ELASTIC AGENT AND FLEET SERVER SETUP

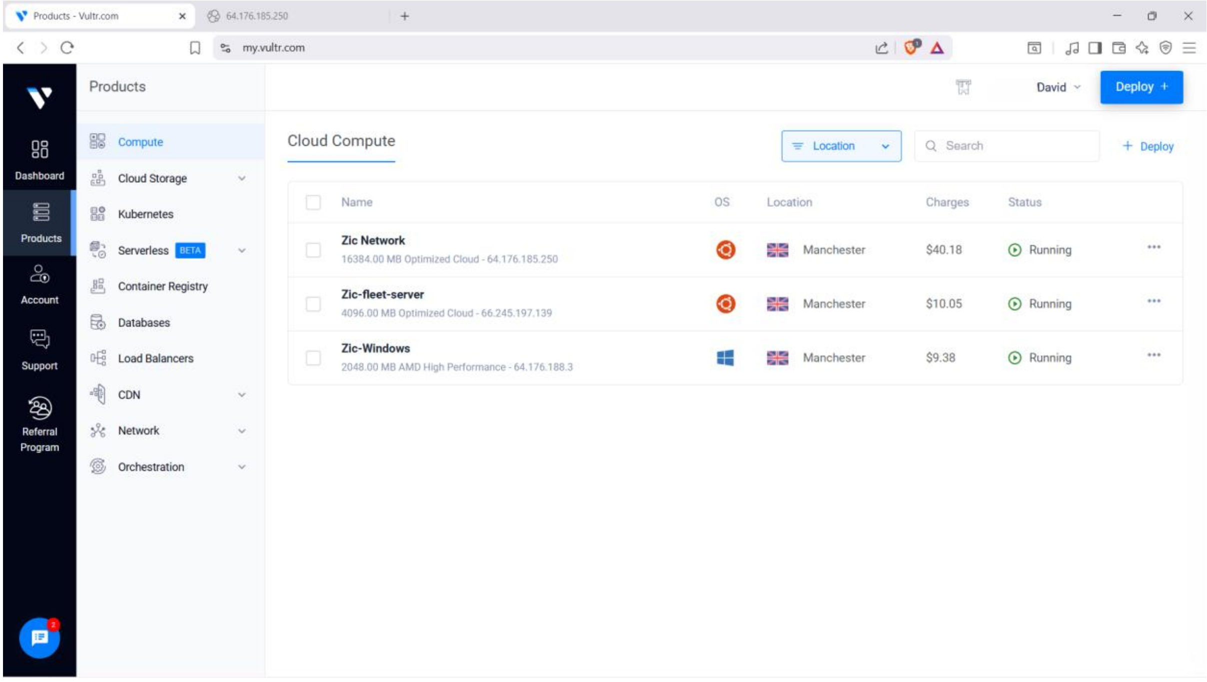
Objective: how to install elastic agent on windows server and enroll the server into a fleet server.

Tools Used

- **Elastic Agent** – Installed on servers to collect and forward data to Fleet Server.
- **Fleet Server** – Acts as the central service that manages Elastic Agents and ensures policies are applied.
- **Elasticsearch & Kibana** – Provide indexing, storage, visualization, and management dashboards.
- **Firewall & Networking Tools (ufw, IP rules, ports 9200 & 8220)** – For controlling network traffic and enabling communication between servers.
- **PowerShell & Linux SSH** – For running installation and enrollment commands on Windows and Linux environments

Note: to deploy a new server under the same Virtual Private Cloud (VPC), the location must always be the same.

In the image below, Fleet server has been created and also a windows server in the cloud has been created. It took the same process to create as I did in the **Elastic and kibana setup project.**

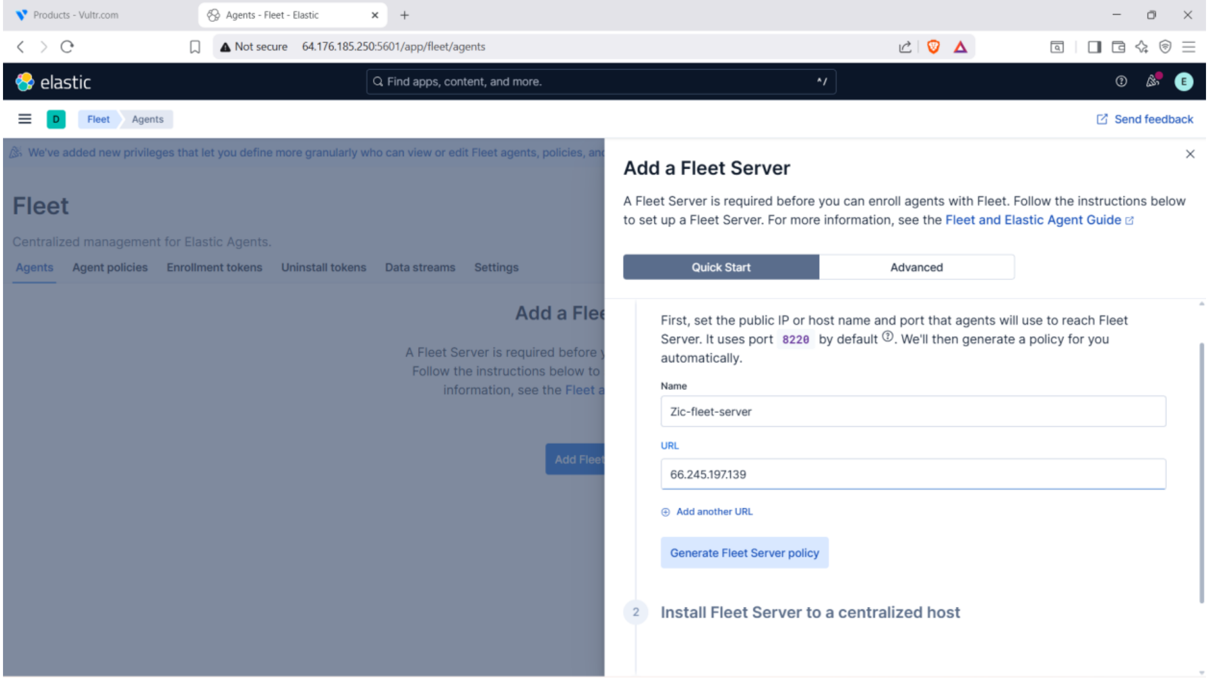


Cloud Compute

Name	OS	Location	Charges	Status
Zic Network 16384.00 MB Optimized Cloud - 64.176.185.250		Manchester	$40.18	Running
Zic-fleet-server 4096.00 MB Optimized Cloud - 66.245.197.139		Manchester	$10.05	Running
Zic-Windows 2048.00 MB AMD High Performance - 64.176.188.3		Manchester	$9.38	Running

You go to your elasticsearch, click the hamburger menu, scroll to fleet under **management** and click **add fleet server.** You include your fleet server name and the IP address of the fleet server created on the cloud.

Note: for the url, it must be https:// ip address before it can generate fleet server policy.



We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, an

Fleet

Centralized management for Elastic Agents.

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the Fleet and Elastic Agent Guide

