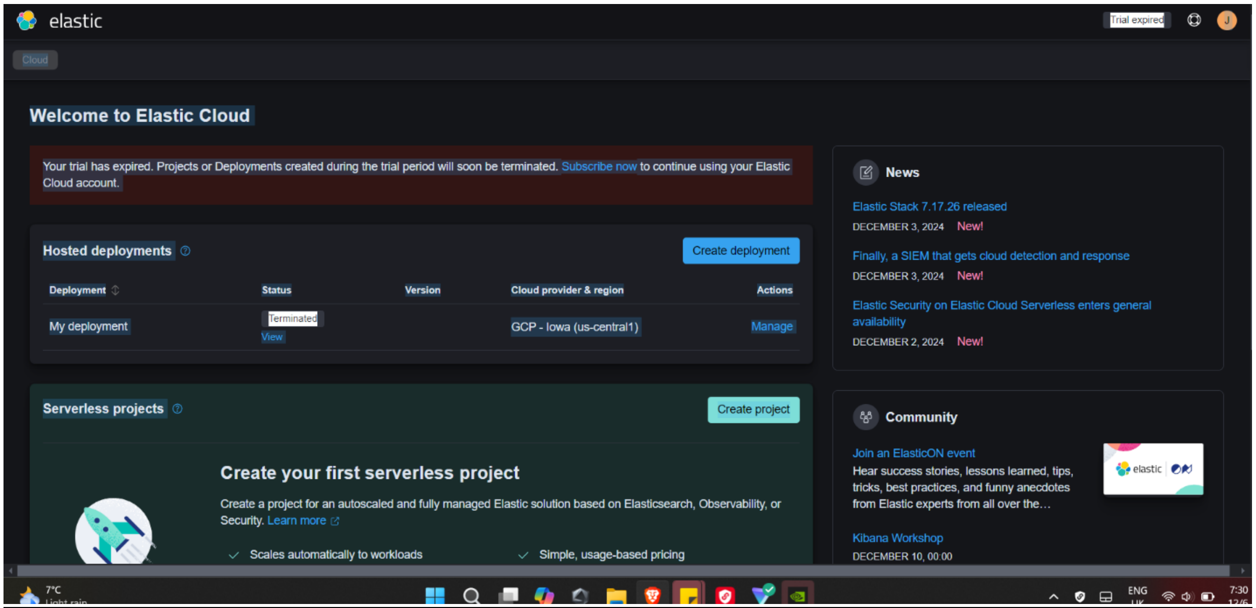
Images Document – SIEM tool Project

Done by **D.James Chrishan**



Welcome to Elastic Cloud

Your trial has expired. Projects or Deployments created during the trial period will soon be terminated. Subscribe now to continue using your Elastic Cloud account.

Hosted deployments

Deployment	Status	Version	Cloud provider & region	Actions
My deployment	Terminated View		GCP - Iowa (us-central1)	Manage

Serverless projects

Create your first serverless project

Create a project for an autoscaled and fully managed Elastic solution based on Elasticsearch, Observability, or Security. Learn more

✓ Scales automatically to workloads ✓ Simple, usage-based pricing

News

Elastic Stack 7.17.26 released
DECEMBER 3, 2024 New!

Finally, a SIEM that gets cloud detection and response
DECEMBER 3, 2024 New!

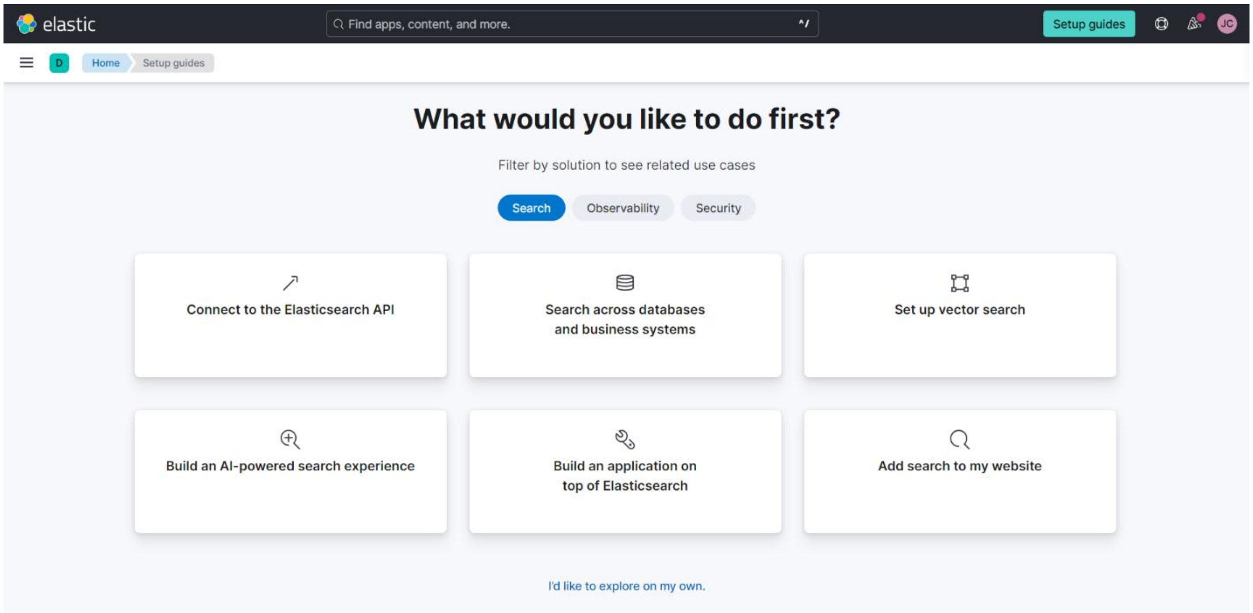
Elastic Security on Elastic Cloud Serverless enters general availability
DECEMBER 2, 2024 New!

Community

Join an ElasticON event
Hear success stories, lessons learned, tips, tricks, best practices, and funny anecdotes from Elastic experts from all over the…

Kibana Workshop
DECEMBER 10, 00:00

7°C
Light rain
ENG
UK
7:30

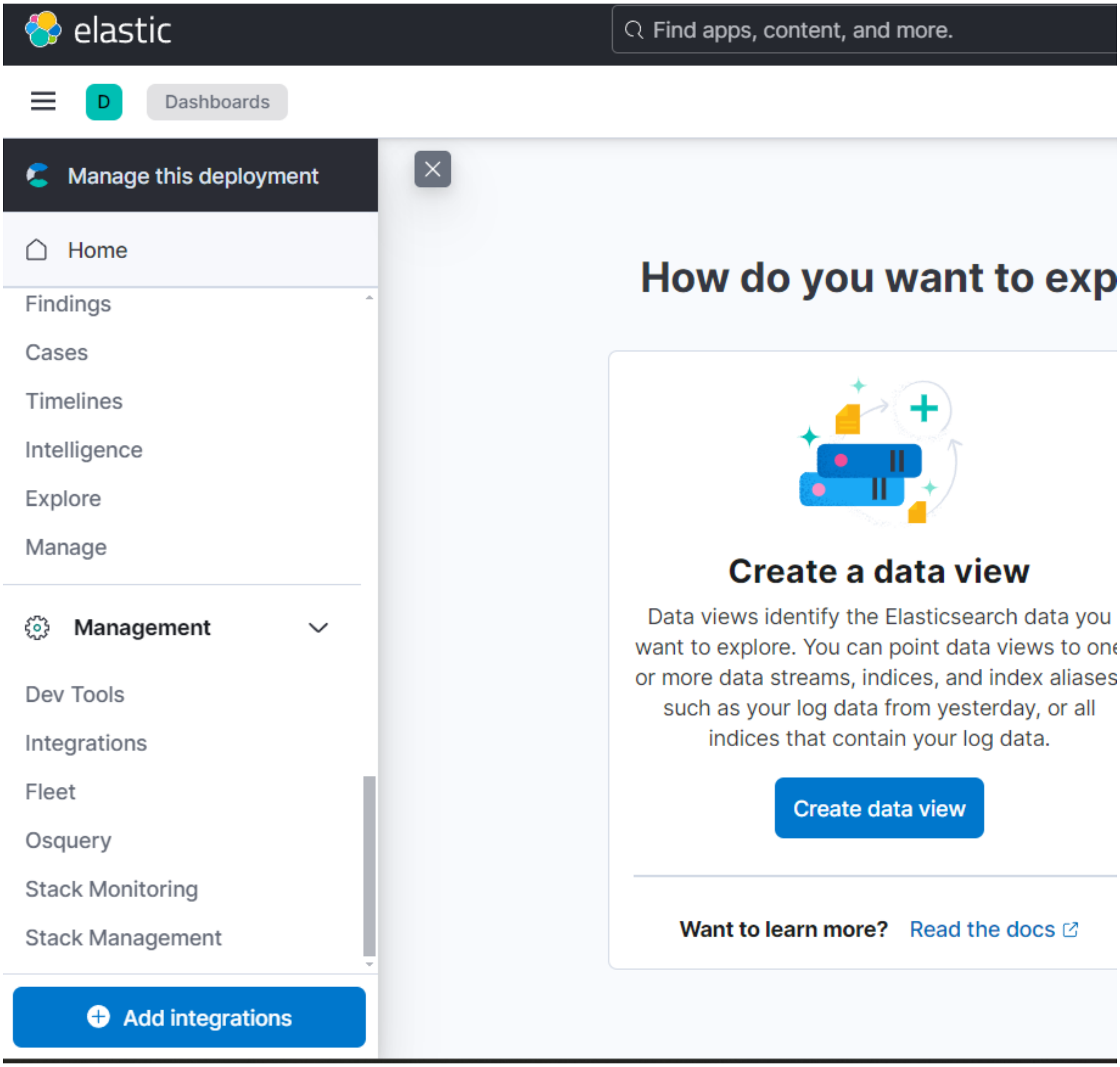


elastic
Find apps, content, and more.
Setup guides
JC
D
Home
Setup guides

What would you like to do first?

Filter by solution to see related use cases

Search
Observability
Security
Connect to the Elasticsearch API
Search across databases and business systems
Set up vector search
Build an AI-powered search experience
Build an application on top of Elasticsearch
Add search to my website
I'd like to explore on my own.

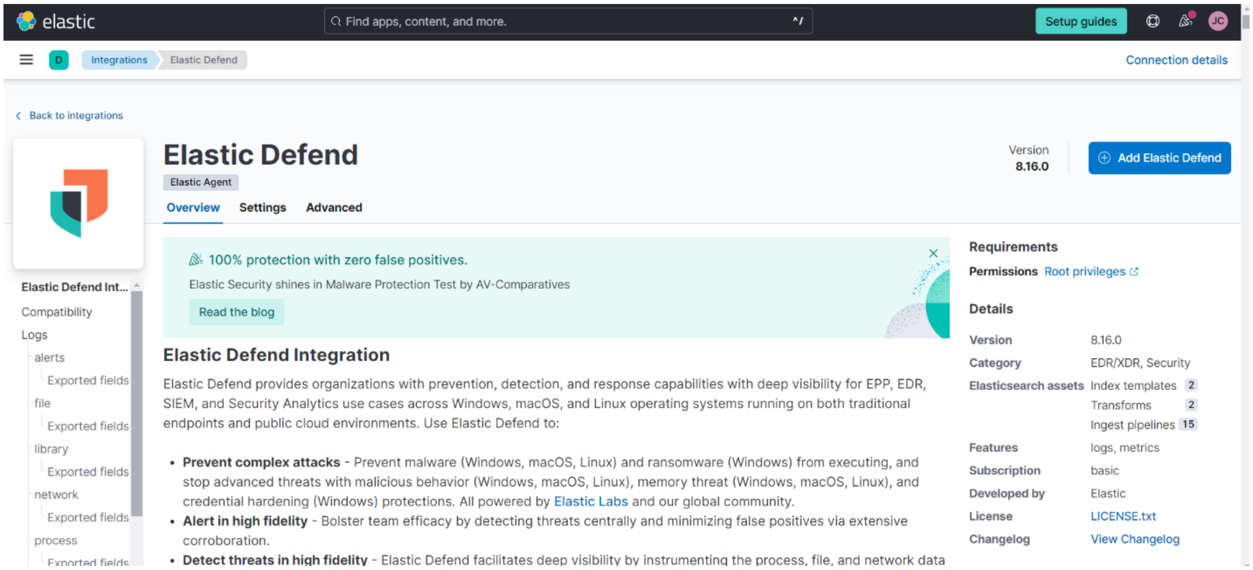


How do you want to exp

Create a data view

Data views identify the Elasticsearch data you want to explore. You can point data views to one or more data streams, indices, and index aliases such as your log data from yesterday, or all indices that contain your log data.

Want to learn more? Read the docs



Elastic Defend

Elastic Agent

100% protection with zero false positives.

