


Day 7 – Elastic Agent and Fleet Server Setup


Obiettivi


- **Setup del Fleet Server**
- **Installare un Elastic Agent sul server Windows**
- **Integrare Windows Server con il Fleet Server**


Fleet Server


Procediamo con il deployment di un **Fleet Server**, configurato con le seguenti specifiche:

**Optimized Cloud Compute - Dedicated CPU**
Virtual machines for more demanding business apps, e.g. production websites, CI/CD, video transcoding, or larger databases.

 **Toronto** Canada



Ubuntu
22.04 LTS x64

**MYDFIR-SOC-Challenge**
IP Address
172.31.0.4

**Virtual Private Cloud 2.0** Free
If you have VPCs in this region, you can select one below. Otherwise a default VPC will be created. An IP is provided, but you may set a different IP if desired.
[Learn more](#)

Choose Plan

General Purpose CPU Optimized Memory Optimized Storage Optimized

Name	Cores	Memory	Storage	Bandwidth	Price
 30 GB NVMe	1 vCPU	4 GB	30 GB NVMe	4 TB	\$30/month \$0.045/hour

Setup Fleet Server

Ci colleghiamo alla Web UI di **Elasticsearch**, vado nella sezione «Fleet» ed inseriamo il nome e l'IP pubblico del **Fleet Server**. Successivamente, clicchiamo su 'Generate' per completare la configurazione.

⚙ Management

Dev Tools

Integrations

Fleet

Osquery

Stack Monitoring

Stack Management

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](#)

Add Fleet Server

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

1

Get started with Fleet Server

First, set the public IP or host name and port that agents will use to reach Fleet Server. It uses port **8220** by default ^②. We'll then generate a policy for you automatically.

Name

Fleet-server

URL

216.

+ Add another URL

Generate Fleet Server policy

Setup Fleet Server

La policy per il **Fleet Server** è stata creata. Ora dobbiamo installare **l'Elastic Agent** sul **Fleet Server** appena avviata su **Vultr**. Questo server fungerà da punto centrale a cui si connetteranno tutti gli host che vogliamo monitorare.

✓ Get started with Fleet Server

✓ Fleet Server policy created.

Fleet server policy and service token have been generated. Host configured at [https://216\[REDACTED\]](https://216[REDACTED]). You can edit your Fleet Server hosts in [Fleet Settings](#).

2 Install Fleet Server to a centralized host

Install Fleet Server agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. For additional guidance, see our [installation docs](#).

Linux Tar Mac Windows RPM DEB

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.1-linux-x86_64.tar.gz
tar xzvf elastic-agent-8.15.1-linux-x86_64.tar.gz
cd elastic-agent-8.15.1-linux-x86_64
sudo ./elastic-agent install \
  --fleet-server-es=https://155[REDACTED] \
  --fleet-server-service-token=[REDACTED] \
  --fleet-server-policy=fleet-s[REDACTED] \
  --fleet-server-es-ca-trusted-[REDACTED] \
  --fleet-server-port=8220
```

Setup Fleet Server

Anche in questo caso, mi collego al **Fleet Server** tramite **SSH**, eseguo l'aggiornamento dei repository con i comandi ``apt-get update`` e ``apt-get upgrade``.


```
root@Fleet-server: ~  
PS C:\Windows\system32> ssh root@  
The authenticity of host '216.128.  
ECDSA key fingerprint is SHA256:r  
  
* Management:  https://landscape.canonical.com  
* Support:      https://ubuntu.com/pro  
  