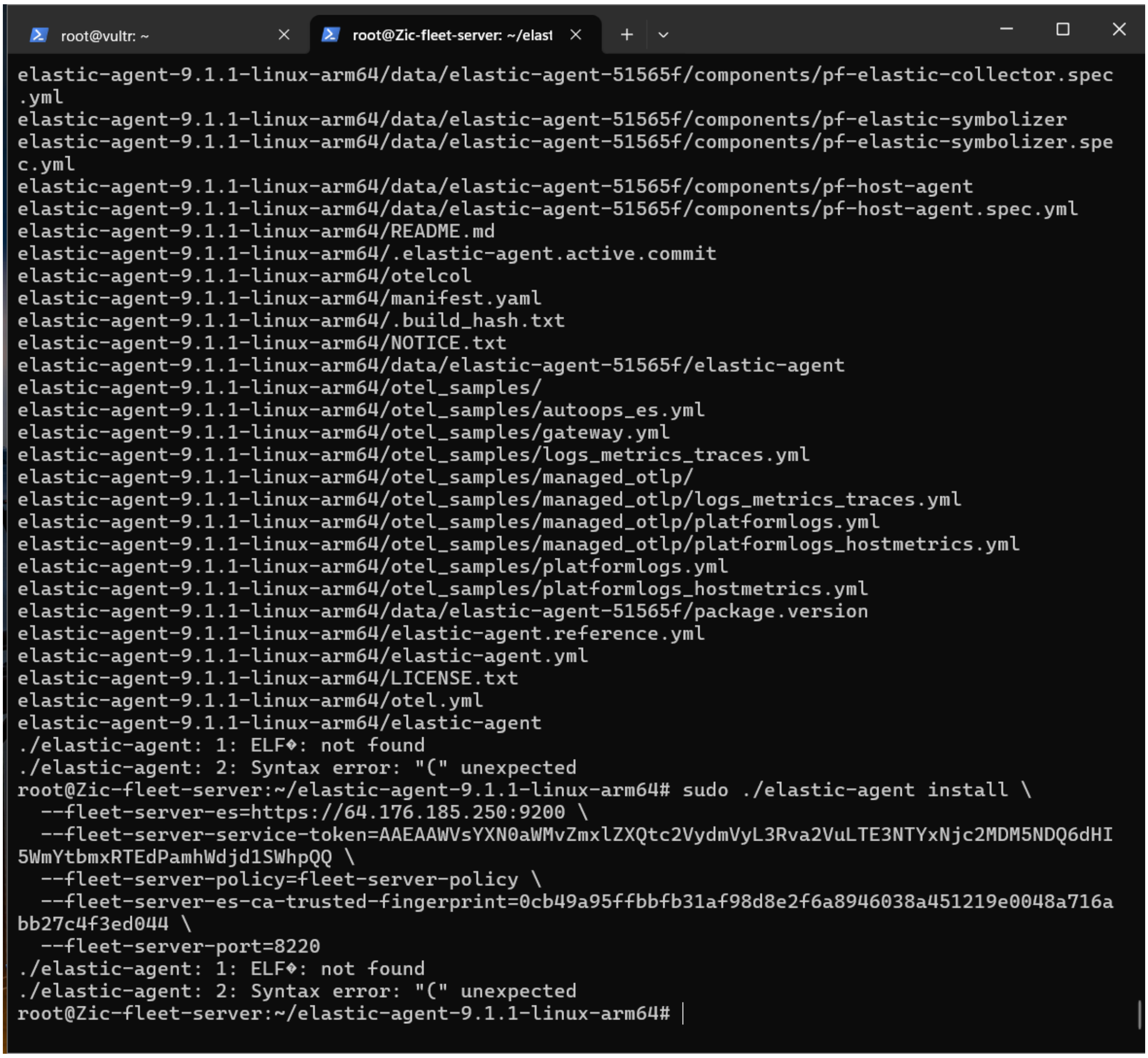
First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port `8220` by default. We'll then generate a policy for you automatically.

Name: Zic-fleet-server

URL: 66.245.197.139

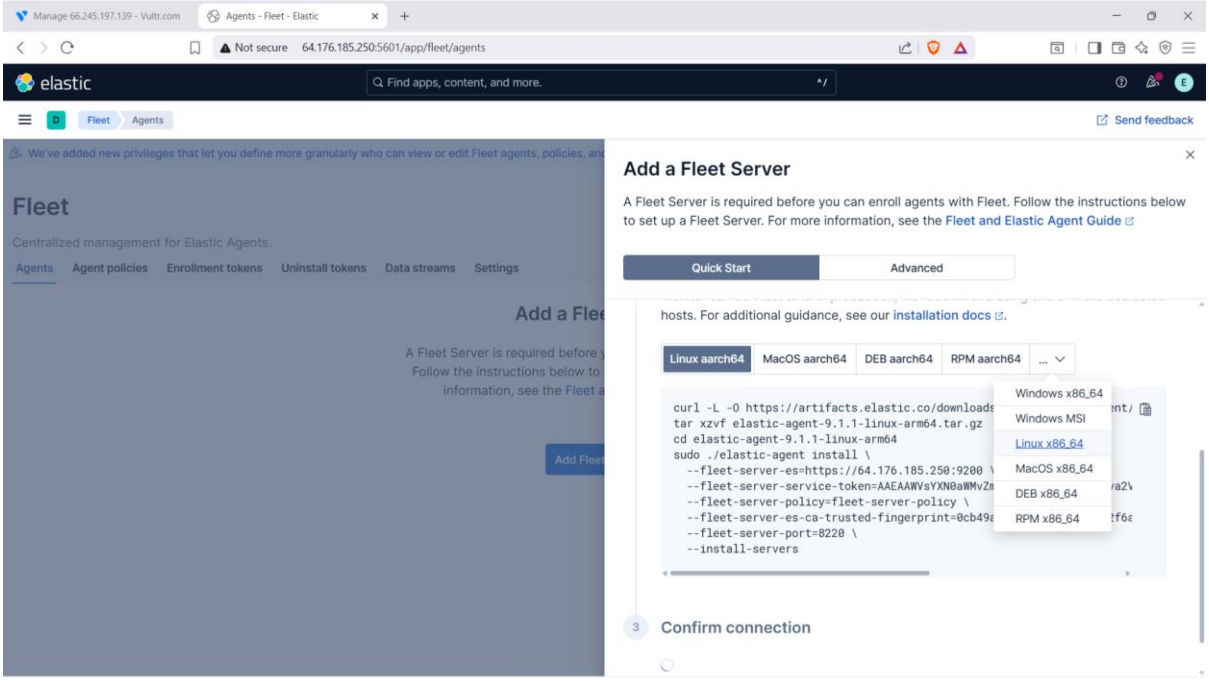
2 Install Fleet Server to a centralized host

The next process is to **install fleet server to a centralized host.** Here, I chose the **linux arm64 to install** and I copied the command to paste in the fleet server ssh. I was getting a syntax error.



```
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/components/pf-elastic-collector.spec
.yml
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/components/pf-elastic-symbolizer
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/components/pf-elastic-symbolizer.spe
c.yml
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/components/pf-host-agent
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/components/pf-host-agent.spec.yml
elastic-agent-9.1.1-linux-arm64/README.md
elastic-agent-9.1.1-linux-arm64/.elastic-agent.active.commit
elastic-agent-9.1.1-linux-arm64/otelcol
elastic-agent-9.1.1-linux-arm64/manifest.yaml
elastic-agent-9.1.1-linux-arm64/.build_hash.txt
elastic-agent-9.1.1-linux-arm64/NOTICE.txt
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/elastic-agent
elastic-agent-9.1.1-linux-arm64/otel_samples/
elastic-agent-9.1.1-linux-arm64/otel_samples/autoops_es.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/gateway.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/logs_metrics_traces.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/managed_otlp/
elastic-agent-9.1.1-linux-arm64/otel_samples/managed_otlp/logs_metrics_traces.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/managed_otlp/platformlogs.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/managed_otlp/platformlogs_hostmetrics.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/platformlogs.yml
elastic-agent-9.1.1-linux-arm64/otel_samples/platformlogs_hostmetrics.yml
elastic-agent-9.1.1-linux-arm64/data/elastic-agent-51565f/package.version
elastic-agent-9.1.1-linux-arm64/elastic-agent.reference.yml
elastic-agent-9.1.1-linux-arm64/elastic-agent.yml
elastic-agent-9.1.1-linux-arm64/LICENSE.txt
elastic-agent-9.1.1-linux-arm64/otel.yml
elastic-agent-9.1.1-linux-arm64/elastic-agent
./elastic-agent: 1: ELF�: not found
./elastic-agent: 2: Syntax error: "(" unexpected
root@Zic-fleet-server:~/elastic-agent-9.1.1-linux-arm64# sudo ./elastic-agent install \
  --fleet-server-es=https://64.176.185.250:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3NTYxNjc2MDM5NDQ6dHI
5WmYtbmxRTEdPamhWdjd1SWhpQQ \
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=0cb49a95ffbbfb31af98d8e2f6a8946038a451219e0048a716a
bb27c4f3ed044 \
  --fleet-server-port=8220
./elastic-agent: 1: ELF�: not found
./elastic-agent: 2: Syntax error: "(" unexpected
root@Zic-fleet-server:~/elastic-agent-9.1.1-linux-arm64# 
```

I realized that I copied the wrong linux distribution, so I changed it to **linux x86_64**


Manage 66.245.197.139 - Vultr.com
Agents - Fleet - Elastic
Not secure 64.176.185.250:5601/app/fleet/agents
elastic
Find apps, content, and more.
Fleet
Agents
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, an
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Uninstall tokens
Data streams
Settings
Add a Flee
Add Fleet

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the Fleet and Elastic Agent Guide

Quick Start | Advanced

hosts. For additional guidance, see our installation docs.

