Add elastic-agent to DShield Sensor

TLS Certificate is Need to Connect to ELK

Login the ELK server home user account and copy the ca.crt to ~.

```
$ sudo cp /var/lib/docker/volumes/dshield-elk_certs/_data/ca/ca.crt  .
```

```
$ sudo chown guy:guy ca.crt (change it to your username:username)
```

Login DShield Sensor

From the DShield sensor, copy the certificate to this directory

```
$ scp guy@192.168.25.231:/home/guy/ca.crt .
```

```
$ sudo mv ca.crt /usr/local/share/ca-certificates
```

```
$ sudo update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

Add ELK IP to DShield sensor:

```
$ sudo su -
```

```
# echo "192.168.25.231 fleet-server" >> /etc/hosts
```

```
# echo "192.168.25.231 es01" >> /etc/hosts
```

```
# sudo apt-get install elastic-agent
```

Note: elastic-agent must be the same version as the ELK server. If the agent is a newer version, you need to use a command like this or update the .env file to reflect the current version of ELK:

```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.0-amd64.deb
```

```
sudo dpkg -i elastic-agent-8.11.0-amd64.deb
```

Enable the elastic-agent

```
$ sudo systemctl enable elastic-agent
```

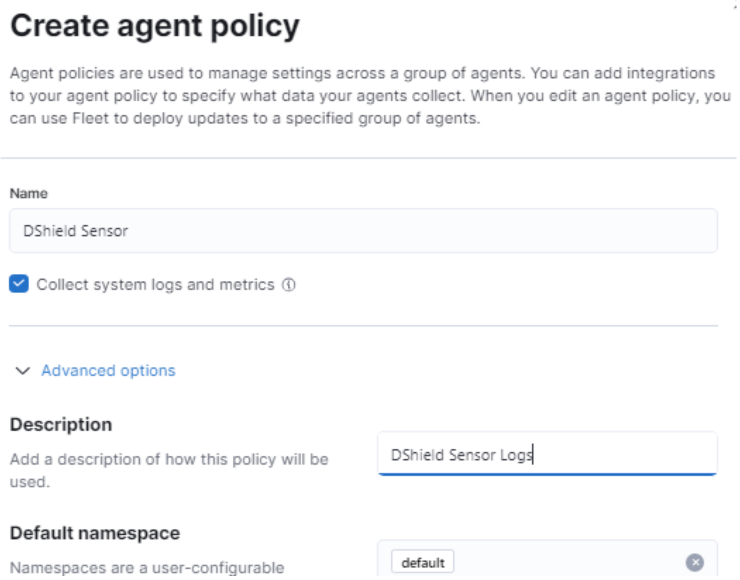
```
$ sudo systemctl stop elastic-agent
```

```
$ sudo systemctl start elastic-agent
```

Reference: https://hub.docker.com/_/elasticsearch

To add elastic-agent to DShield sensor do:

Management -> Fleet -> Agent policies -> Create agent policy:



Create agent policy

Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

Name

DShield Sensor

☑ Collect system logs and metrics ⓘ

Description

Add a description of how this policy will be used.

DShield Sensor Logs

Default namespace

Namespaces are a user-configurable

default

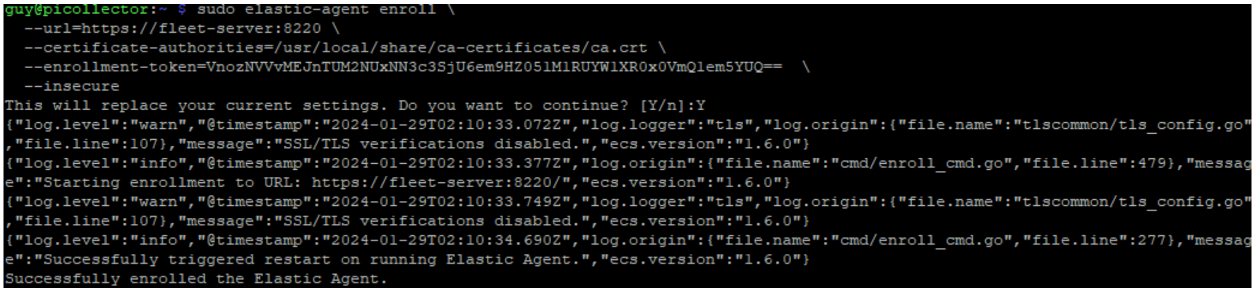
Select: Create agent policy

After the policy is created, select the policy (DShield Sensor), Actions -> Add agent

Pick RPM and copy line 3 and format it like this:

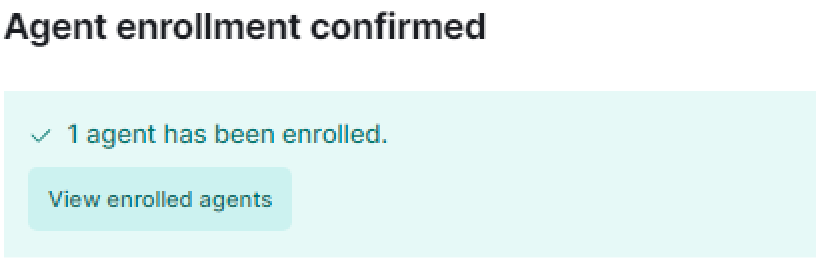
```
sudo elastic-agent enroll \