Elastic Security shines in Malware Protection Test by AV-Comparatives

Elastic Defend Integration

Elastic Defend provides organizations with prevention, detection, and response capabilities with deep visibility for EPP, EDR, SIEM, and Security Analytics use cases across Windows, macOS, and Linux operating systems running on both traditional endpoints and public cloud environments. Use Elastic Defend to:

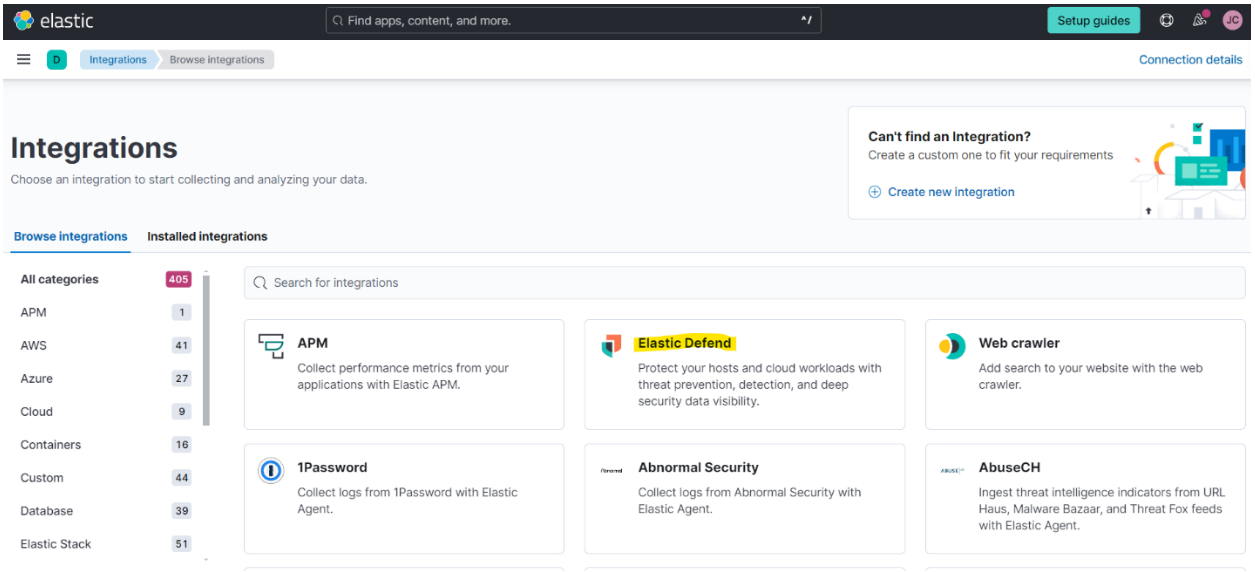
- **Prevent complex attacks** - Prevent malware (Windows, macOS, Linux) and ransomware (Windows) from executing, and stop advanced threats with malicious behavior (Windows, macOS, Linux), memory threat (Windows, macOS, Linux), and credential hardening (Windows) protections. All powered by Elastic Labs and our global community.
- **Alert in high fidelity** - Bolster team efficacy by detecting threats centrally and minimizing false positives via extensive corroboration.
- **Detect threats in high fidelity** - Elastic Defend facilitates deep visibility by instrumenting the process, file, and network data

Requirements

Permissions Root privileges

Details

Version	8.16.0
Category	EDR/XDR, Security
Elasticsearch assets	Index templates 2
	Transforms 2
	Ingest pipelines 15
Features	logs, metrics
Subscription	basic
Developed by	Elastic
License	LICENSE.txt
Changelog	View Changelog



Integrations

Choose an integration to start collecting and analyzing your data.

Can't find an Integration?

Create a custom one to fit your requirements

All categories	405
APM	1
AWS	41
Azure	27
Cloud	9
Containers	16
Custom	44
Database	39
Elastic Stack	51

APM
Collect performance metrics from your applications with Elastic APM.

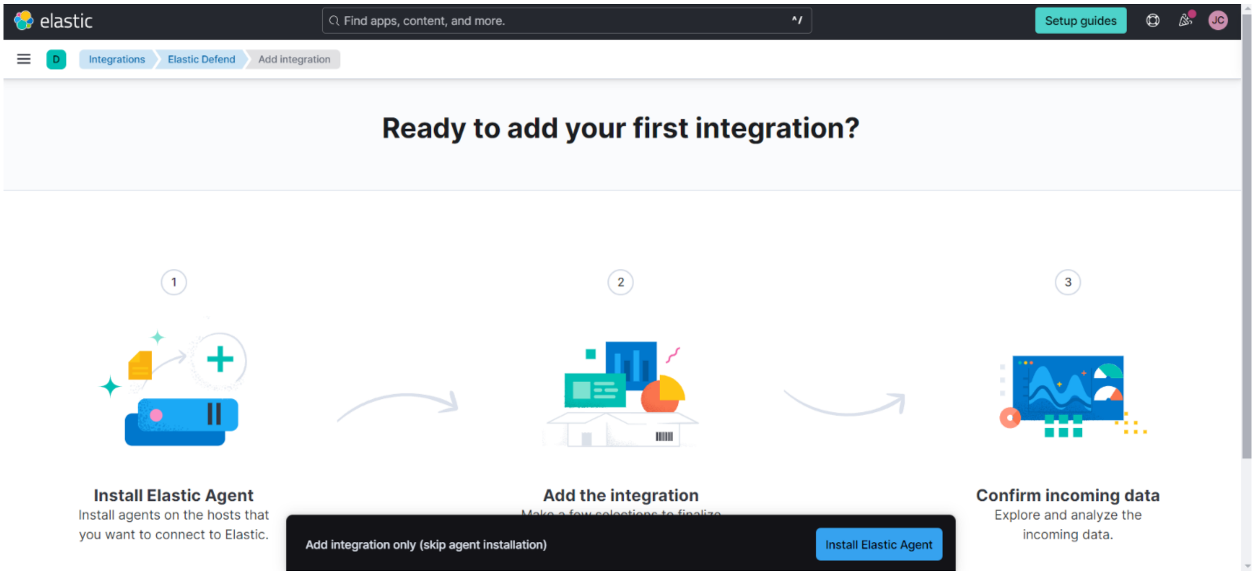
Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

Web crawler
Add search to your website with the web crawler.

1Password
Collect logs from 1Password with Elastic Agent.

Abnormal Security
Collect logs from Abnormal Security with Elastic Agent.

AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

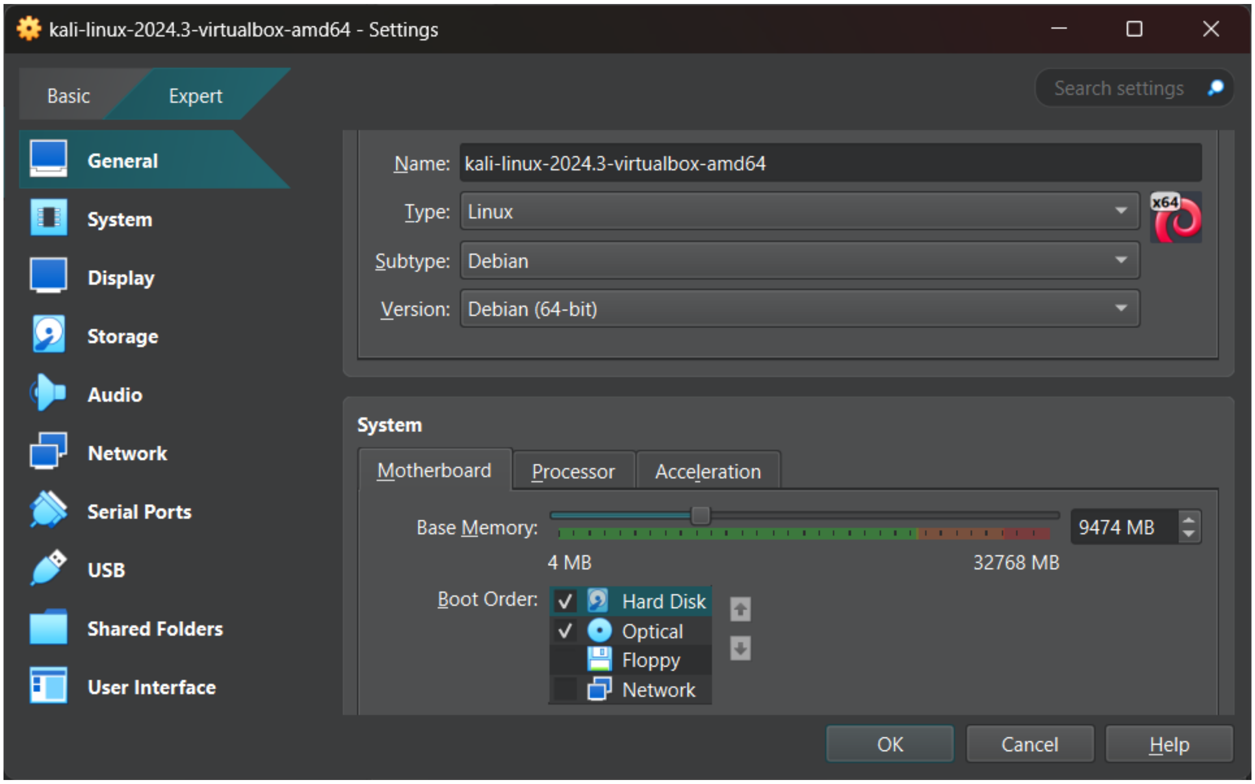


Ready to add your first integration?

1 **Install Elastic Agent**
Install agents on the hosts that you want to connect to Elastic.

2 **Add the integration**
Make a few selections to finalize

3 **Confirm incoming data**
Explore and analyze the incoming data.



Name: kali-linux-2024.3-virtualbox-amd64

Type: Linux

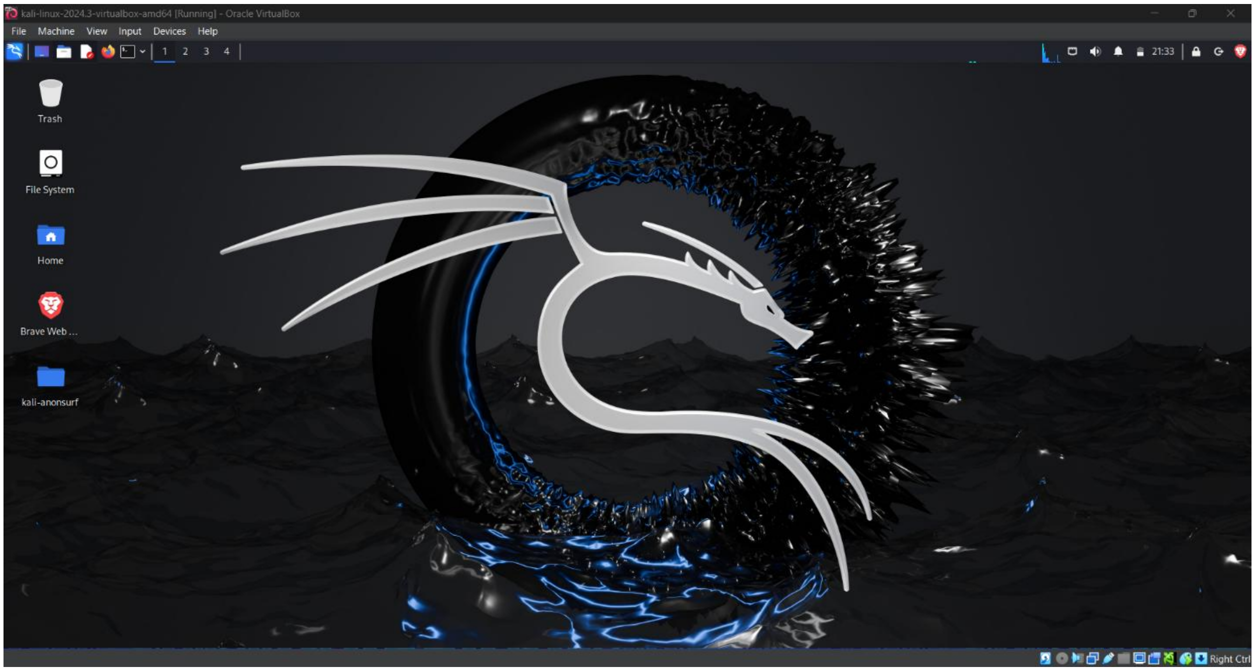
Subtype: Debian

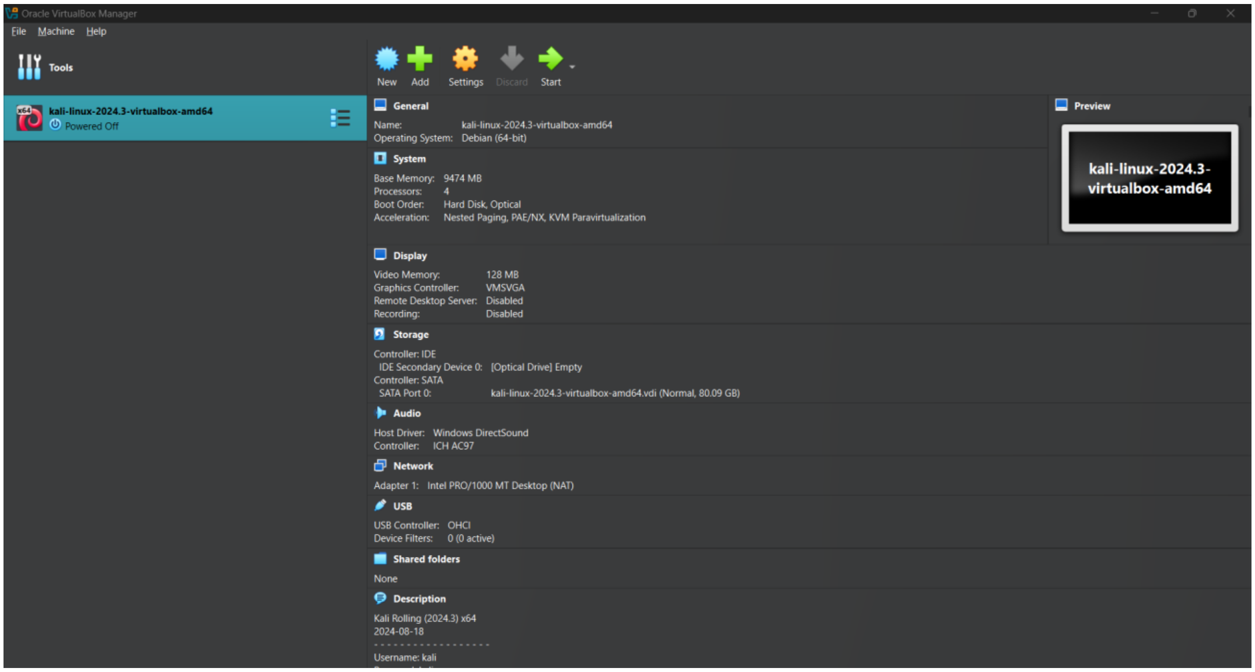
Version: Debian (64-bit)