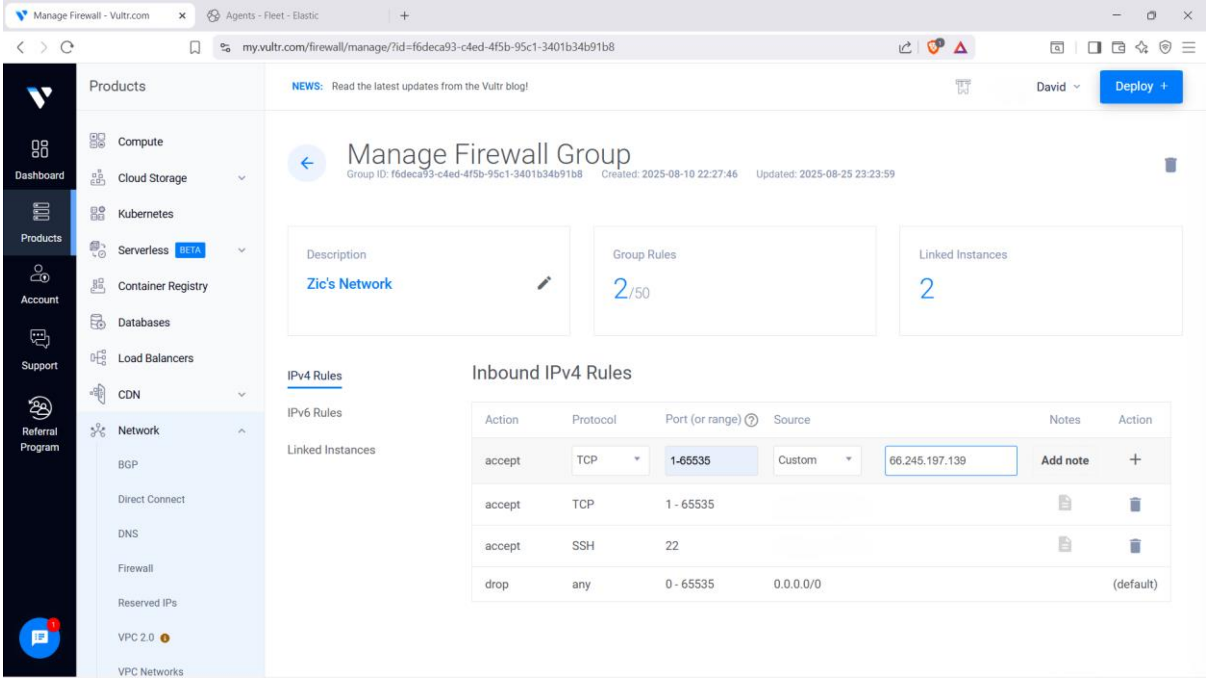
Linux aarch64 | MacOS aarch64 | DEB aarch64 | RPM aarch64 | ...

Windows x86_64
Windows MSI
Linux x86_64
MacOS x86_64
DEB x86_64
RPM x86_64

```
curl -L -O https://artifacts.elastic.co/downloads                    ent/
tar xzvf elastic-agent-9.1.1-linux-arm64.tar.gz
cd elastic-agent-9.1.1-linux-arm64
sudo ./elastic-agent install \
  --fleet-server-es=https://64.176.185.250:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZm                    /a2\
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=0cb49a                    2f6a
  --fleet-server-port=8220 \
  --install-servers
```

3 Confirm connection

After this change, I included the firewall rule to allow the ip address of the fleet server.



Manage Firewall Group

Group ID: f6deca93-c4ed-4f5b-95c1-3401b34b91b8 Created: 2025-08-10 22:27:46 Updated: 2025-08-25 23:23:59

Description: Zic's Network

Group Rules: 2/50

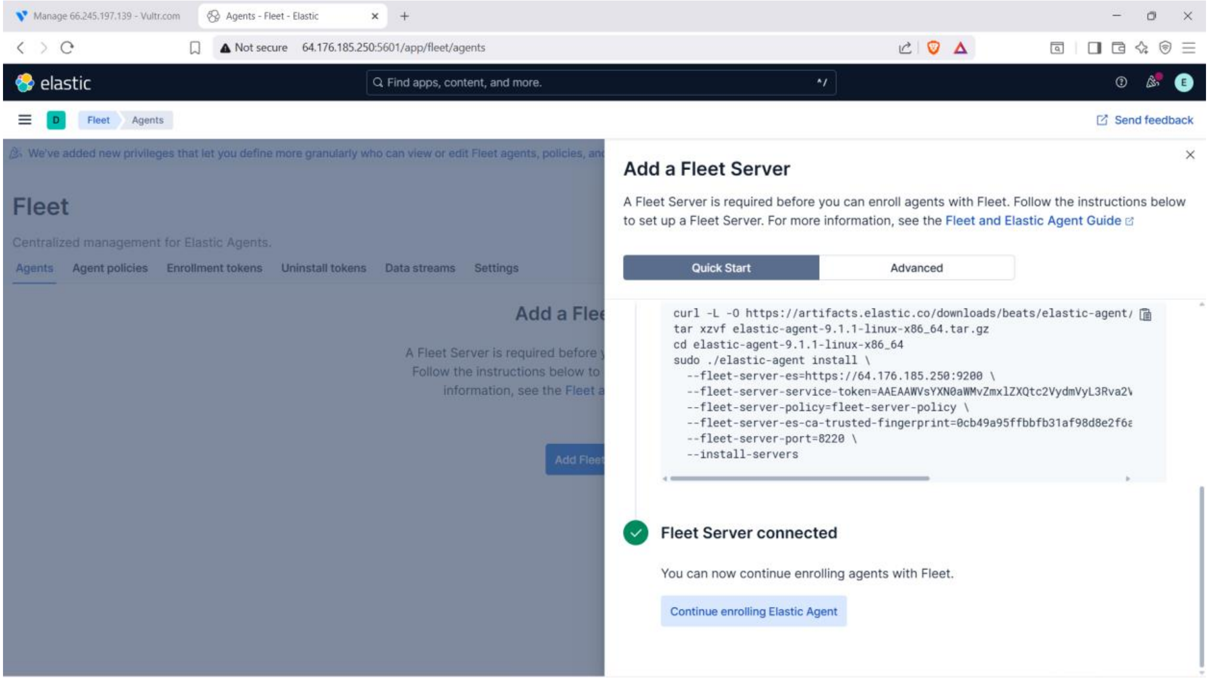
Linked Instances: 2

IPv4 Rules | IPv6 Rules | Linked Instances

Inbound IPv4 Rules

Action	Protocol	Port (or range)	Source		Notes	Action
accept	TCP	1-65535	Custom	66.245.197.139	Add note	+
accept	TCP	1 - 65535	[redacted]			
accept	SSH	22	[redacted]			
drop	any	0 - 65535	0.0.0.0/0			(default)

I also allowed the port 9200 using the command **ufw allow 9200 in the kibana directory**. The elastic agent successfully installed and the fleet server connected.


Manage 66.245.197.139 - Vultr.com
Agents - Fleet - Elastic
Not secure 64.176.185.250:5601/app/fleet/agents
elastic
Find apps, content, and more.
Fleet
Agents
Send feedback

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, an

Fleet

Centralized management for Elastic Agents.