  --url=https://fleet-server:8220 \

  --certificate-authorities=/usr/local/share/ca-certificates/ca.crt \

  --enrollment-token=RVFIbEo0MEJKRzNBblNzWHJCb3U6dy1WemJnRnVRVzJJZTdDX29PR2Ftdw== \

  --insecure
```

The DShield sensor should show this confirmation after it is added:



```
guy@picollector:~ $ sudo elastic-agent enroll \
  --url=https://fleet-server:8220 \
  --certificate-authorities=/usr/local/share/ca-certificates/ca.crt \
  --enrollment-token=VnozNVVvMEJnTUM2NUxNN3c3SjU6em9HZ05lM1RUYW1XR0x0VmQ1em5YUQ==  \
  --insecure
This will replace your current settings. Do you want to continue? [Y/n]:Y
{"log.level":"warn","@timestamp":"2024-01-29T02:10:33.072Z","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go"
,"file.line":107},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-01-29T02:10:33.377Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":479},"messag
e":"Starting enrollment to URL: https://fleet-server:8220/","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2024-01-29T02:10:33.749Z","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go"
,"file.line":107},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-01-29T02:10:34.690Z","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":277},"messag
e":"Successfully triggered restart on running Elastic Agent.","ecs.version":"1.6.0"}
Successfully enrolled the Elastic Agent.
```

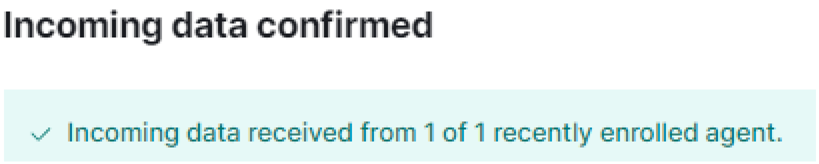
The server will show the following:



Agent enrollment confirmed

✓ 1 agent has been enrolled.

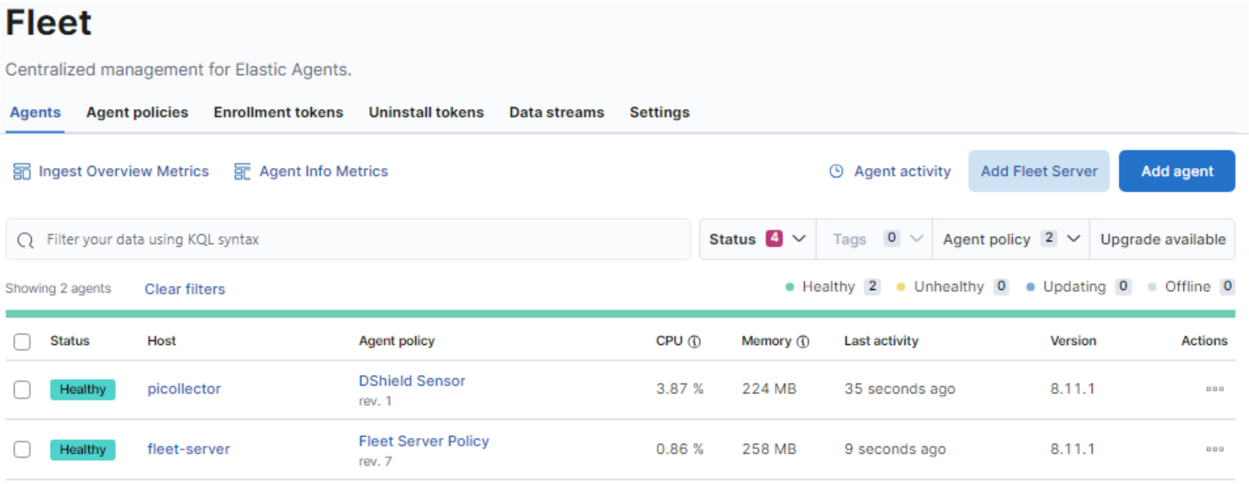
View enrolled agents



Incoming data confirmed

✓ Incoming data received from 1 of 1 recently enrolled agent.

This confirm the DShield sensor is now added to ELK



Fleet

Centralized management for Elastic Agents.

Filter your data using KQL syntax | Status 4 | Tags 0 | Agent policy 2 | Upgrade available

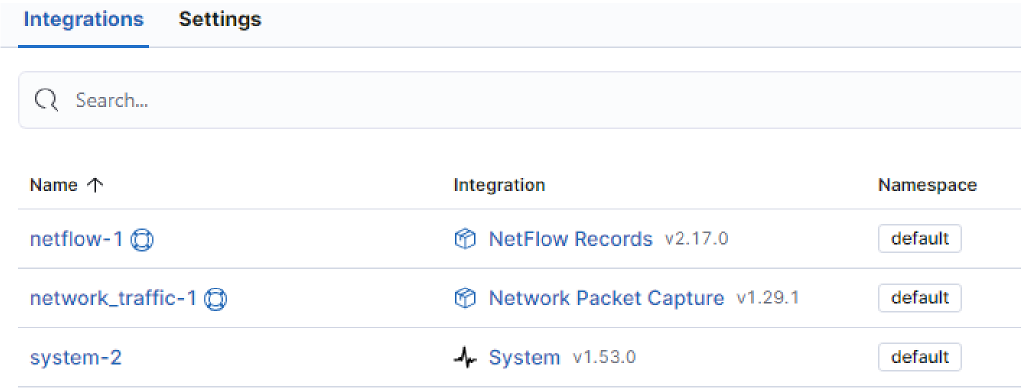
Showing 2 agents Clear filters

● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 0

☐	Status	Host	Agent policy	CPU ⓘ	Memory ⓘ	Last activity	Version	Actions
☐	Healthy	picollector	DShield Sensor rev. 1	3.87 %	224 MB	35 seconds ago	8.11.1	···
☐	Healthy	fleet-server	Fleet Server Policy rev. 7	0.86 %	258 MB	9 seconds ago	8.11.1	···

Now we can configure the Agent policies by adding integration like we did for the Fleet Server Policy, select Agent policies -> DShield Sensor -> Add integration:

- NetFlow Records (add-on with softflowd if you want NetFlow data from the sensor)
- Network Traffic (packetbeat equivalent)
- System is the default agent



Name ↑	Integration	Namespace
netflow-1	NetFlow Records v2.17.0	default
network_traffic-1	Network Packet Capture v1.29.1	default
system-2	System v1.53.0	default

Configure softflowd Application

This application will capture NetFlow traffic targeting your DShield sensor and report it to ELK under the NetFlow dashboard