System

Base Memory: 9474 MB

Boot Order:
☑ Hard Disk
☑ Optical
□ Floppy
□ Network





kali-linux-2024.3-virtualbox-amd64
Powered Off

General

Name: kali-linux-2024.3-virtualbox-amd64
Operating System: Debian (64-bit)

System

Base Memory: 9474 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Empty
Controller: SATA
SATA Port 0: kali-linux-2024.3-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

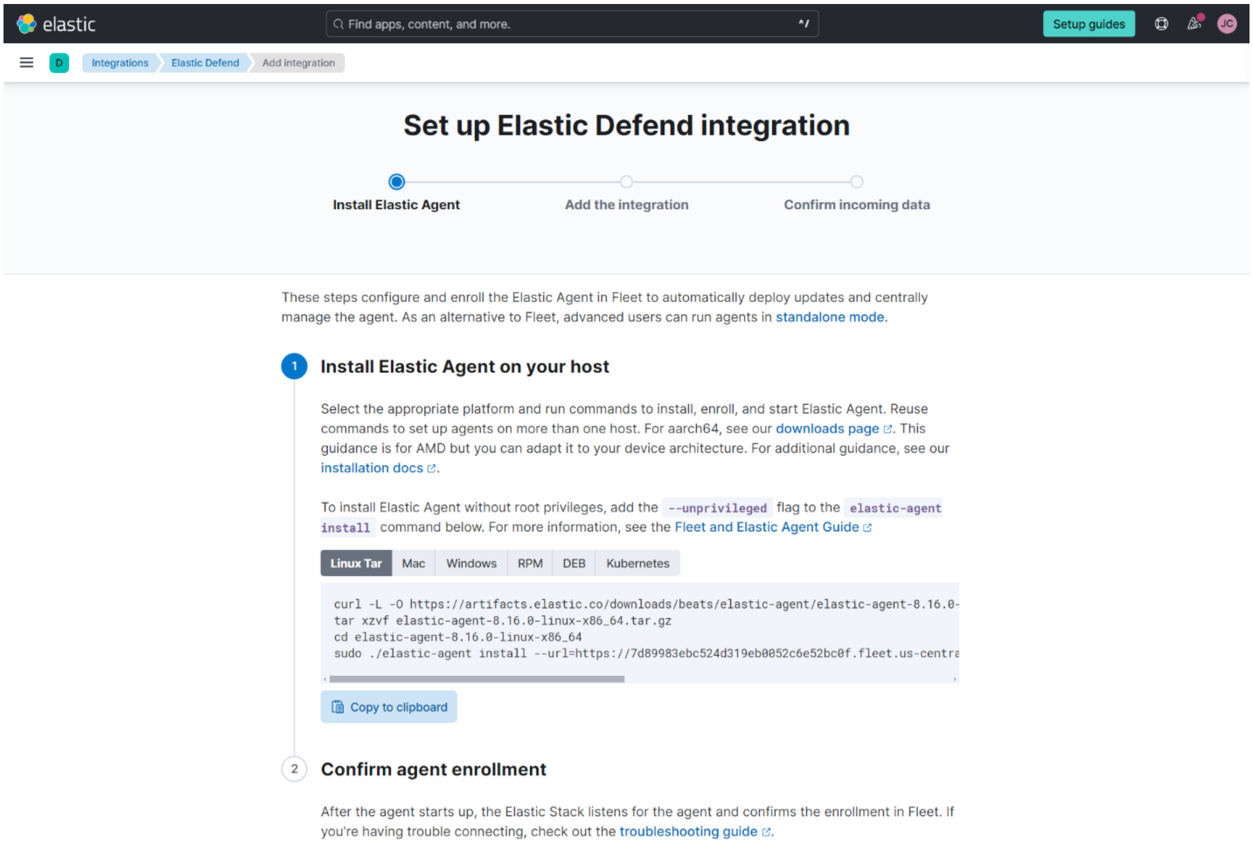
Shared folders

None

Description

Kali Rolling (2024.3) x64
2024-08-18

Username: kali



Set up Elastic Defend integration

These steps configure and enroll the Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent. As an alternative to Fleet, advanced users can run agents in standalone mode.

1 Install Elastic Agent on your host

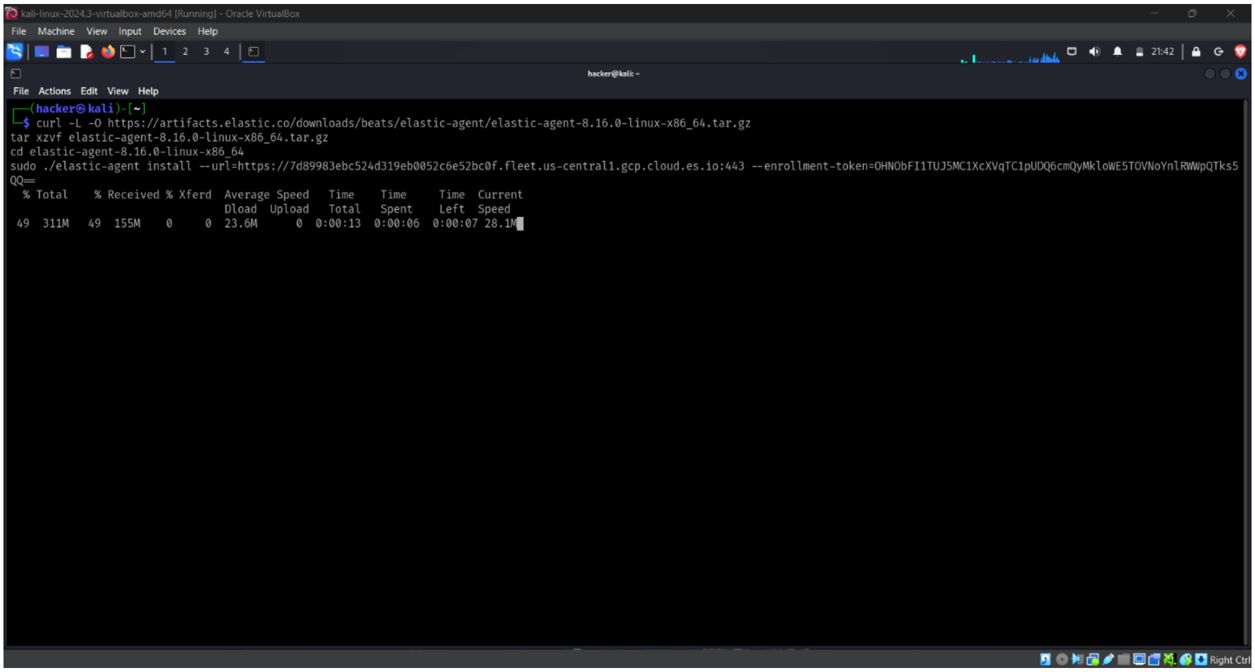
Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the Fleet and Elastic Agent Guide

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.0-
tar xzvf elastic-agent-8.16.0-linux-x86_64.tar.gz
cd elastic-agent-8.16.0-linux-x86_64
sudo ./elastic-agent install --url=https://7d89983ebc524d319eb0052c6e52bc0f.fleet.us-centra
```

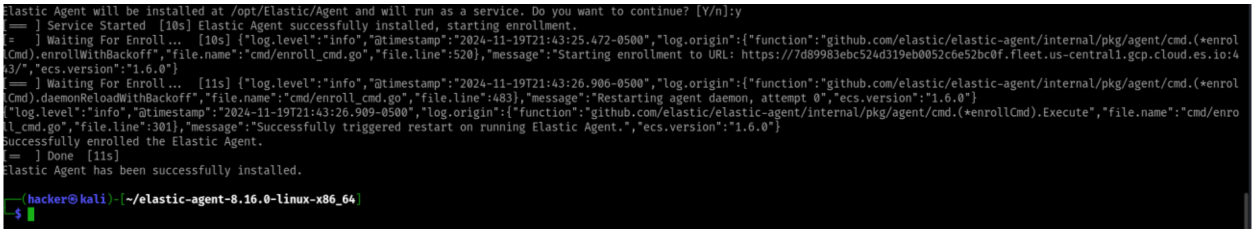
2 Confirm agent enrollment

After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the troubleshooting guide.

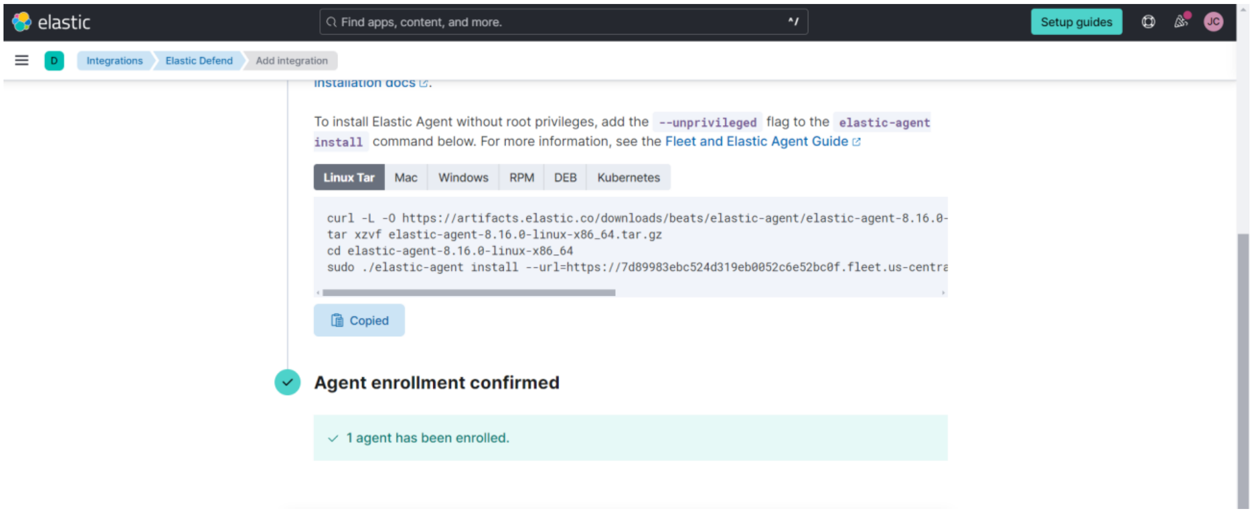


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
21:42
hacker@kali: ~
File Actions Edit View Help
Right Ctrl

```
┌──(hacker㉿kali)-[~]
└─$ curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.0-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.16.0-linux-x86_64.tar.gz
cd elastic-agent-8.16.0-linux-x86_64
sudo ./elastic-agent install --url=https://7d89983ebc524d319eb0052c6e52bc0f.fleet.us-central1.gcp.cloud.es.io:443 --enrollment-token=OHNObFI1TUJ5MC1XcXVqTC1pUDQ6cmQyMkloWE5TOVNoYnlRWWpQTks5
QQ==
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 49  311M   49  155M    0     0  23.6M      0  0:00:13  0:00:06  0:00:07 28.1M
```



```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want to continue? [Y/n]:y
[== ] Service Started  [10s] Elastic Agent successfully installed, starting enrollment.
[=  ] Waiting For Enroll...  [10s] {"log.level":"info","@timestamp":"2024-11-19T21:43:25.472-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrol
lCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":520},"message":"Starting enrollment to URL: https://7d89983ebc524d319eb0052c6e52bc0f.fleet.us-central1.gcp.cloud.es.io:4
43/","ecs.version":"1.6.0"}
[== ] Waiting For Enroll...  [11s] {"log.level":"info","@timestamp":"2024-11-19T21:43:26.906-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrol
lCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":483},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-11-19T21:43:26.909-0500","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enro
ll_cmd.go","file.line":301},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[=  ] Done  [11s]
Elastic Agent has been successfully installed.