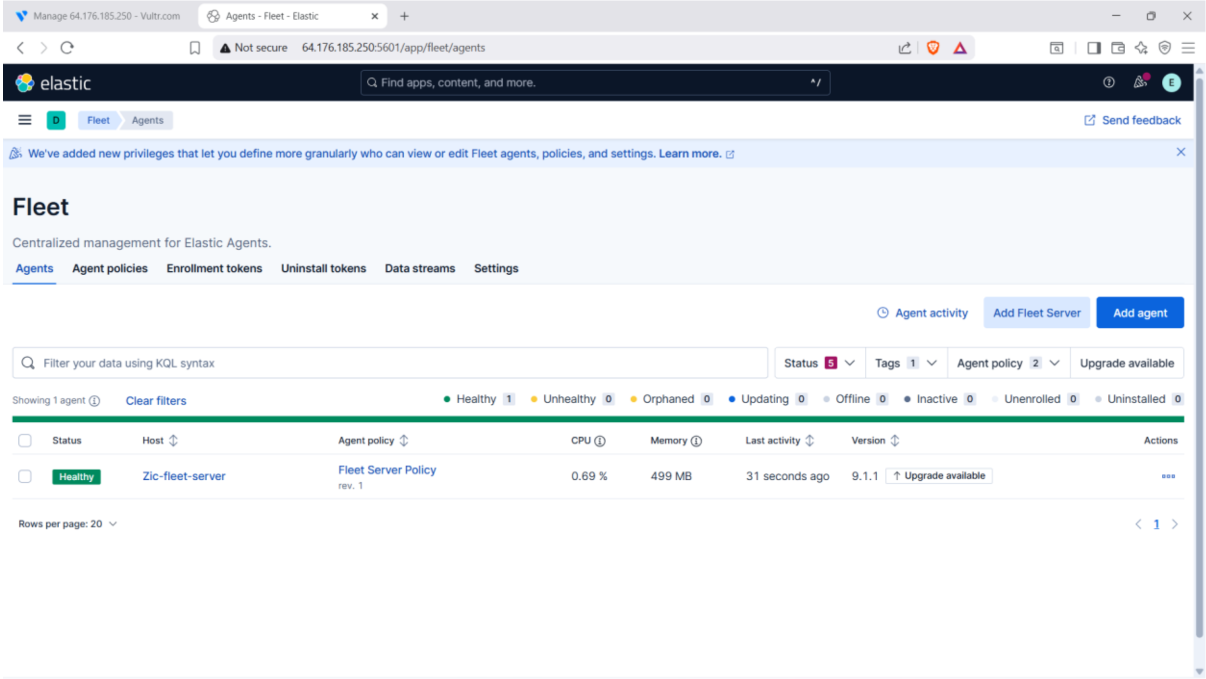
Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. 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-9.1.1-linux-x86_64.tar.gz
cd elastic-agent-9.1.1-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://64.176.185.250:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2V
  --fleet-server-policy=fleet-server-policy \
  --fleet-server-es-ca-trusted-fingerprint=0cb49a95ffbbfb31af98d8e2f6a
  --fleet-server-port=8220 \
  --install-servers
```

Fleet Server connected

You can now continue enrolling agents with Fleet.


Manage 64.176.185.250 - Vultr.com
Agents - Fleet - Elastic
Not secure 64.176.185.250:5601/app/fleet/agents
elastic
Find apps, content, and more.
Fleet
Agents
Send feedback

We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

Fleet

Centralized management for Elastic Agents.

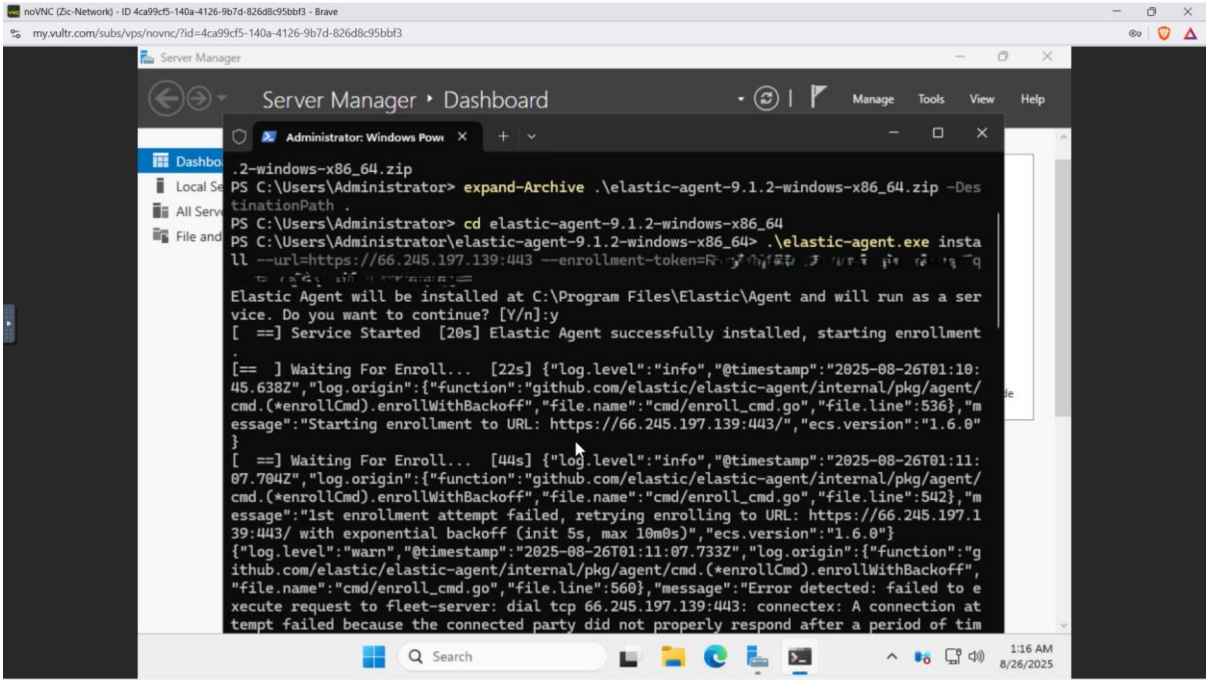
Showing 1 agent Clear filters

● Healthy 1 ● Unhealthy 0 ● Orphaned 0 ● Updating 0 ● Offline 0 ● Inactive 0 ● Unenrolled 0 ● Uninstalled 0

□	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
□	Healthy	Zic-fleet-server	Fleet Server Policy rev. 1	0.69 %	499 MB	31 seconds ago	9.1.1 ↑ Upgrade available	•••

Rows per page: 20

Click on **add agent** to add new agent. Rename the new agent to **zic windows policy.** In the section of **add elastic agent to your host,** select windows in the options and copy the command. Ensure to use root privileges(administrator) when inputting the command. Login to your windows server created on the cloud, login and open **powershell and run as administrator** and paste in the copied command from the fleet server.

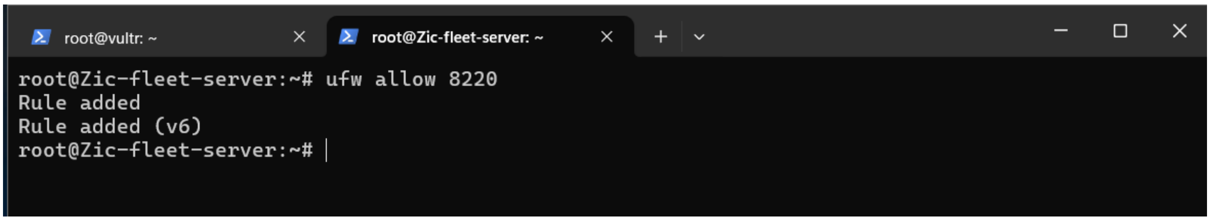


```
.2-windows-x86_64.zip
PS C:\Users\Administrator> expand-Archive .\elastic-agent-9.1.2-windows-x86_64.zip -Des
tinationPath .
PS C:\Users\Administrator> cd elastic-agent-9.1.2-windows-x86_64
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64> .\elastic-agent.exe insta
ll --url=https://66.245.197.139:443 --enrollment-token=[redacted]
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a ser
vice. Do you want to continue? [Y/n]:y
[  ==] Service Started  [20s] Elastic Agent successfully installed, starting enrollment
.
[==  ] Waiting For Enroll...  [22s] {"log.level":"info","@timestamp":"2025-08-26T01:10:
45.638Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/
cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":536},"m
essage":"Starting enrollment to URL: https://66.245.197.139:443/","ecs.version":"1.6.0"
}
[  ==] Waiting For Enroll...  [44s] {"log.level":"info","@timestamp":"2025-08-26T01:11:
07.704Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/
cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":542},"m
essage":"1st enrollment attempt failed, retrying enrolling to URL: https://66.245.197.1
39:443/ with exponential backoff (init 5s, max 10m0s)","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2025-08-26T01:11:07.733Z","log.origin":{"function":"g
ithub.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff",
"file.name":"cmd/enroll_cmd.go","file.line":560},"message":"Error detected: failed to e
xecute request to fleet-server: dial tcp 66.245.197.139:443: connectex: A connection at
tempt failed because the connected party did not properly respond after a period of tim
```

noVNC (Zic-Network) - ID 4ca99cf5-140a-4126-9b7d-826d8c95bbf3 - Brave
my.vultr.com/subs/vps/novnc/?id=4ca99cf5-140a-4126-9b7d-826d8c95bbf3
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Administrator: Windows Pow
Dashbo
Local Se
All Serv
File and
Search
1:16 AM
8/26/2025

From the screenshot above, I got an error of **failed to execute request to fleet server.** Fleet server runs on **port 8220** and the fleet server in the screenshot shows **port 443**. That is why we got the failed connection.

We head to the **fleet server** on our powershell, and use the command **ufw allow 8220**