System information as of Wed Sep 18 09:42:23 PM UTC 2024  
  
System load:  0.0          Processes:           119  
Usage of /:   25.0% of 27.57GB  Users logged in:    0  
Memory usage: 5%          IPv4 address for enp1s0: 216.128.184.207  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
root@Fleet-server:~#
```





Setup Fleet Server


Prima di installare l'**Elastic Agent** sul **Fleet Server**, è necessario configurare il firewall del server **ELK** per consentire il traffico dal Fleet Server verso l'ELK. Questo passaggio include due azioni:

- Modificare il firewall della macchina ELK per permettere il traffico proveniente dall'IP pubblico del Fleet Server.
- Configurare il sistema operativo dell'ELK per consentire il traffico in entrata attraverso la porta 9200, che è quella utilizzata da Elasticsearch per comunicare con l'agent

Inbound IPv4 Rules

 **Please note:** rule updates may take up to 120 seconds to propagate to all servers

Action	Protocol	Port (or range) ?	Source	Notes	Action
accept	SSH	22	Anywhere	0.0.0.0/0	Add note +
accept	TCP	1 - 65535	151		 
accept	TCP	1 - 65535	216		 

 root@ELK: ~

```
root@ELK:~# root@ELK:~# ufw allow 9200
Rule added
Rule added (v6)
root@ELK:~#
```

Setup Fleet Server

Procediamo con l'installazione dell'**Elastic Agent** (grazie ai comandi indicati su Elasticsearch come in figura nella slide 5) sul **Fleet Server** fino a completamento. Una volta conclusa, possiamo verificare la corretta registrazione dell'agente nell'istanza di Elasticsearch, sotto la sezione Fleet. A questo punto, possiamo procedere con l'installazione di un agente anche sul **Windows Server** precedentemente implementato su **Vultr**.

```
[ ==] Waiting For Enroll... [12s] {"log.level":"info","@timestamp":"2024-09-18T22:00:25.931Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).enrollWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":518},"message":"Starting enrollment to URL: https://Fleet-server:8220/","ecs.version":"1.6.0"}
[    ] Waiting For Enroll... [13s] {"log.level":"info","@timestamp":"2024-09-18T22:00:27.225Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).daemonReloadWithBackoff","file.name":"cmd/enroll_cmd.go","file.line":481},"message":"Restarting agent daemon, attempt 0","ecs.version":"1.6.0"}
[  =] Waiting For Enroll... [13s] {"log.level":"info","@timestamp":"2024-09-18T22:00:27.228Z","log.origin":{"function":"github.com/elastic/elastic-agent/internal/pkg/agent/cmd.(*enrollCmd).Execute","file.name":"cmd/enroll_cmd.go","file.line":299},"message":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
[  =] Done [13s]
Elastic Agent has been successfully installed.
root@fleet-server:~/elastic-agent-8.15.1-linux-x86_64#
```



Fleet Server connected

You can now continue enrolling agents with Fleet.

[Continue enrolling Elastic Agent](#)

Da Elasticsearch, selezioniamo l'agente che desideriamo installare sul Windows Server e otteniamo i comandi necessari dalla piattaforma. Questi comandi verranno eseguiti tramite PowerShell sul server Windows, permettendo l'installazione dell'Elastic Agent, che si interfacerà direttamente con il Fleet Server. Una volta lanciati i comandi, procederemo con l'installazione dell'agente sul Windows Server.

Add agent

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

[Enroll in Fleet](#) [Run standalone](#)

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

1 What type of host do you want to monitor?

Settings for the monitored host are configured in the [agent policy](#). Create a new agent policy to get started.

Windows Policy

Create policy

☒ Collect system logs and metrics ⓘ

> [Advanced options](#)

Add agent

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

[Enroll in Fleet](#) [Run standalone](#)

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

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](#).

Linux Tar Mac **Windows** RPM DEB Kubernetes

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.15.1-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.15.1-windows-x86_64.zip
cd elastic-agent-8.15.1-windows-x86_64
.\elastic-agent.exe install --url=https://fleet.example.com
```

Setup Fleet Server

Abbiamo scelto l'agent in base alla piattaforma, in questo caso Windows. Una volta avviato il **Windows Server** su **Vultr**, avviamo lo script di installazione dell'agent fornito da Elasticsearch.

Questo script è eseguito tramite **PowerShell** sul server. Prima di proseguire, però, dobbiamo modificare l'host URL del Fleet Server, che comunica con l'**Elastic Agent**.