┌──(hacker㉿kali)-[~/elastic-agent-8.16.0-linux-x86_64]
└─$
```



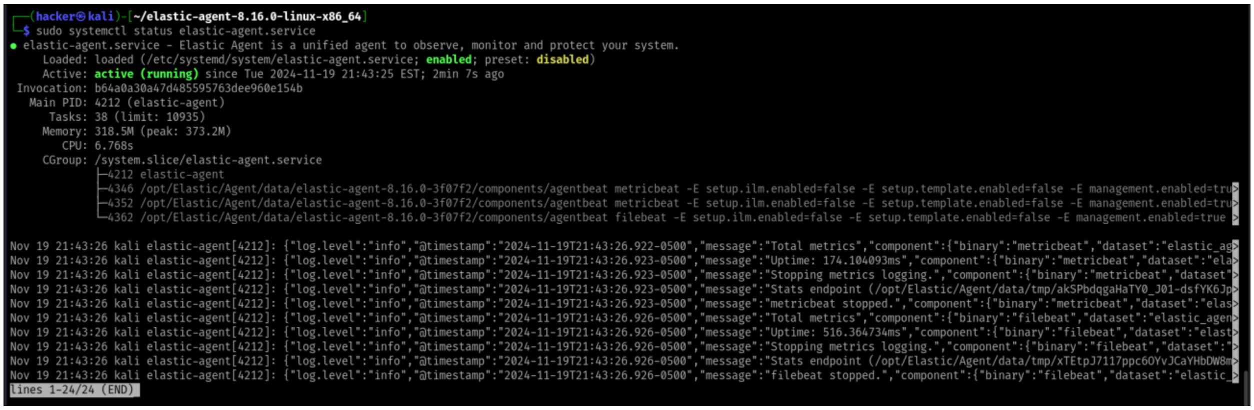
installation docs.

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the Fleet and Elastic Agent Guide

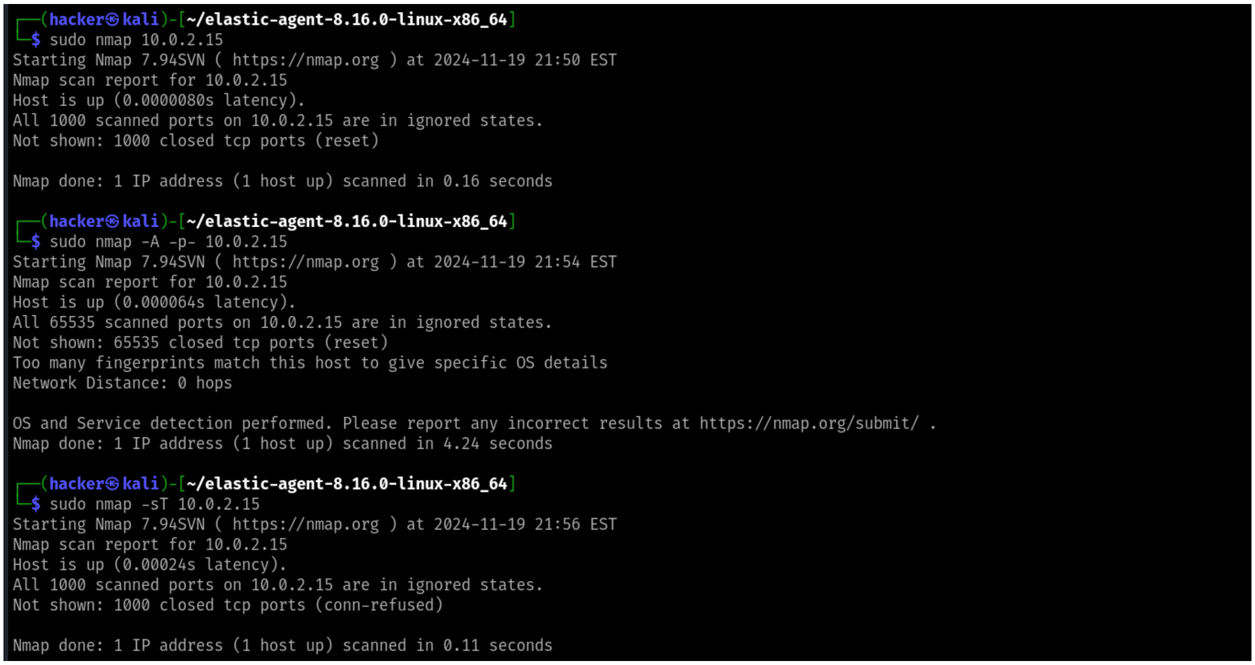
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.16.0-
tar xzvf elastic-agent-8.16.0-linux-x86_64.tar.gz
cd elastic-agent-8.16.0-linux-x86_64
sudo ./elastic-agent install --url=https://7d89983ebc524d319eb0052c6e52bc0f.fleet.us-centra
```

Agent enrollment confirmed

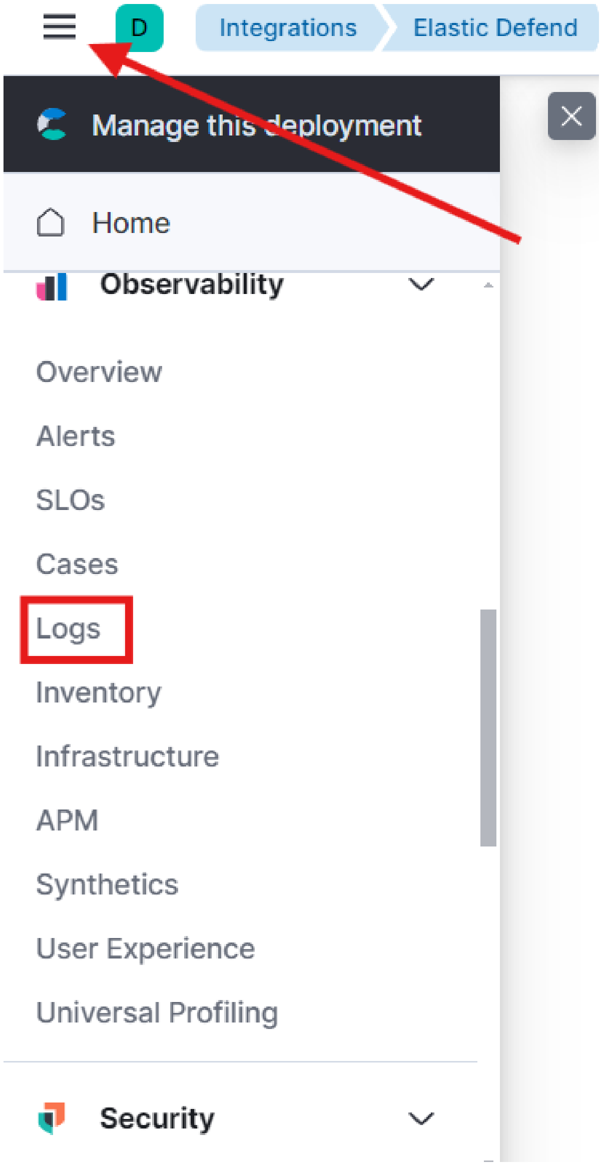
✓ 1 agent has been enrolled.

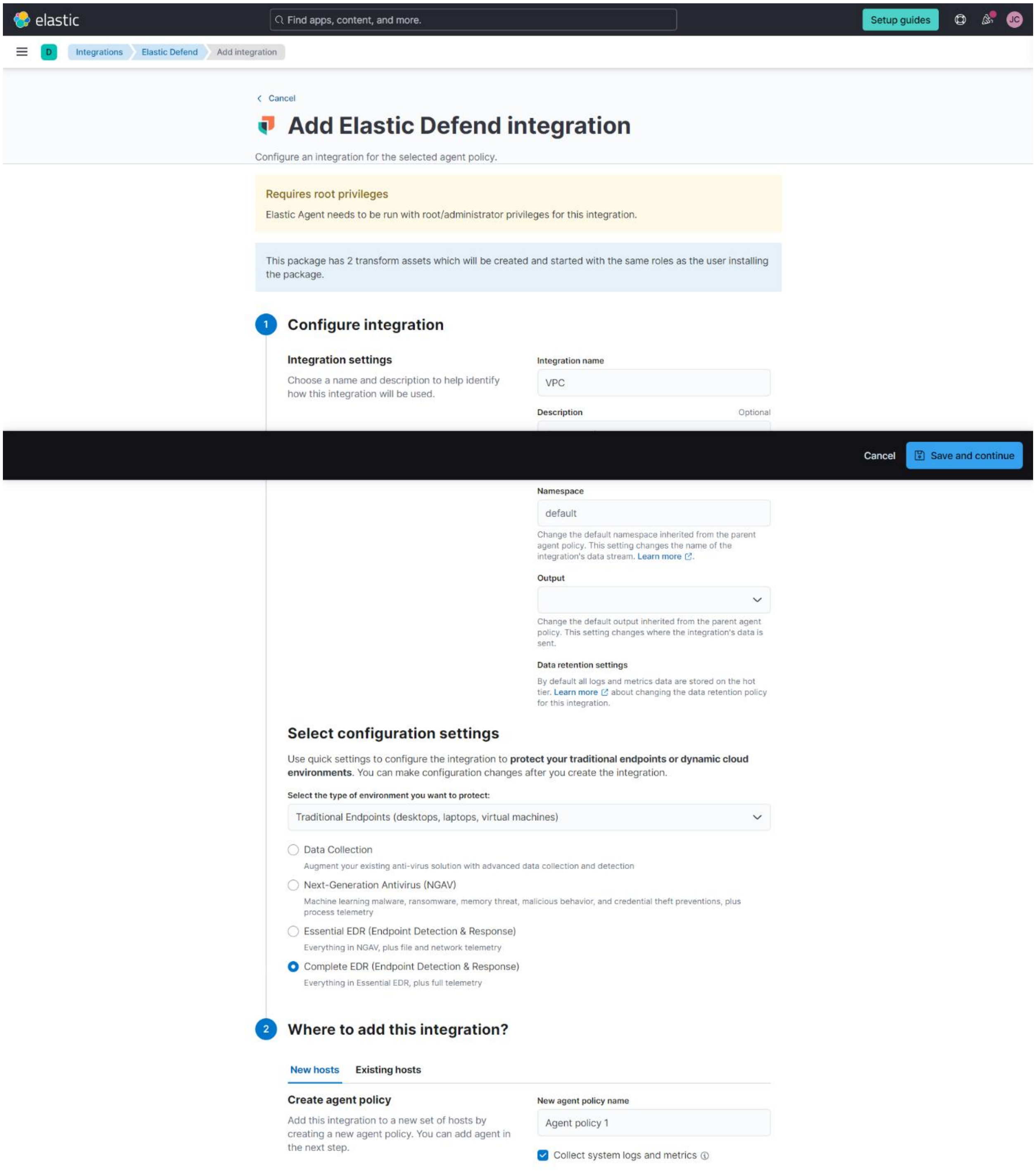


```
┌──(hacker㉿kali)-[~/elastic-agent-8.16.0-linux-x86_64]
└─$ sudo systemctl status elastic-agent.service
● elastic-agent.service - Elastic Agent is a unified agent to observe, monitor and protect your system.
     Loaded: loaded (/etc/systemd/system/elastic-agent.service; enabled; preset: disabled)
     Active: active (running) since Tue 2024-11-19 21:43:25 EST; 2min 7s ago
 Invocation: b64a0a30a47d485595763dee960e154b
   Main PID: 4212 (elastic-agent)
      Tasks: 38 (limit: 10935)
     Memory: 318.5M (peak: 373.2M)
        CPU: 6.768s
     CGroup: /system.slice/elastic-agent.service
             ├─4212 elastic-agent
             ├─4346 /opt/Elastic/Agent/data/elastic-agent-8.16.0-3f07f2/components/agentbeat metricbeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.enabled=tru>
             ├─4352 /opt/Elastic/Agent/data/elastic-agent-8.16.0-3f07f2/components/agentbeat metricbeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.enabled=tru>
             └─4362 /opt/Elastic/Agent/data/elastic-agent-8.16.0-3f07f2/components/agentbeat filebeat -E setup.ilm.enabled=false -E setup.template.enabled=false -E management.enabled=true >

Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.922-0500","message":"Total metrics","component":{"binary":"metricbeat","dataset":"elastic_ag>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.923-0500","message":"Uptime: 174.104093ms","component":{"binary":"metricbeat","dataset":"ela>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.923-0500","message":"Stopping metrics logging.","component":{"binary":"metricbeat","dataset">
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.923-0500","message":"Stats endpoint (/opt/Elastic/Agent/data/tmp/akSPbdqgaHaTY0_J01-dsfYK6Jp>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.923-0500","message":"metricbeat stopped.","component":{"binary":"metricbeat","dataset":"elas>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.926-0500","message":"Total metrics","component":{"binary":"filebeat","dataset":"elastic_agen>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.926-0500","message":"Uptime: 516.364734ms","component":{"binary":"filebeat","dataset":"elast>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.926-0500","message":"Stopping metrics logging.","component":{"binary":"filebeat","dataset":">
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.926-0500","message":"Stats endpoint (/opt/Elastic/Agent/data/tmp/xTEtpJ7117ppc6OYvJCaYHbDW8m>
Nov 19 21:43:26 kali elastic-agent[4212]: {"log.level":"info","@timestamp":"2024-11-19T21:43:26.926-0500","message":"filebeat stopped.","component":{"binary":"filebeat","dataset":"elastic_>
lines 1-24/24 (END)
```



```
┌──(hacker㉿kali)-[~/elastic-agent-8.16.0-linux-x86_64]
└─$ sudo nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 21:50 EST
Nmap scan report for 10.0.2.15
Host is up (0.0000080s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds

┌──(hacker㉿kali)-[~/elastic-agent-8.16.0-linux-x86_64]
└─$ sudo nmap -A -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 21:54 EST
Nmap scan report for 10.0.2.15
Host is up (0.000064s latency).
All 65535 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.24 seconds

┌──(hacker㉿kali)-[~/elastic-agent-8.16.0-linux-x86_64]
└─$ sudo nmap -sT 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 21:56 EST
Nmap scan report for 10.0.2.15
Host is up (0.00024s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
```


D
Integrations
Elastic Defend
Manage this deployment
Home
Observability
Overview
Alerts
SLOs
Cases
Logs
Inventory
Infrastructure
APM
Synthetics
User Experience
Universal Profiling
Security



Add Elastic Defend integration

Configure an integration for the selected agent policy.

Requires root privileges

Elastic Agent needs to be run with root/administrator privileges for this integration.

This package has 2 transform assets which will be created and started with the same roles as the user installing the package.

1 Configure integration

Integration settings

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

Integration name

VPC

Description Optional

Namespace

default

Change the default namespace inherited from the parent agent policy. This setting changes the name of the integration's data stream. Learn more.

Output

Change the default output inherited from the parent agent policy. This setting changes where the integration's data is sent.

Data retention settings

By default all logs and metrics data are stored on the hot tier. Learn more about changing the data retention policy for this integration.

Select configuration settings

Use quick settings to configure the integration to **protect your traditional endpoints or dynamic cloud environments**. You can make configuration changes after you create the integration.