```
root@Zic-fleet-server:~# ufw allow 8220
Rule added
Rule added (v6)
root@Zic-fleet-server:~#
```

and also head to the **fleet** under **management on Elasticsearch.** Go to **settings** and change the **port 443** to **port 8220,** save and apply settings, then save and deploy.

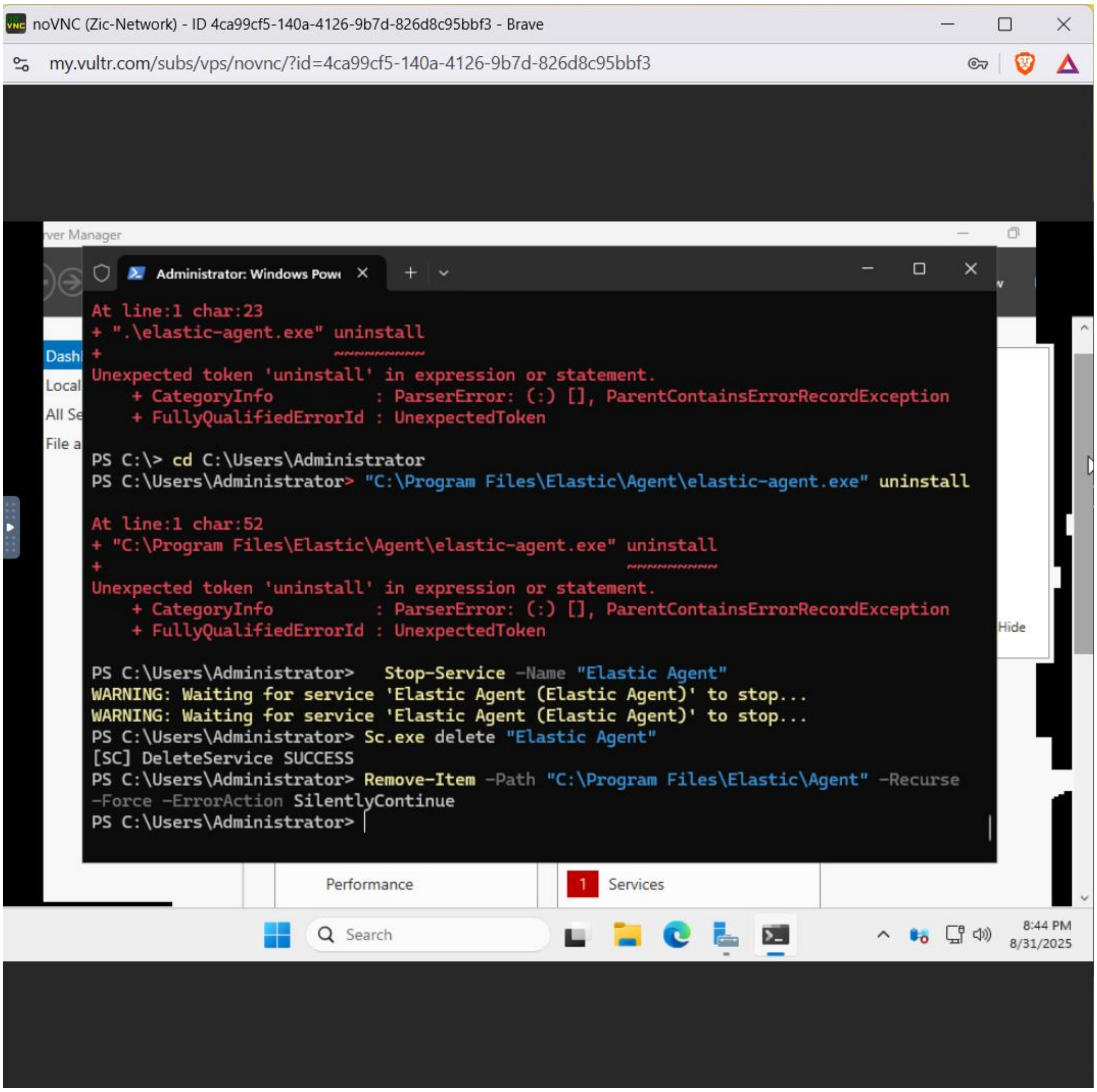
I had to remove the previously installed elastic agent with the **port 443,** I used the commands

Stop-Service -Name "Elastic Agent"

sc.exe delete "Elastic Agent"

Remove-Item -Path "C:\Program Files\Elastic\Agent" -Recurse -Force -ErrorAction SilentlyContinue

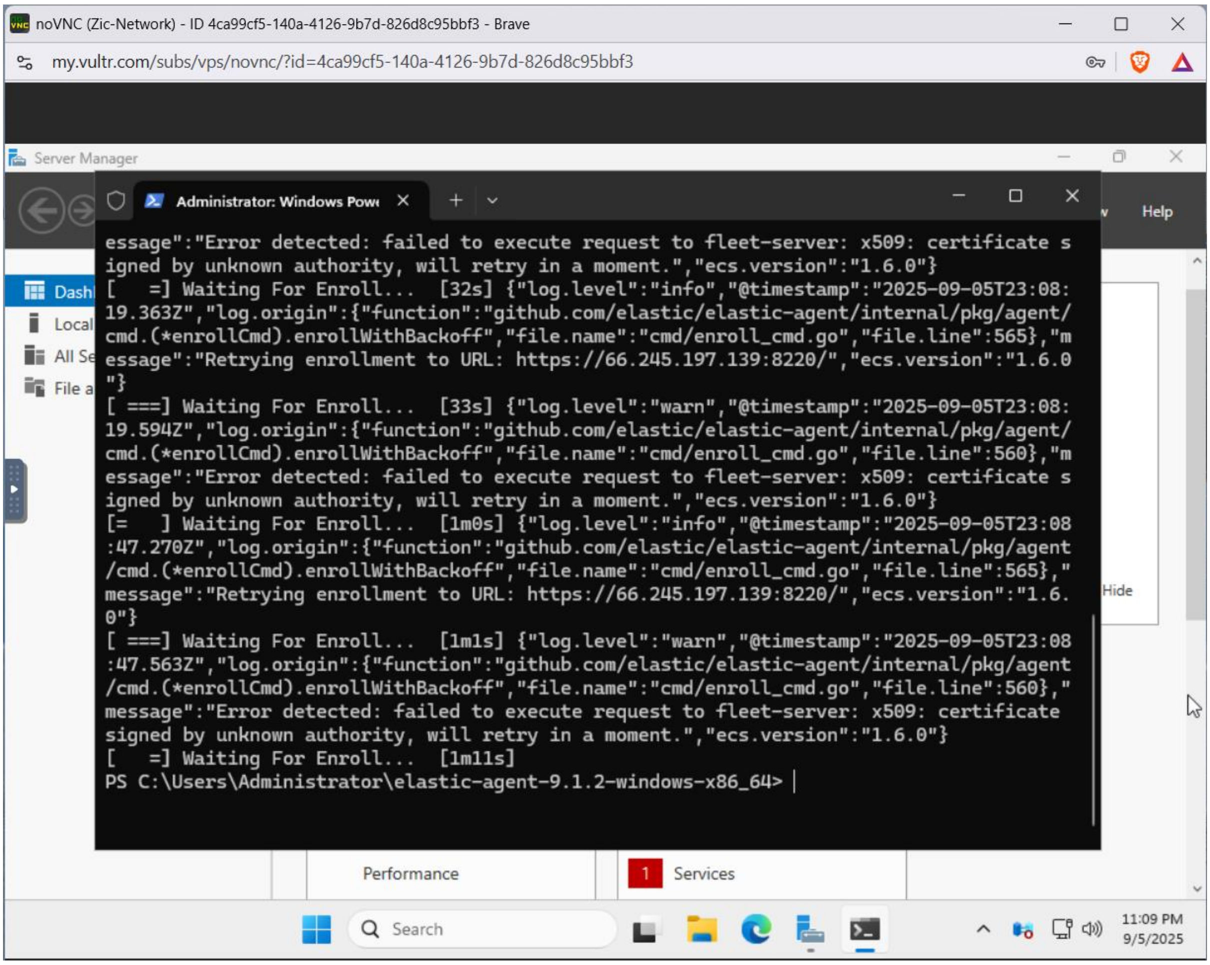
Note: I ran the command from the default directory **C:\Users\Administrator**



noVNC (Zic-Network) - ID 4ca99cf5-140a-4126-9b7d-826d8c95bbf3 - Brave
my.vultr.com/subs/vps/novnc/?id=4ca99cf5-140a-4126-9b7d-826d8c95bbf3
Administrator: Windows Powe
Performance
Services
Search
8:44 PM
8/31/2025

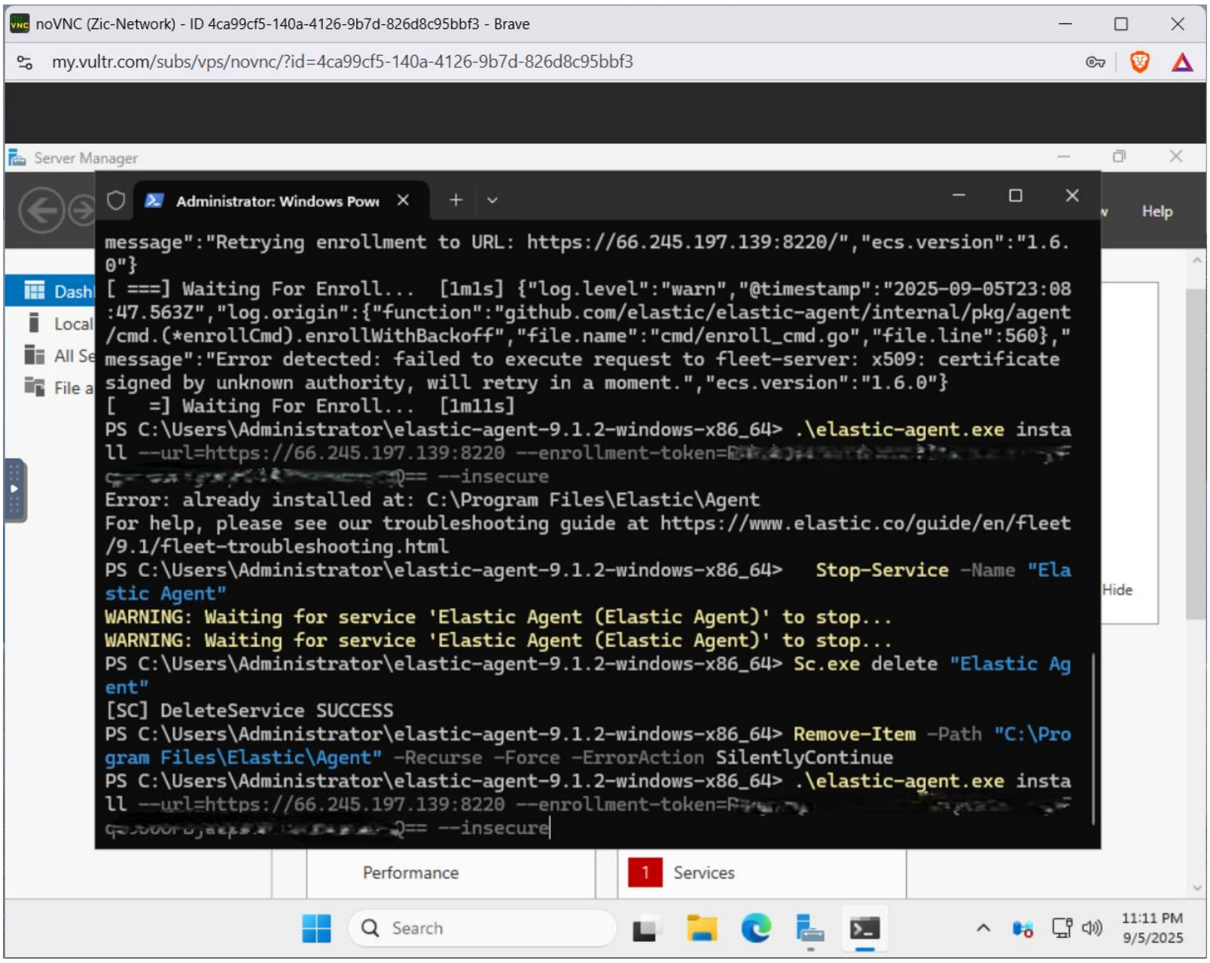
```
At line:1 char:23
+ ".\elastic-agent.exe" uninstall
+                       ~~~~~~~~~
Unexpected token 'uninstall' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\> cd C:\Users\Administrator
PS C:\Users\Administrator> "C:\Program Files\Elastic\Agent\elastic-agent.exe" uninstall

At line:1 char:52
+ "C:\Program Files\Elastic\Agent\elastic-agent.exe" uninstall
+                                                    ~~~~~~~~~
Unexpected token 'uninstall' in expression or statement.
    + CategoryInfo          : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnexpectedToken

PS C:\Users\Administrator>   Stop-Service -Name "Elastic Agent"
WARNING: Waiting for service 'Elastic Agent (Elastic Agent)' to stop...
WARNING: Waiting for service 'Elastic Agent (Elastic Agent)' to stop...
PS C:\Users\Administrator> Sc.exe delete "Elastic Agent"
[SC] DeleteService SUCCESS
PS C:\Users\Administrator> Remove-Item -Path "C:\Program Files\Elastic\Agent" -Recurse
-Force -ErrorAction SilentlyContinue
PS C:\Users\Administrator>
```

I ran the command to install fleet server on windows server and it gave an error of **x509: certificate signed by unknown authority.**


noVNC (Zic-Network) - ID 4ca99cf5-140a-4126-9b7d-826d8c95bbf3 - Brave
my.vultr.com/subs/vps/novnc/?id=4ca99cf5-140a-4126-9b7d-826d8c95bbf3
Server Manager
Administrator: Windows Powe
Help
Dash
Local
All Se
File a
Hide
Performance
1
Services
Search
11:09 PM
9/5/2025

```
essage":"Error detected: failed to execute request to fleet-server: x509: certificate s
igned by unknown authority, will retry in a moment.","ecs.version":"1.6.0"}
[   =] Waiting For Enroll...  [32s] {"log.level":"info","@timestamp":"2025-09-05T23:08:
19.363Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/
cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":565},"m
essage":"Retrying enrollment to URL: https://66.245.197.139:8220/","ecs.version":"1.6.0
"}
[ ===] Waiting For Enroll...  [33s] {"log.level":"warn","@timestamp":"2025-09-05T23:08:
19.594Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/
cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":560},"m
essage":"Error detected: failed to execute request to fleet-server: x509: certificate s
igned by unknown authority, will retry in a moment.","ecs.version":"1.6.0"}
[=   ] Waiting For Enroll...  [1m0s] {"log.level":"info","@timestamp":"2025-09-05T23:08
:47.270Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent
/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":565},"
message":"Retrying enrollment to URL: https://66.245.197.139:8220/","ecs.version":"1.6.
0"}
[ ===] Waiting For Enroll...  [1m1s] {"log.level":"warn","@timestamp":"2025-09-05T23:08
:47.563Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent
/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":560},"
message":"Error detected: failed to execute request to fleet-server: x509: certificate
signed by unknown authority, will retry in a moment.","ecs.version":"1.6.0"}
[   =] Waiting For Enroll...  [1m11s]
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64>
```

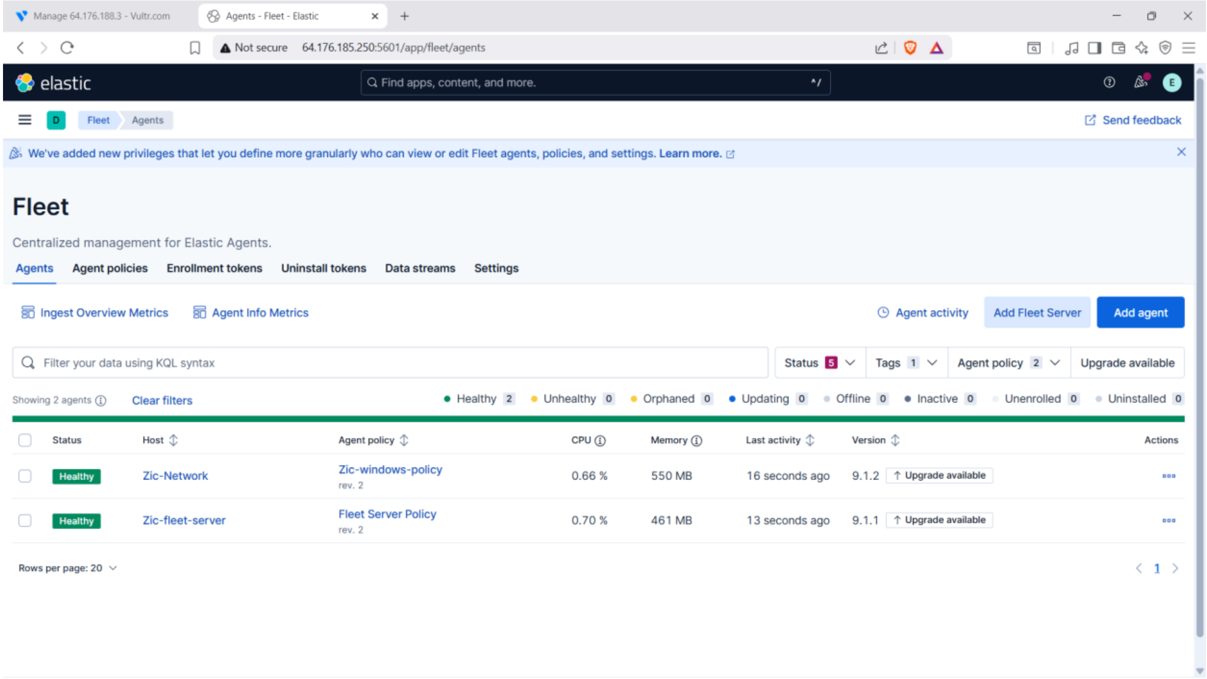
I just had to include the command **--insecure** to the end of the enrollment token and ran the command again.



noVNC (Zic-Network) - ID 4ca99cf5-140a-4126-9b7d-826d8c95bbf3 - Brave
my.vultr.com/subs/vps/novnc/?id=4ca99cf5-140a-4126-9b7d-826d8c95bbf3
Server Manager
Administrator: Windows Powe
Help
Dash
Local
All Se
File a
Hide
Performance
1
Services
Search
11:11 PM
9/5/2025