Andando nella sezione 'Fleet' di **Elasticsearch**, sotto 'Settings' e 'Fleet Server Hosts', abbiamo cambiato la porta da 443 a 8220, che è la porta corretta per la comunicazione con il Fleet Server.

Dopo questa modifica, l'agent su Windows completerà correttamente l'enrollment e l'installazione, permettendo la comunicazione con il Fleet Server e l'invio dei dati verso Elasticsearch/Kibana.

Fleet

Centralized management for Elastic Agents.

- Agents
- Agent policies
- Enrollment tokens
- Uninstall tokens
- Data streams
- Settings**

Fleet server hosts


Specify the URLs that your agents will use to connect to a Fleet Server. If multiple URLs exist, Fleet will show the first provided URL. [Elastic Agent Guide](#).

Name	Host URLs
Fleet-server	https://216.144.443

+ Add Fleet Server

Outputs

Specify where agents will send data.

Name	Type	Hosts	Status
default 	Elasticsearch	https://153.9200	

+ Add output


Agent Binary Download

Specify where the agents will download their binary from. Checked default will apply to all policies unless overwritten.

Name	Host
Elastic Artifacts	https://artifacts.elastic.co/downloads/

+ Add agent binary source

Edit Fleet Server

 Changing these settings can break your agent connections

Invalid settings can break the connection between Elastic Agent and Fleet Server. If this happens, you will need to re-enroll your agents.


Name

URL

Specify multiple URLs to scale out your deployment and provide automatic failover. If multiple URLs exist, Fleet shows the first provided URL for enrollment purposes. Enrolled Elastic Agents will connect to the URLs in round robin order until they connect successfully. For more information, see the [Fleet and Elastic Agent Guide](#).