Select the type of environment you want to protect:

Traditional Endpoints (desktops, laptops, virtual machines)

○ Data Collection
Augment your existing anti-virus solution with advanced data collection and detection

○ Next-Generation Antivirus (NGAV)
Machine learning malware, ransomware, memory threat, malicious behavior, and credential theft preventions, plus process telemetry

○ Essential EDR (Endpoint Detection & Response)
Everything in NGAV, plus file and network telemetry

● Complete EDR (Endpoint Detection & Response)
Everything in Essential EDR, plus full telemetry

2 Where to add this integration?

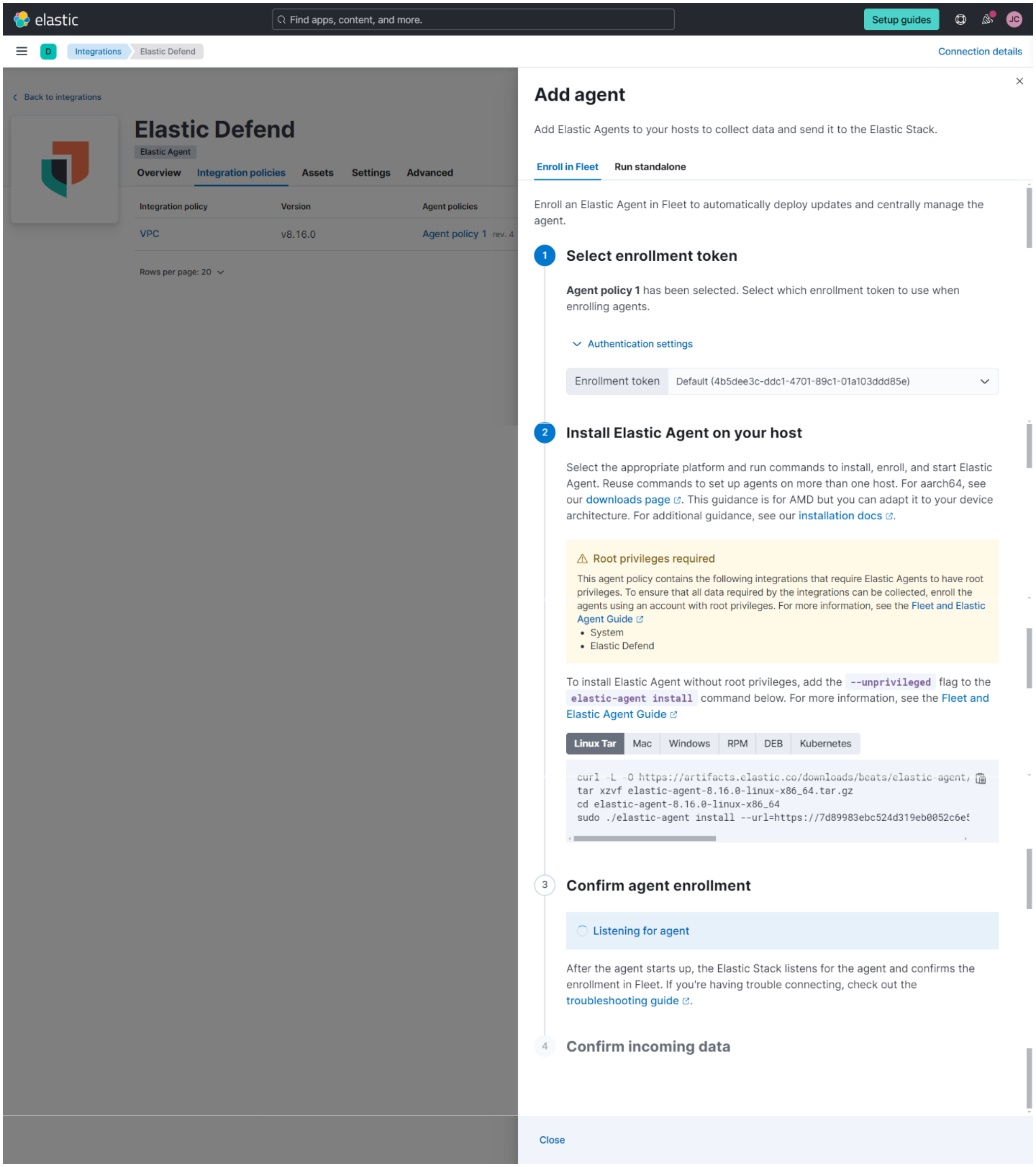
Create agent policy

Add this integration to a new set of hosts by creating a new agent policy. You can add agent in the next step.

New agent policy name

Agent policy 1

☑ Collect system logs and metrics



Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

Enroll an Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.

1 Select enrollment token

Agent policy 1 has been selected. Select which enrollment token to use when enrolling agents.

Enrollment token: Default (4b5dee3c-ddc1-4701-89c1-01a103ddd85e)

2 Install Elastic Agent on your host

Select the appropriate platform and run commands to install, enroll, and start Elastic Agent. Reuse commands to set up agents on more than one host. For aarch64, see our downloads page. This guidance is for AMD but you can adapt it to your device architecture. For additional guidance, see our installation docs.

⚠ Root privileges required

This agent policy contains the following integrations that require Elastic Agents to have root privileges. To ensure that all data required by the integrations can be collected, enroll the agents using an account with root privileges. For more information, see the Fleet and Elastic Agent Guide

- System
- Elastic Defend

To install Elastic Agent without root privileges, add the `--unprivileged` flag to the `elastic-agent install` command below. For more information, see the Fleet and Elastic Agent Guide

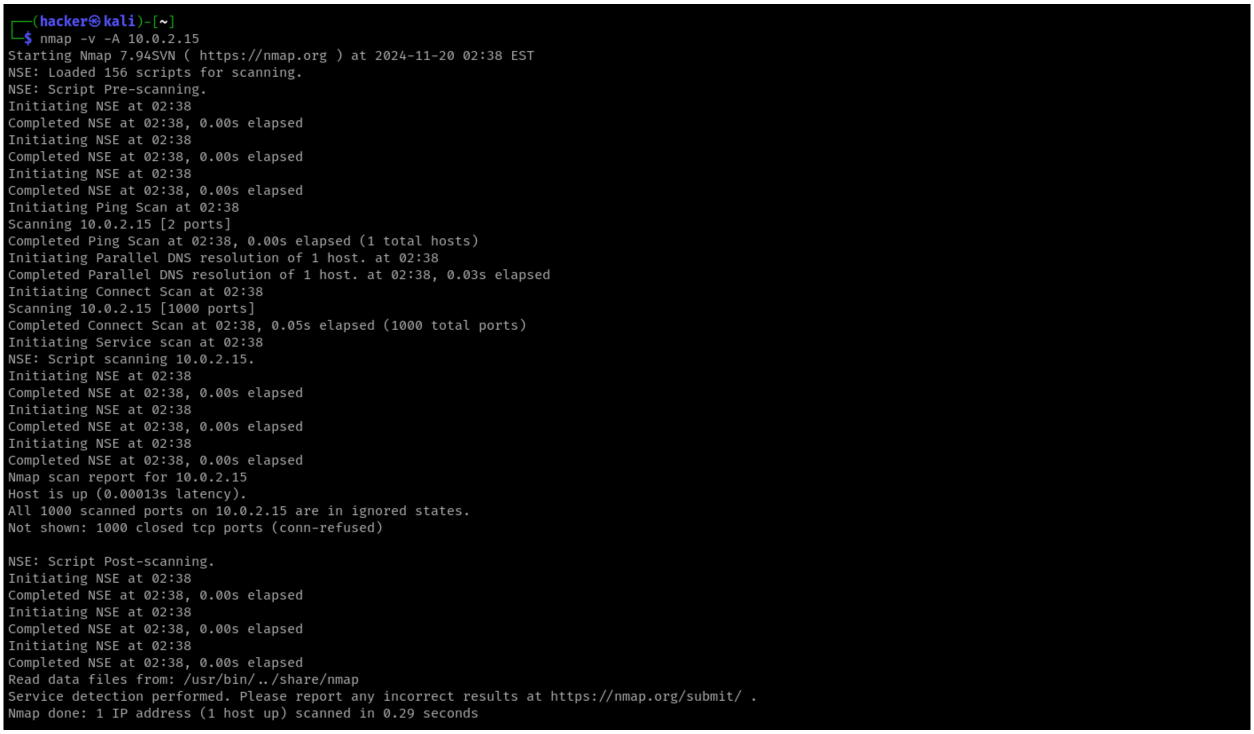
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/
tar xzvf elastic-agent-8.16.0-linux-x86_64.tar.gz
cd elastic-agent-8.16.0-linux-x86_64
sudo ./elastic-agent install --url=https://7d89983ebc524d319eb0052c6e5
```

3 Confirm agent enrollment

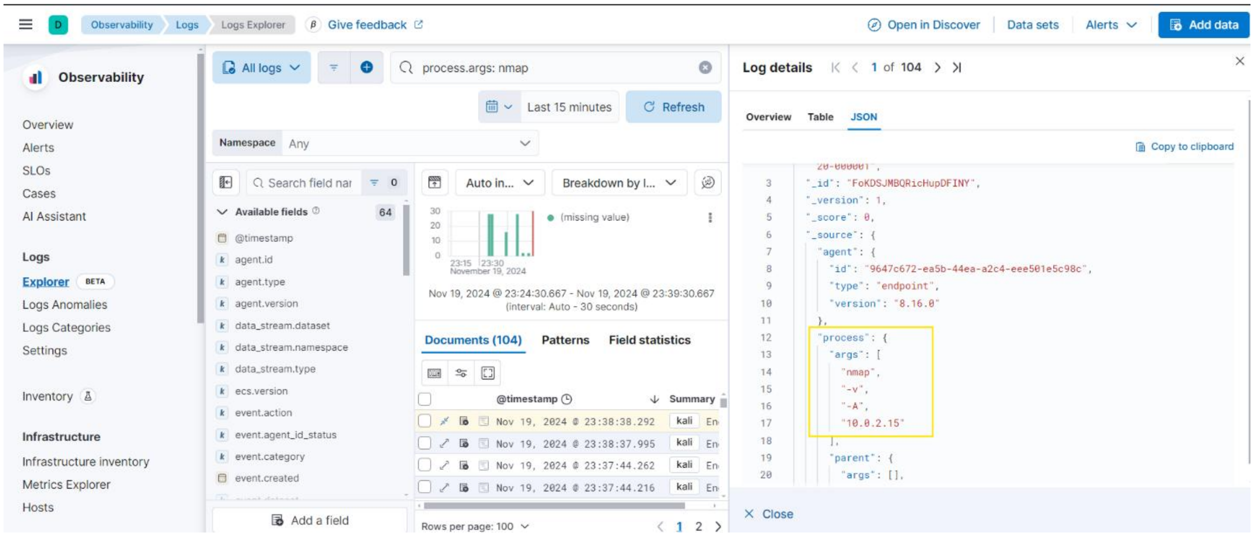
Listening for agent

After the agent starts up, the Elastic Stack listens for the agent and confirms the enrollment in Fleet. If you're having trouble connecting, check out the troubleshooting guide.

4 Confirm incoming data



```
┌──(hacker㉿kali)-[~]
└─$ nmap -v -A 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 02:38 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating Ping Scan at 02:38
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 02:38, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:38
Completed Parallel DNS resolution of 1 host. at 02:38, 0.03s elapsed
Initiating Connect Scan at 02:38
Scanning 10.0.2.15 [1000 ports]
Completed Connect Scan at 02:38, 0.05s elapsed (1000 total ports)
Initiating Service scan at 02:38
NSE: Script scanning 10.0.2.15.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