```
message":"Retrying enrollment to URL: https://66.245.197.139:8220/","ecs.version":"1.6.
0"}
[ ===] Waiting For Enroll...  [1m1s] {"log.level":"warn","@timestamp":"2025-09-05T23:08
:47.563Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent
/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":560},"
message":"Error detected: failed to execute request to fleet-server: x509: certificate
signed by unknown authority, will retry in a moment.","ecs.version":"1.6.0"}
[   =] Waiting For Enroll...  [1m11s]
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64> .\elastic-agent.exe insta
ll --url=https://66.245.197.139:8220 --enrollment-token=[redacted]== --insecure
Error: already installed at: C:\Program Files\Elastic\Agent
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet
/9.1/fleet-troubleshooting.html
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64>  Stop-Service -Name "Ela
stic Agent"
WARNING: Waiting for service 'Elastic Agent (Elastic Agent)' to stop...
WARNING: Waiting for service 'Elastic Agent (Elastic Agent)' to stop...
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64> Sc.exe delete "Elastic Ag
ent"
[SC] DeleteService SUCCESS
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64> Remove-Item -Path "C:\Pro
gram Files\Elastic\Agent" -Recurse -Force -ErrorAction SilentlyContinue
PS C:\Users\Administrator\elastic-agent-9.1.2-windows-x86_64> .\elastic-agent.exe insta
ll --url=https://66.245.197.139:8220 --enrollment-token=[redacted]== --insecure
```

The elastic agent successfully installed on the windows server, that is why we can see the windows policy appear on the fleet server.



Manage 64.176.188.3 - Vultr.com
Agents - Fleet - Elastic
Not secure
64.176.185.250:5601/app/fleet/agents
elastic
Find apps, content, and more.
Fleet
Agents
Send feedback
We've added new privileges that let you define more granularly who can view or edit Fleet agents, policies, and settings. Learn more.

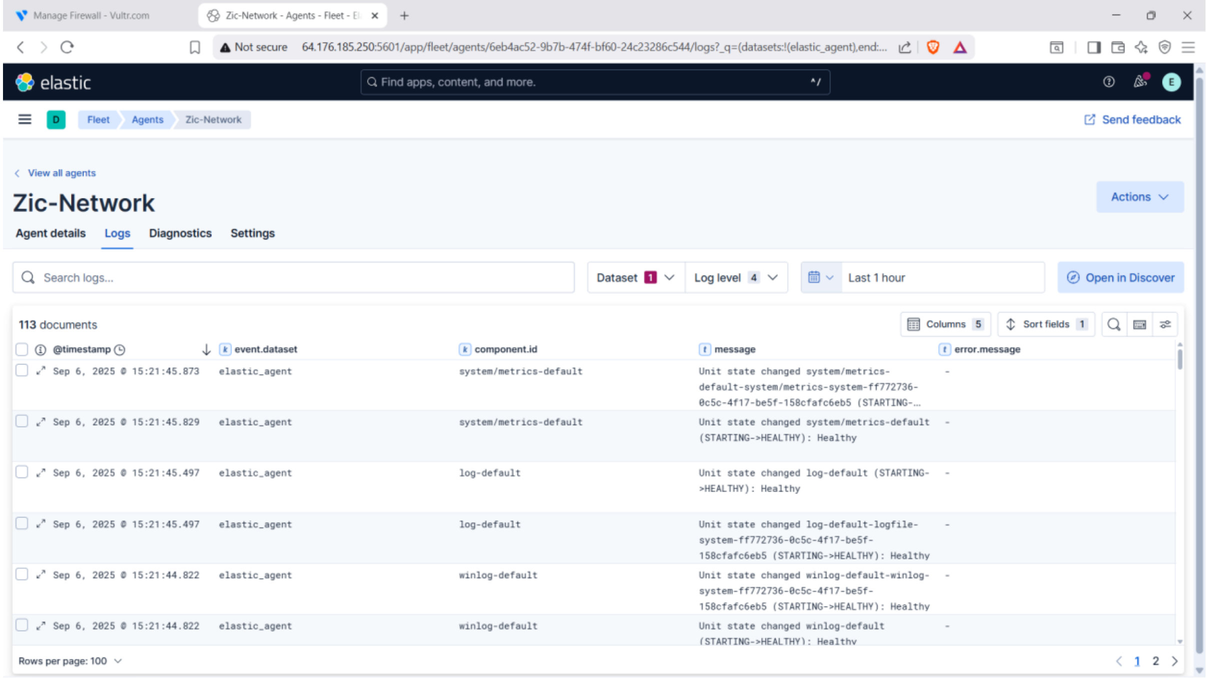
Fleet

Centralized management for Elastic Agents.

□	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
□	Healthy	Zic-Network	Zic-windows-policy rev. 2	0.66 %	550 MB	16 seconds ago	9.1.2 ↑ Upgrade available	•••
□	Healthy	Zic-fleet-server	Fleet Server Policy rev. 2	0.70 %	461 MB	13 seconds ago	9.1.1 ↑ Upgrade available	•••

One issue I encountered was that my fleet server kept installing on the windows server but was not enrolling and this happened because of the fleet server IP address I added to the firewall rule. So I had to remove it so that the fleet server will be installed and enrolled on the windows server.

When you head to the fleet server and you click the **Zic-Network**, go to the **logs** section and click it, you will see logs being generated. This shows that the windows server has been integrated into fleet.

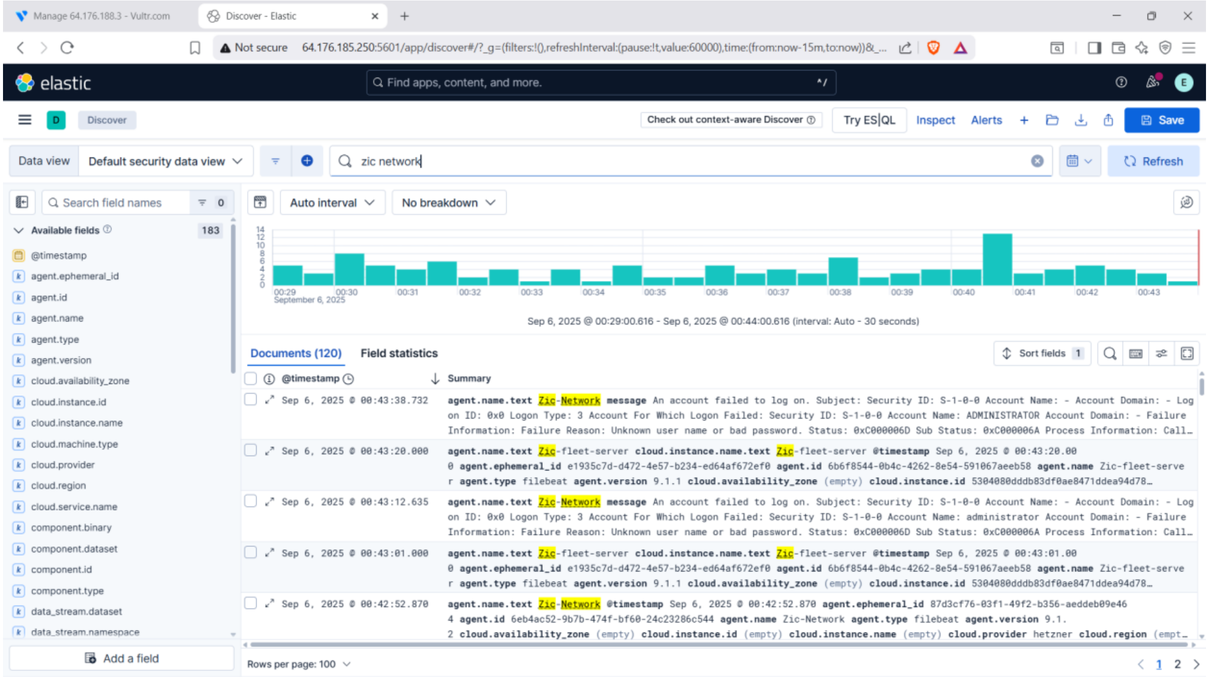


Zic-Network

113 documents

@timestamp	event.dataset	component.id	message	error.message
Sep 6, 2025 @ 15:21:45.873	elastic_agent	system/metrics-default	Unit state changed system/metrics-default-system/metrics-system-ff772736-0c5c-4f17-be5f-158cfafc6eb5 (STARTING-…	-
Sep 6, 2025 @ 15:21:45.829	elastic_agent	system/metrics-default	Unit state changed system/metrics-default (STARTING->HEALTHY): Healthy	-
Sep 6, 2025 @ 15:21:45.497	elastic_agent	log-default	Unit state changed log-default (STARTING->HEALTHY): Healthy	-
Sep 6, 2025 @ 15:21:45.497	elastic_agent	log-default	Unit state changed log-default-logfile-system-ff772736-0c5c-4f17-be5f-158cfafc6eb5 (STARTING->HEALTHY): Healthy	-
Sep 6, 2025 @ 15:21:44.822	elastic_agent	winlog-default	Unit state changed winlog-default-winlog-system-ff772736-0c5c-4f17-be5f-158cfafc6eb5 (STARTING->HEALTHY): Healthy	-
Sep 6, 2025 @ 15:21:44.822	elastic_agent	winlog-default	Unit state changed winlog-default (STARTING->HEALTHY): Healthy	-

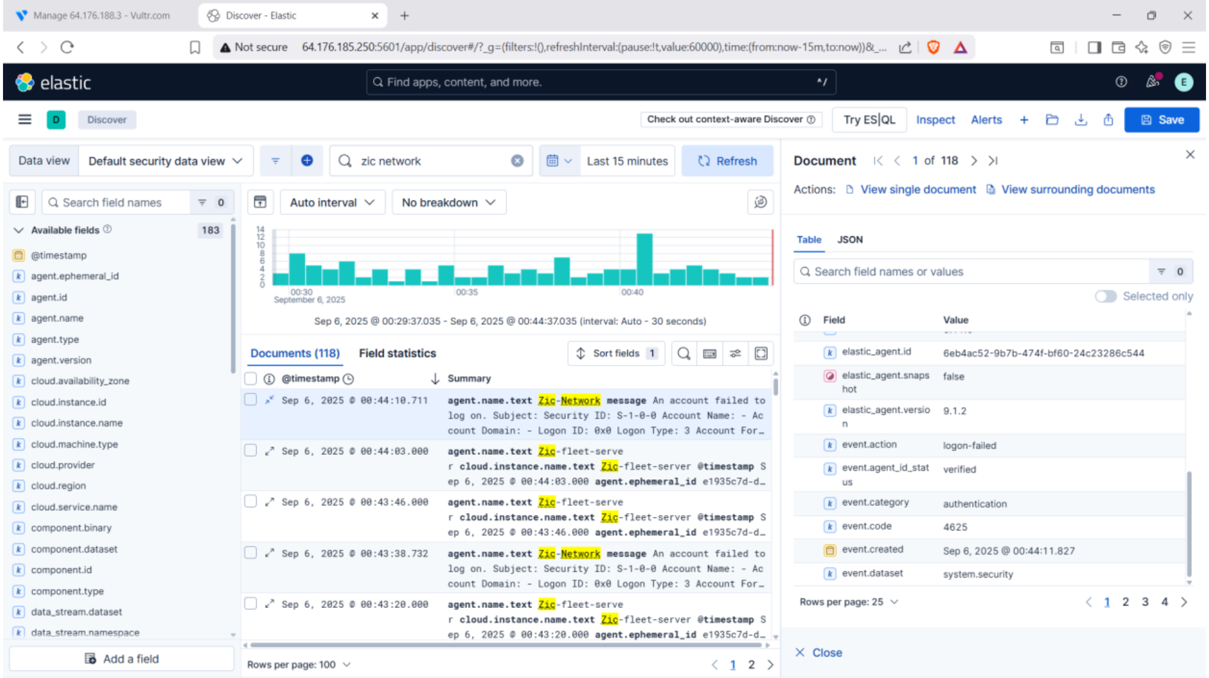
We can search out the **Zic network** (which is the windows server; I renamed it to Zic Windows) and see it pop up in the logs on elastic search as seen in the screenshot below.



Sep 6, 2025 @ 00:29:00.616 - Sep 6, 2025 @ 00:44:00.616 (interval: Auto - 30 seconds)