+ Add another URL

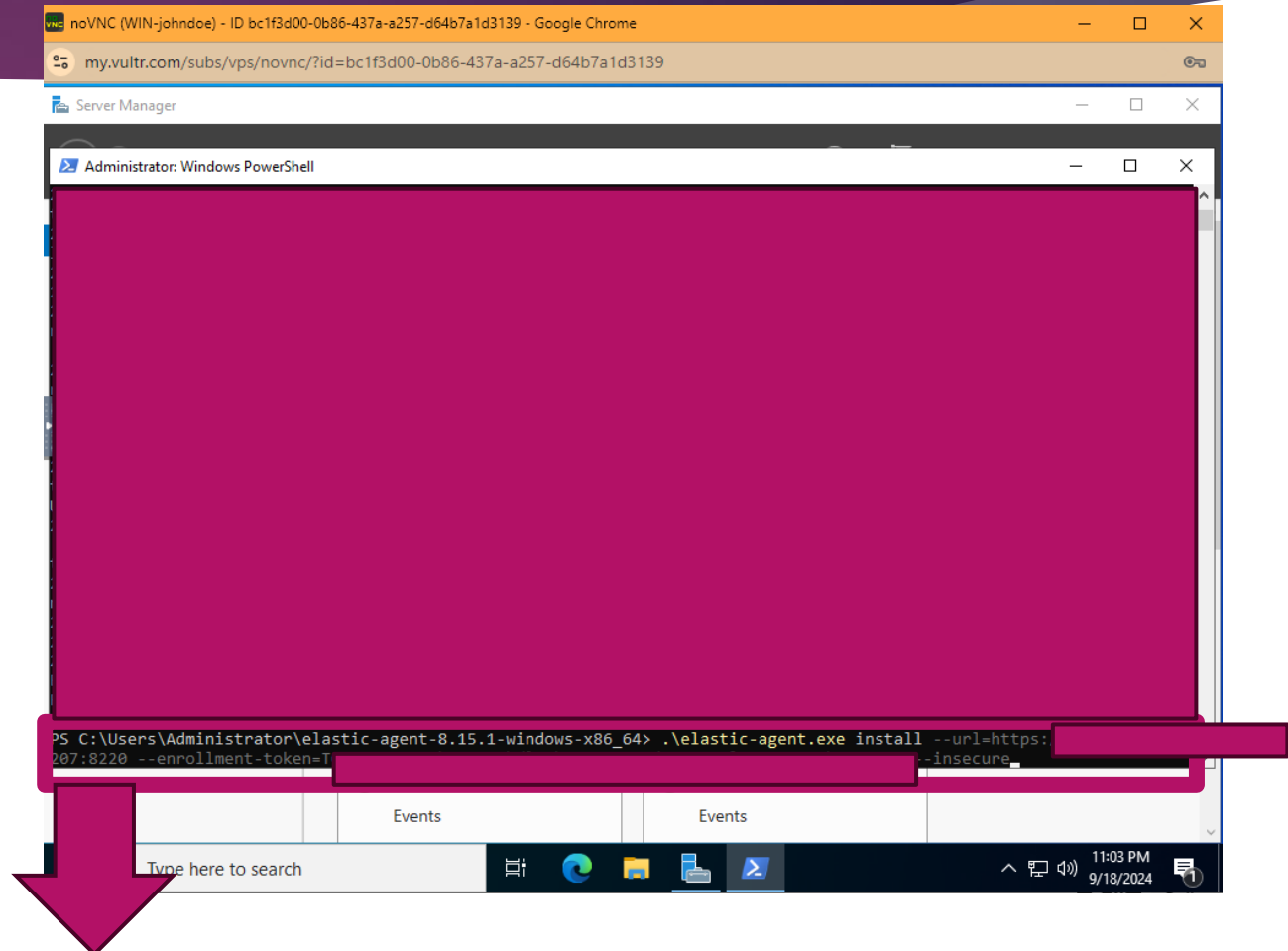
Proxy

 Be aware that changing the proxy settings may cause Elastic Agents to lose connectivity. Please ensure that agents have reachability to the proxy in the context that it is being used for.

☒ Make this Fleet server the default one.