NSE: Script Post-scanning.
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Initiating NSE at 02:38
Completed NSE at 02:38, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
```



process.args: nmap

Namespace: Any

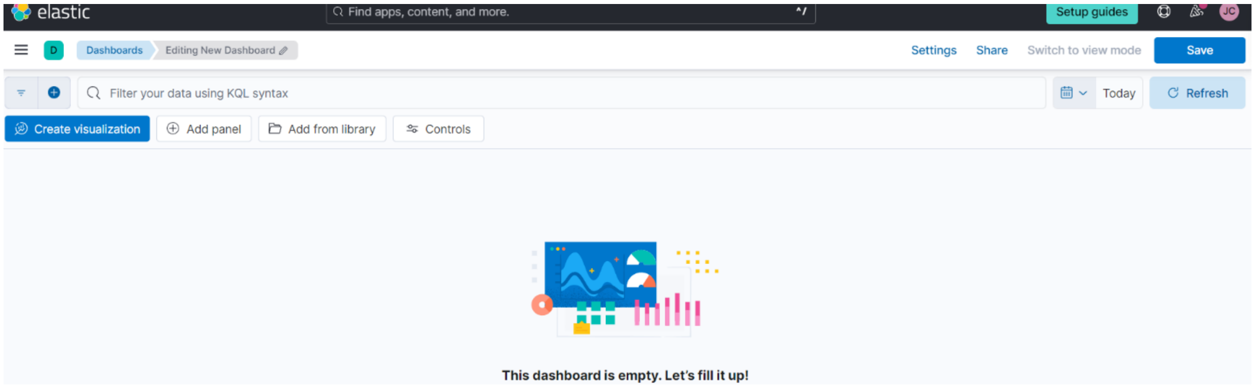
Available fields 64

- @timestamp
- agent.id
- agent.type
- agent.version
- data_stream.dataset
- data_stream.namespace
- data_stream.type
- ecs.version
- event.action
- event.agent_id_status
- event.category
- event.created

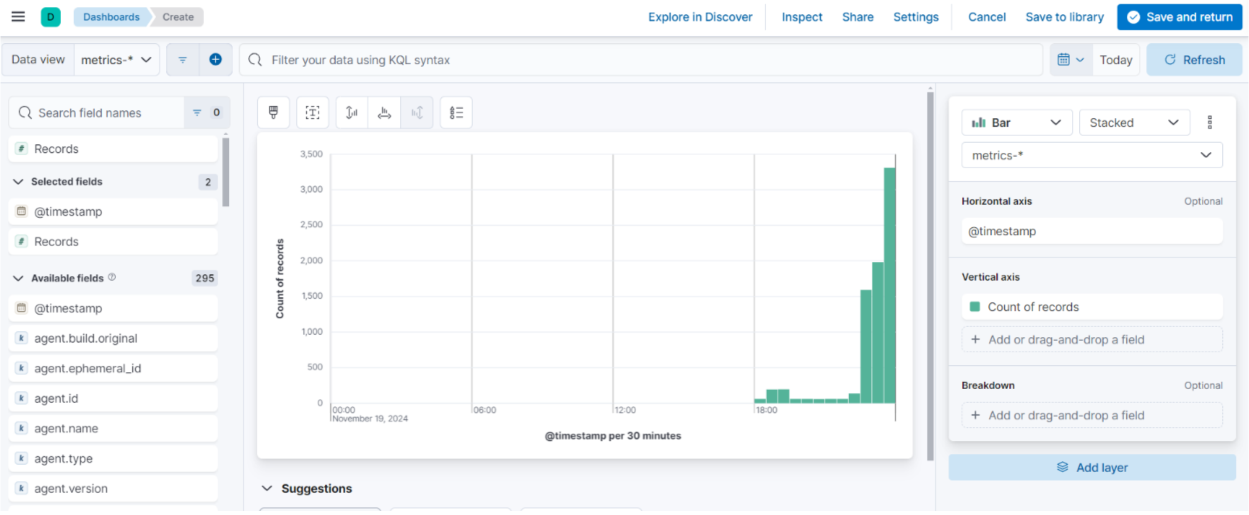
Nov 19, 2024 @ 23:24:30.667 - Nov 19, 2024 @ 23:39:30.667
(interval: Auto - 30 seconds)

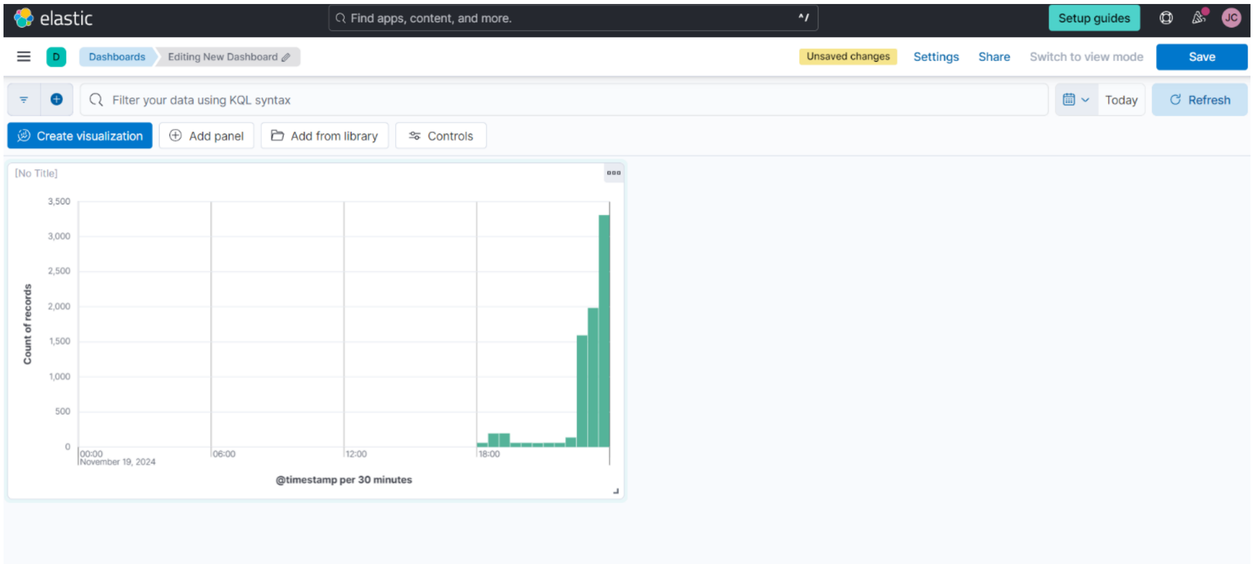
```
@timestamp                     Summary
Nov 19, 2024 @ 23:38:38.292    kali  En
Nov 19, 2024 @ 23:38:37.995    kali  En
Nov 19, 2024 @ 23:37:44.262    kali  En
Nov 19, 2024 @ 23:37:44.216    kali  En
```

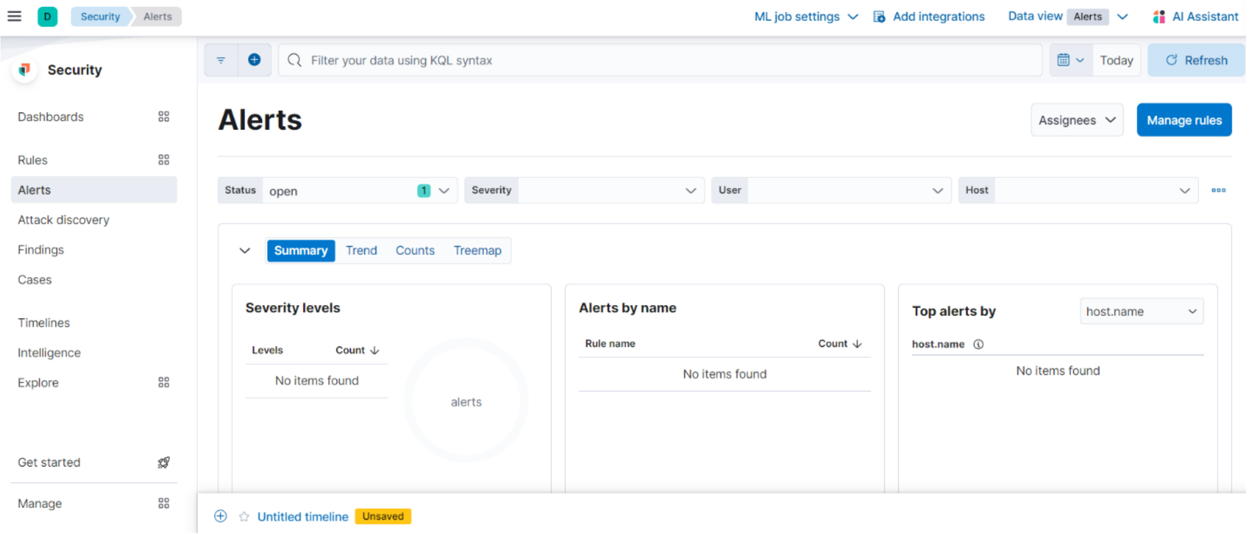
```
  20-000001",
  "_id": "FoKDSJMBQRicHupDFINY",
  "_version": 1,
  "_score": 0,
  "_source": {
    "agent": {
      "id": "9647c672-ea5b-44ea-a2c4-eee501e5c98c",
      "type": "endpoint",
      "version": "8.16.0"
    },
    "process": {
      "args": [
        "nmap",
        "-v",
        "-A",
        "10.0.2.15"
      ],
      "parent": {
        "args": [],
```

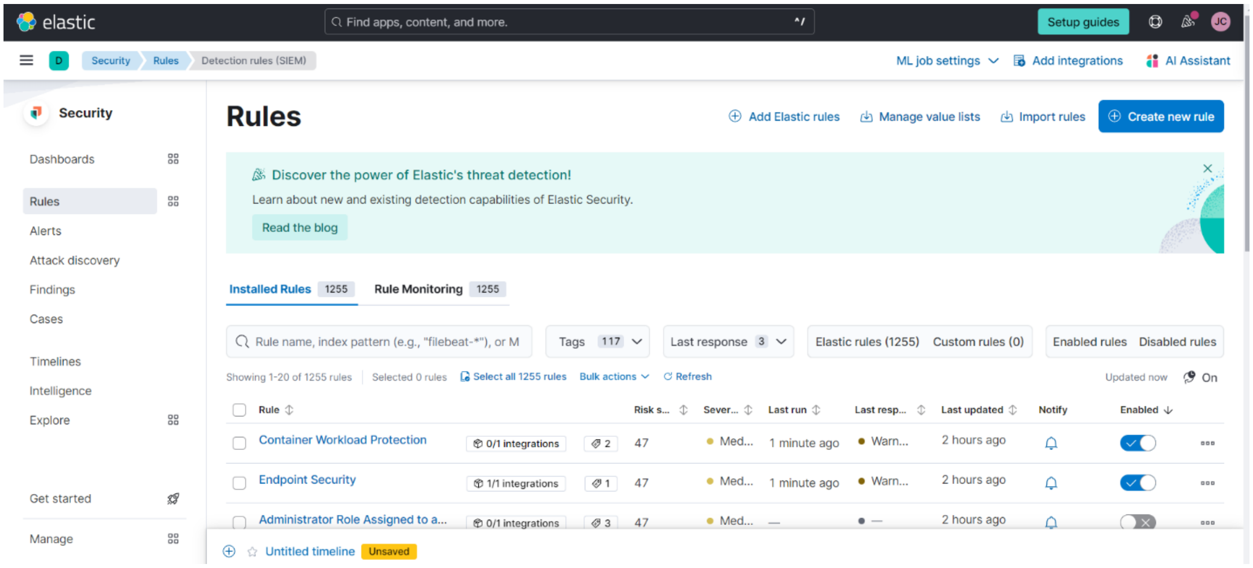


This dashboard is empty. Let's fill it up!


Dashboards
Create
Explore in Discover
Inspect
Share
Settings
Cancel
Save to library
Save and return
Data view
metrics-*
Filter your data using KQL syntax
Today
Refresh
Search field names
0
Records
Selected fields
2
@timestamp
Records
Available fields
295
@timestamp
agent.build.original
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
3,500
3,000
2,500
2,000
1,500
1,000
500
0
Count of records
00:00
November 19, 2024
06:00
12:00
18:00
@timestamp per 30 minutes
Suggestions
Bar
Stacked
metrics-*
Horizontal axis
Optional
@timestamp
Vertical axis
Count of records
Add or drag-and-drop a field
Breakdown
Optional
Add or drag-and-drop a field
Add layer


elastic
Find apps, content, and more.
Setup guides
JC
Dashboards
Editing New Dashboard
Unsaved changes
Settings
Share
Switch to view mode
Save
Filter your data using KQL syntax
Today
Refresh
Create visualization
Add panel
Add from library
Controls
[No Title]
3,500
3,000
2,500
2,000
1,500
1,000
500
0
Count of records
00:00
November 19, 2024
06:00
12:00
18:00
@timestamp per 30 minutes


Security
Alerts
ML job settings
Add integrations
Data view
Alerts
AI Assistant
Filter your data using KQL syntax
Today
Refresh
Security
Dashboards
Rules
Alerts
Attack discovery
Findings
Cases
Timelines
Intelligence
Explore
Get started
Manage
Alerts
Assignees
Manage rules
Status
open
1
Severity
User
Host
Summary
Trend
Counts
Treemap
Severity levels
Levels
Count
No items found
alerts
Alerts by name
Rule name
Count
No items found
Top alerts by
host.name
host.name
No items found
Untitled timeline
Unsaved



elastic Find apps, content, and more. Setup guides

D Security Rules Detection rules (SIEM) ML job settings Add integrations AI Assistant

Security

- Dashboards
- Rules
- Alerts
- Attack discovery
- Findings
- Cases
- Timelines
- Intelligence
- Explore
- Get started
- Manage

Rules

Add Elastic rules Manage value lists Import rules Create new rule

Discover the power of Elastic's threat detection!

Learn about new and existing detection capabilities of Elastic Security.

Read the blog

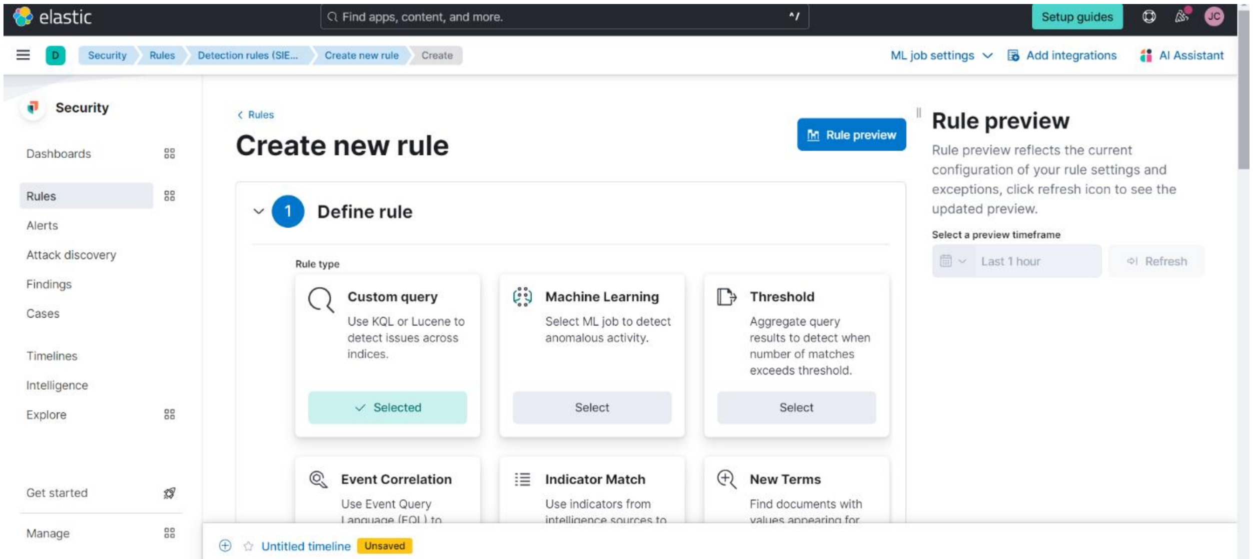
Installed Rules 1255 Rule Monitoring 1255

Rule name, index pattern (e.g., "filebeat-*"), or M Tags 117 Last response 3 Elastic rules (1255) Custom rules (0) Enabled rules Disabled rules

Showing 1-20 of 1255 rules Selected 0 rules Select all 1255 rules Bulk actions Refresh Updated now On

Rule			Risk s...	Sever...	Last run	Last resp...	Last updated	Notify	Enabled
Container Workload Protection	0/1 integrations	2	47	● Med...	1 minute ago	● Warn...	2 hours ago		✓
Endpoint Security	1/1 integrations	1	47	● Med...	1 minute ago	● Warn...	2 hours ago		✓
Administrator Role Assigned to a...	0/1 integrations	3	47	● Med...	—	● —	2 hours ago		✗

Untitled timeline Unsaved



elastic Find apps, content, and more. Setup guides

D Security Rules Detection rules (SIE... Create new rule Create ML job settings Add integrations AI Assistant

Security

- Dashboards
- Rules
- Alerts
- Attack discovery
- Findings
- Cases
- Timelines
- Intelligence
- Explore
- Get started
- Manage

‹ Rules

Create new rule

Rule preview

1 Define rule

Rule type

Custom query Use KQL or Lucene to detect issues across indices. ✓ Selected

Machine Learning Select ML job to detect anomalous activity. Select

Threshold Aggregate query results to detect when number of matches exceeds threshold. Select

Event Correlation Use Event Query Language (EQL) to

Indicator Match Use indicators from intelligence sources to

New Terms Find documents with values appearing for

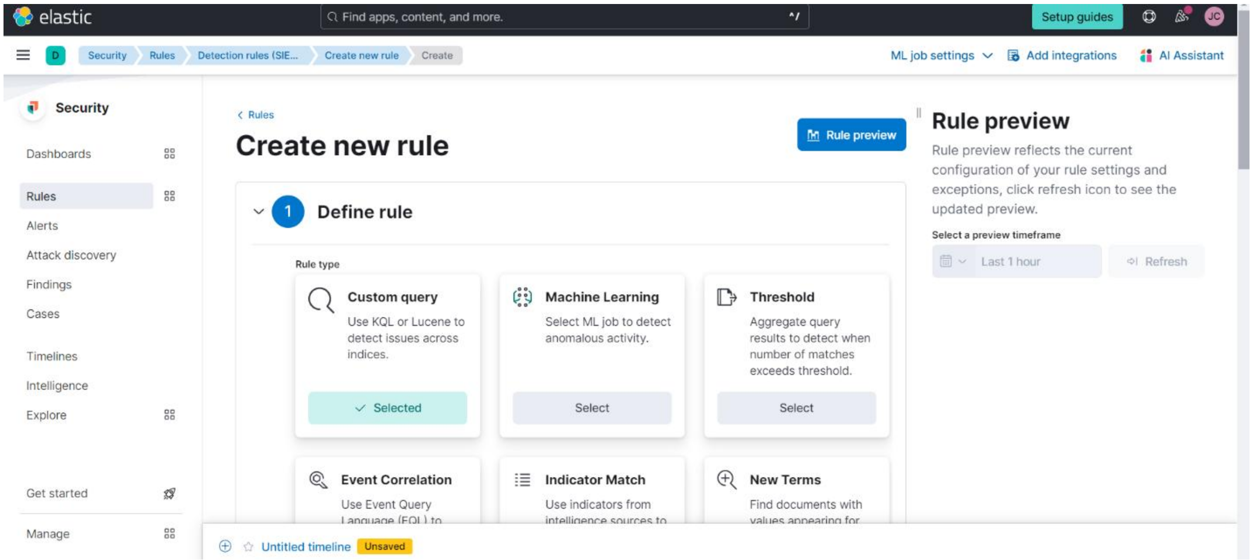
Rule preview

Rule preview reflects the current configuration of your rule settings and exceptions, click refresh icon to see the updated preview.

Select a preview timeframe

Last 1 hour Refresh

Untitled timeline Unsaved



elastic Find apps, content, and more. Setup guides

D Security Rules Detection rules (SIE... Create new rule Create ML job settings Add integrations AI Assistant

Security

- Dashboards
- Rules
- Alerts
- Attack discovery
- Findings
- Cases
- Timelines
- Intelligence
- Explore