```
@timestamp                  Summary
Sep 6, 2025 @ 00:43:38.732  agent.name.text Zic-Network message An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Log
                            on ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: ADMINISTRATOR Account Domain: - Failure
                            Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Call…
Sep 6, 2025 @ 00:43:20.000  agent.name.text Zic-fleet-server cloud.instance.name.text Zic-fleet-server @timestamp Sep 6, 2025 @ 00:43:20.00
                            0 agent.ephemeral_id e1935c7d-d472-4e57-b234-ed64af672ef0 agent.id 6b6f8544-0b4c-4262-8e54-591067aeeb58 agent.name Zic-fleet-serve
                            r agent.type filebeat agent.version 9.1.1 cloud.availability_zone (empty) cloud.instance.id 5304080dddb83df0ae8471ddea94d78…
Sep 6, 2025 @ 00:43:12.635  agent.name.text Zic-Network message An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Log
                            on ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: administrator Account Domain: - Failure
                            Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC000006A Process Information: Call…
Sep 6, 2025 @ 00:43:01.000  agent.name.text Zic-fleet-server cloud.instance.name.text Zic-fleet-server @timestamp Sep 6, 2025 @ 00:43:01.00
                            0 agent.ephemeral_id e1935c7d-d472-4e57-b234-ed64af672ef0 agent.id 6b6f8544-0b4c-4262-8e54-591067aeeb58 agent.name Zic-fleet-serve
                            r agent.type filebeat agent.version 9.1.1 cloud.availability_zone (empty) cloud.instance.id 5304080dddb83df0ae8471ddea94d78…
Sep 6, 2025 @ 00:42:52.870  agent.name.text Zic-Network @timestamp Sep 6, 2025 @ 00:42:52.870 agent.ephemeral_id 87d3cf76-03f1-49f2-b356-aeddeb09e46
                            4 agent.id 6eb4ac52-9b7b-474f-bf60-24c23286c544 agent.name Zic-Network agent.type filebeat agent.version 9.1.
                            2 cloud.availability_zone (empty) cloud.instance.id (empty) cloud.instance.name (empty) cloud.provider hetzner cloud.region (empt…
```

Expanding one of the logs, you see more details like the Event Code, event category and the likes.



Sep 6, 2025 @ 00:29:37.035 - Sep 6, 2025 @ 00:44:37.035 (interval: Auto - 30 seconds)

```
@timestamp                  Summary
Sep 6, 2025 @ 00:44:10.711  agent.name.text Zic-Network message An account failed to
                            log on. Subject: Security ID: S-1-0-0 Account Name: - Ac
                            count Domain: - Logon ID: 0x0 Logon Type: 3 Account For…
Sep 6, 2025 @ 00:44:03.000  agent.name.text Zic-fleet-serve
                            r cloud.instance.name.text Zic-fleet-server @timestamp S
                            ep 6, 2025 @ 00:44:03.000 agent.ephemeral_id e1935c7d-d…
Sep 6, 2025 @ 00:43:46.000  agent.name.text Zic-fleet-serve
                            r cloud.instance.name.text Zic-fleet-server @timestamp S
                            ep 6, 2025 @ 00:43:46.000 agent.ephemeral_id e1935c7d-d…
Sep 6, 2025 @ 00:43:38.732  agent.name.text Zic-Network message An account failed to
                            log on. Subject: Security ID: S-1-0-0 Account Name: - Ac
                            count Domain: - Logon ID: 0x0 Logon Type: 3 Account For…
Sep 6, 2025 @ 00:43:20.000  agent.name.text Zic-fleet-serve
                            r cloud.instance.name.text Zic-fleet-server @timestamp S
                            ep 6, 2025 @ 00:43:20.000 agent.ephemeral_id e1935c7d-d…
```

Field	Value
elastic_agent.id	6eb4ac52-9b7b-474f-bf60-24c23286c544
elastic_agent.snapshot	false
elastic_agent.version	9.1.2
event.action	logon-failed
event.agent_id_status	verified
event.category	authentication
event.code	4625
event.created	Sep 6, 2025 @ 00:44:11.827
event.dataset	system.security

Use of Elastic Agent and Fleet Server.

- **Elastic Agent**: A unified agent that collects logs, metrics, and endpoint security data from hosts and forwards them to Fleet Server. It replaces multiple Beats agents with a single, streamlined solution.
- **Fleet Server**: The central service that coordinates Elastic Agents, manages their enrollment, distributes configuration policies, and ensures secure communication with Elasticsearch. It acts as the control point for large-scale deployments.

Challenges faced.

- Syntax errors due to incorrect Linux distribution choice.
- Firewall misconfigurations (blocked ports or wrong IP rules).
- Incorrect port usage (e.g., Fleet Server requiring port 8220 instead of 443).
- Certificate errors (x509: certificate signed by unknown authority) requiring the --insecure flag.
- Failed agent enrollment due to misconfigured firewall rules or IP address restrictions.