Setup Fleet Server

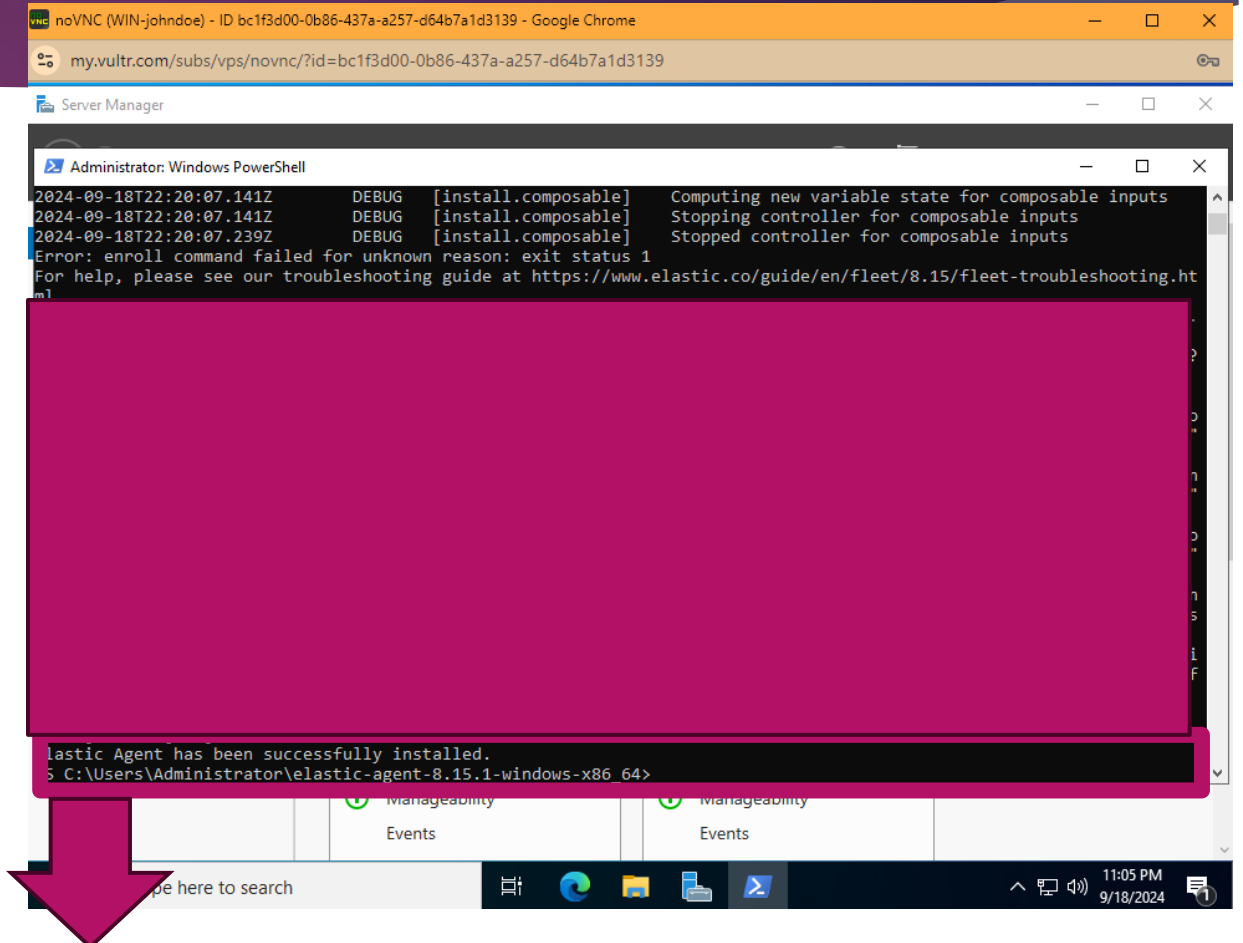
Prima di avviare lo script di installazione dell'agent, abbiamo effettuato alcune modifiche necessarie. Abbiamo aggiornato lo script per cambiare la porta di comunicazione del Fleet Server da 443 a 8220, che è la porta corretta per l'interazione con il Fleet Server. Inoltre, per bypassare la verifica dei certificati SSL/TLS e semplificare la configurazione in questo ambiente non di produzione, abbiamo aggiunto l'opzione `--insecure` al comando di installazione. Questa opzione permette di procedere senza richiedere un certificato valido, evitando la necessità di una CA propria



```
PS C:\Users\Administrator\elastic-agent-8.15.1-windows-x86_64> .\elastic-agent.exe install --url=https://216[redacted]  
8220 --enrollment-token=[redacted] --insecure
```

Setup Fleet Server

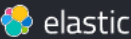
Dopo aver applicato queste modifiche, l'agent su Windows ha completato correttamente l'enrollment e l'installazione, stabilendo la comunicazione con il Fleet Server e permettendo l'invio dei dati verso Elasticsearch/Kibana.






```
[ ] DONE [100%]  
Elastic Agent has been successfully installed.  
PS C:\Users\Administrator\elastic-agent-8.15.1-windows-x86_64>
```


Setup Fleet Server

Nella sezione Agents troviamo ora quello di Windows.



Find apps, content, and more.






D

Fleet


Agents


 Send feedback

Fleet

Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

 Ingest Overview Metrics

 Agent Info Metrics

Agent activity

Add Fleet Server

Add agent

Filter your data using KQL syntax

Status 4

Tags 0

Agent policy 2

Upgrade available

Showing 2 agents

Clear filters

Healthy 2

Unhealthy 0

Updating 0

Offline 0

Inactive 0

Unenrolled 0

<input type="checkbox"/>	Status	Host ↕	Agent policy ↕	CPU ⓘ	Memory ⓘ	Last activity ↕	Version ↕	Actions
<input type="checkbox"/>	Healthy	WIN-johndoe	Windows-Policy rev. 2	N/A ⓘ	N/A ⓘ	35 seconds ago	8.15.1	...
<input type="checkbox"/>	Healthy	Fleet-server	Fleet Server Policy rev. 2	0.51 %	224 MB	25 seconds ago	8.15.1	...

Rows per page: 20

< 1 >

Da 'Discover' possiamo anche vedere le metriche.