- Get started
- Manage

‹ Rules

Create new rule

Rule preview

1 Define rule

Rule type

Custom query Use KQL or Lucene to detect issues across indices. ✓ Selected

Machine Learning Select ML job to detect anomalous activity. Select

Threshold Aggregate query results to detect when number of matches exceeds threshold. Select

Event Correlation Use Event Query Language (EQL) to

Indicator Match Use indicators from intelligence sources to

New Terms Find documents with values appearing for

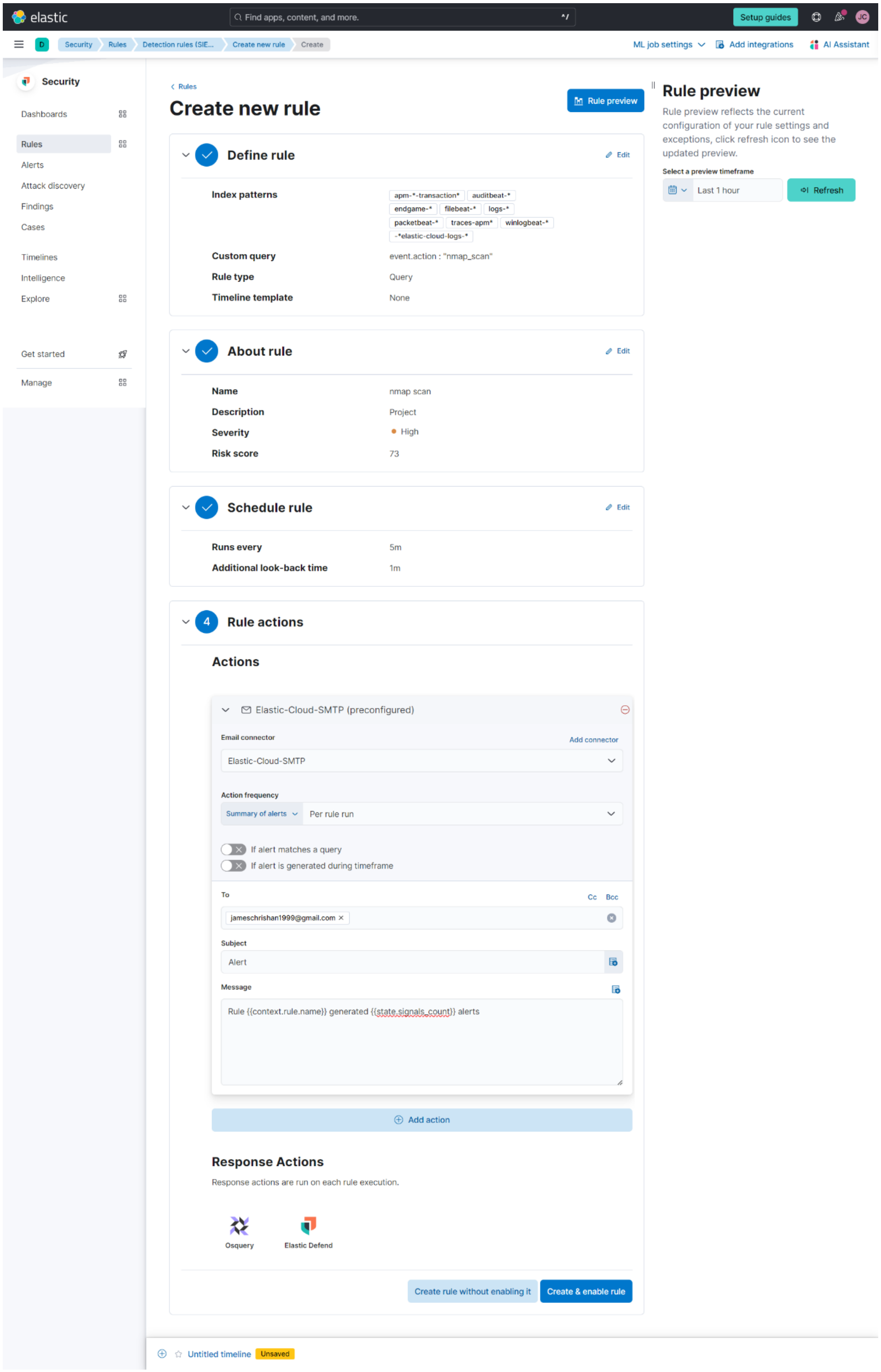
Rule preview

Rule preview reflects the current configuration of your rule settings and exceptions, click refresh icon to see the updated preview.

Select a preview timeframe

Last 1 hour Refresh

Untitled timeline Unsaved



Create new rule

Define rule

Index patterns apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*

Custom query event.action : "nmap_scan"

Rule type Query

Timeline template None

About rule

Name nmap scan

Description Project

Severity ● High

Risk score 73

Schedule rule

Runs every 5m

Additional look-back time 1m

4 Rule actions

Actions

Elastic-Cloud-SMTP (preconfigured)

Email connector: Elastic-Cloud-SMTP

Action frequency: Summary of alerts | Per rule run

○ If alert matches a query

○ If alert is generated during timeframe

To: jameschrishan1999@gmail.com

Cc Bcc

Subject: Alert

Message: Rule {{context.rule.name}} generated {{state.signals_count}} alerts

Response Actions

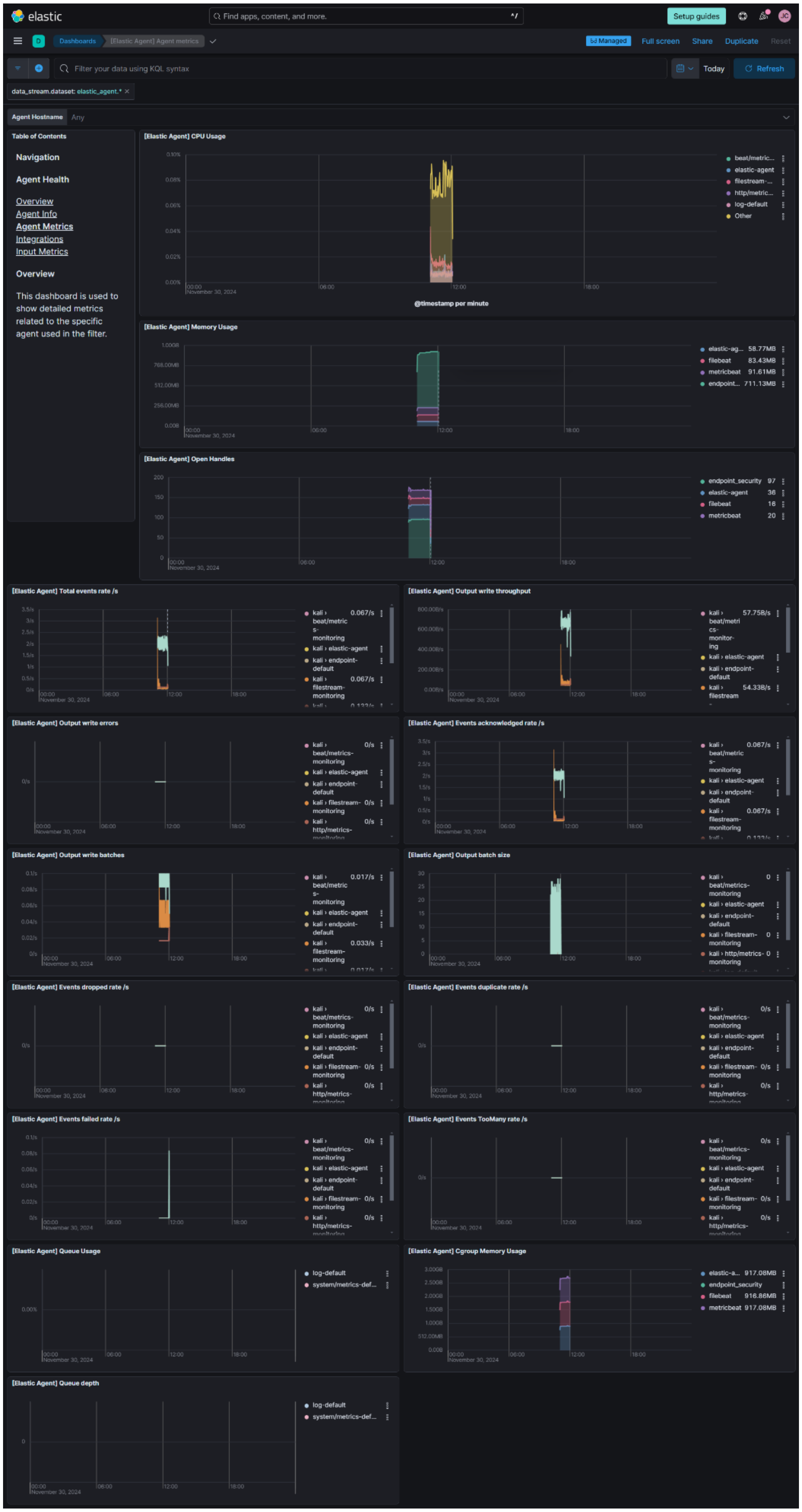
Response actions are run on each rule execution.

Rule preview

Rule preview reflects the current configuration of your rule settings and exceptions, click refresh icon to see the updated preview.

Select a preview timeframe: Last 1 hour

Refresh


elastic
Find apps, content, and more.
Setup guides
JC
Dashboards
[Elastic Agent] Agent metrics
Managed
Full screen
Share
Duplicate
Reset
Filter your data using KQL syntax
Today
Refresh
[Elastic Agent] CPU Usage
0.10%
0.08%
0.06%
0.04%
0.02%
0.00%
00:00 November 30, 2024
06:00
12:00
18:00
@timestamp per minute
beat/metric...
elastic-agent
filestream-...
http/metric...
log-default
Other
[Elastic Agent] Memory Usage
1.00GB
768.00MB
512.00MB
256.00MB
0.00B
elastic-ag... 58.77MB
filebeat 83.43MB
metricbeat 91.61MB
endpoint... 711.13MB
[Elastic Agent] Open Handles
200
150
100
50
0
endpoint_security 97
elastic-agent 36
filebeat 16
metricbeat 20
[Elastic Agent] Total events rate /s
3.5/s
3/s
2.5/s
2/s
1.5/s
1/s
0.5/s
0/s
kali › beat/metrics-monitoring 0.067/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0.067/s
kali › 0.133/s
[Elastic Agent] Output write throughput
800.00B/s
600.00B/s
400.00B/s
200.00B/s
0.00B/s
kali › beat/metrics-monitor-ing 57.75B/s
kali › elastic-agent
kali › endpoint-default
kali › filestream 54.33B/s
[Elastic Agent] Output write errors
0/s
kali › beat/metrics-monitoring 0/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0/s
kali › http/metrics-monitoring 0/s
[Elastic Agent] Events acknowledged rate /s
3.5/s
3/s
2.5/s
2/s
1.5/s
1/s
0.5/s
0/s
kali › beat/metrics-monitoring 0.067/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0.067/s
kali › 0.133/s
[Elastic Agent] Output write batches
0.1/s
0.08/s
0.06/s
0.04/s
0.02/s
0/s
kali › beat/metrics-monitoring 0.017/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0.033/s
kali › 0.017/s
[Elastic Agent] Output batch size
30
25
20
15
10
5
0
kali › beat/metrics-monitoring 0
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0
kali › http/metrics-monitoring 0
[Elastic Agent] Events dropped rate /s
0/s
kali › beat/metrics-monitoring 0/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0/s
kali › http/metrics-monitoring 0/s
[Elastic Agent] Events duplicate rate /s
0/s
kali › beat/metrics-monitoring 0/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0/s
kali › http/metrics-monitoring 0/s
[Elastic Agent] Events failed rate /s
0.1/s
0.08/s
0.06/s
0.04/s
0.02/s
0/s
kali › beat/metrics-monitoring 0/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0/s
kali › http/metrics-monitoring 0/s
[Elastic Agent] Events TooMany rate /s
0/s
kali › beat/metrics-monitoring 0/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0/s
kali › http/metrics-monitoring 0/s
[Elastic Agent] Queue Usage
0.00%
log-default
system/metrics-def...
[Elastic Agent] Cgroup Memory Usage
3.00GB
2.50GB
2.00GB
1.50GB
1.00GB
512.00MB
0.00B
elastic-a... 917.08MB
endpoint_security
filebeat 916.86MB
metricbeat 917.08MB
[Elastic Agent] Queue depth
0
log-default
system/metrics-def...

data_stream.dataset: elastic_agent.*

Agent Hostname Any

Table of Contents

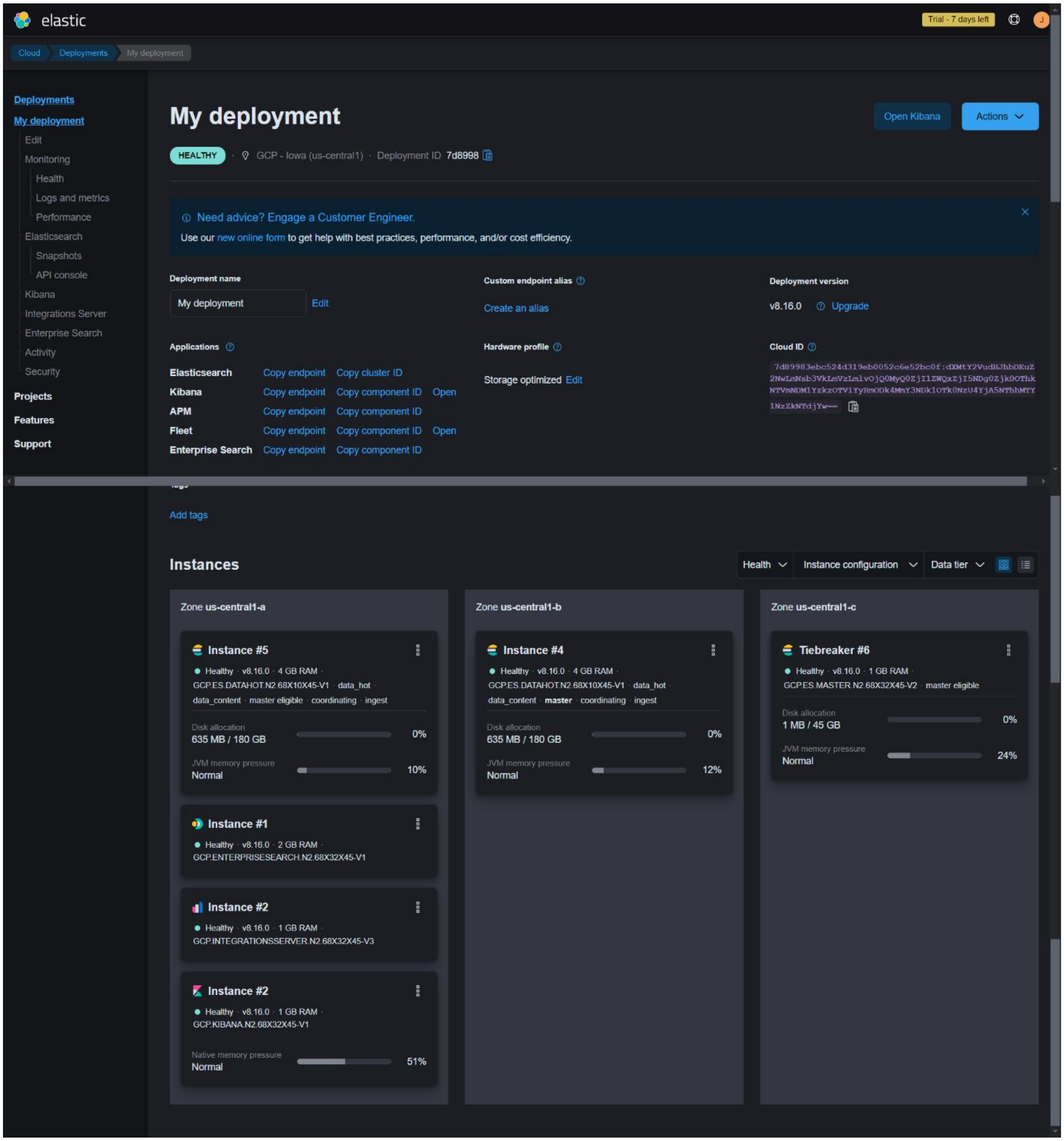
Navigation

Agent Health

Overview
Agent Info
Agent Metrics
Integrations
Input Metrics

Overview

This dashboard is used to show detailed metrics related to the specific agent used in the filter.



My deployment

HEALTHY · GCP - Iowa (us-central1) · Deployment ID 7d8998

Need advice? Engage a Customer Engineer.

Use our new online form to get help with best practices, performance, and/or cost efficiency.

Deployment name

My deployment Edit

Custom endpoint alias

Create an alias

Deployment version

v8.16.0 Upgrade

Applications

Elasticsearch	Copy endpoint	Copy cluster ID	
Kibana	Copy endpoint	Copy component ID	Open
APM	Copy endpoint	Copy component ID	
Fleet	Copy endpoint	Copy component ID	Open
Enterprise Search	Copy endpoint	Copy component ID	

Hardware profile

Storage optimized Edit

Cloud ID

```
7d89983ebc524d319eb0052c6e52bc0f:dXMtY2VudHJhbDEuZ
2NwLmNsb3VkLmVzLmlvOjQ0MyQ0ZjI1ZWQxZjI5NDg0Zjk0OThk
NTVmNDM1YzkzOTViYyRmODk4MmY3NDk1OTk0NzU4YjA5NThhMTY
1NzZkNTdjYw==
```

Add tags

Instances

Zone us-central1-a

Instance #5
● Healthy · v8.16.0 · 4 GB RAM · GCP.ES.DATAHOT.N2.68X10X45-V1 · data_hot · data_content · master eligible · coordinating · ingest
Disk allocation 635 MB / 180 GB 0%
JVM memory pressure Normal 10%

Instance #1
● Healthy · v8.16.0 · 2 GB RAM · GCP.ENTERPRISESEARCH.N2.68X32X45-V1

Instance #2
● Healthy · v8.16.0 · 1 GB RAM · GCP.INTEGRATIONSSERVER.N2.68X32X45-V3

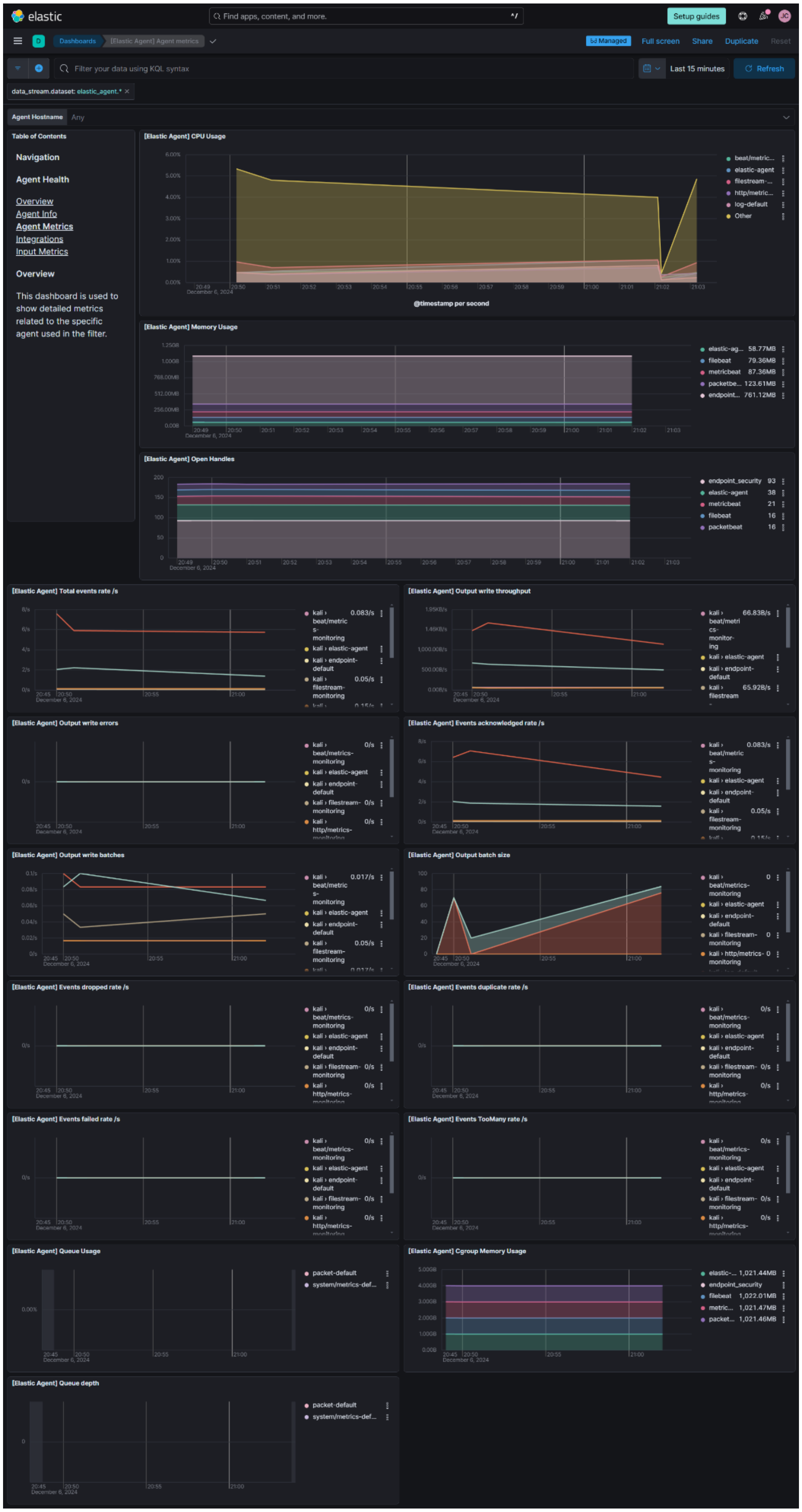
Instance #2
● Healthy · v8.16.0 · 1 GB RAM · GCP.KIBANA.N2.68X32X45-V1
Native memory pressure Normal 51%

Zone us-central1-b

Instance #4
● Healthy · v8.16.0 · 4 GB RAM · GCP.ES.DATAHOT.N2.68X10X45-V1 · data_hot · data_content · **master** · coordinating · ingest
Disk allocation 635 MB / 180 GB 0%
JVM memory pressure Normal 12%

Zone us-central1-c

Tiebreaker #6
● Healthy · v8.16.0 · 1 GB RAM · GCP.ES.MASTER.N2.68X32X45-V2 · master eligible
Disk allocation 1 MB / 45 GB 0%
JVM memory pressure Normal 24%



elastic
Find apps, content, and more.
Setup guides
JC
Dashboards
[Elastic Agent] Agent metrics
Managed
Full screen
Share
Duplicate
Reset
Filter your data using KQL syntax
Last 15 minutes
Refresh

data_stream.dataset: elastic_agent.*

Agent Hostname Any

Table of Contents

Navigation

Agent Health

Overview
Agent Info
Agent Metrics
Integrations
Input Metrics

Overview

This dashboard is used to show detailed metrics related to the specific agent used in the filter.

[Elastic Agent] CPU Usage

[Elastic Agent] Memory Usage

[Elastic Agent] Open Handles

[Elastic Agent] Total events rate /s

[Elastic Agent] Output write throughput

[Elastic Agent] Output write errors

[Elastic Agent] Events acknowledged rate /s

8/s
6/s
4/s
2/s
0/s
kali › beat/metrics-monitoring 0.083/s
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0.05/s

[Elastic Agent] Output write batches

[Elastic Agent] Output batch size

100
80
60
40
20
0
kali › beat/metrics-monitoring 0
kali › elastic-agent
kali › endpoint-default
kali › filestream-monitoring 0
kali › http/metrics-monitoring 0

[Elastic Agent] Events dropped rate /s

[Elastic Agent] Events duplicate rate /s

[Elastic Agent] Events failed rate /s

[Elastic Agent] Events TooMany rate /s

[Elastic Agent] Queue Usage

[Elastic Agent] Cgroup Memory Usage

[Elastic Agent] Queue depth