```
$ sudo vi /etc/softflowd/default.conf
```

Set the interface (usually eth0 for PI)

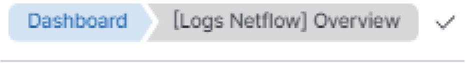
Set: options= "-v 9 -P udp -n 127.0.0.1:2055" (Must be double quotes)

Save the changes and restart the service

```
$ sudo systemctl restart softflowd
```

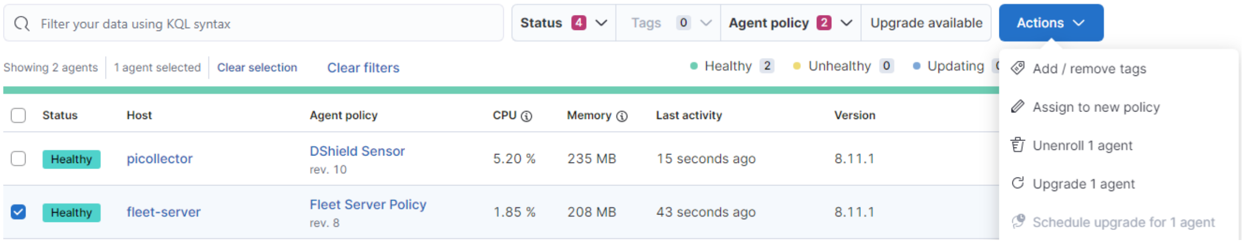
```
$ netstat -an | grep 2055  (Confirm softflowd is running)
```

The flows can be viewed with this dashboard:



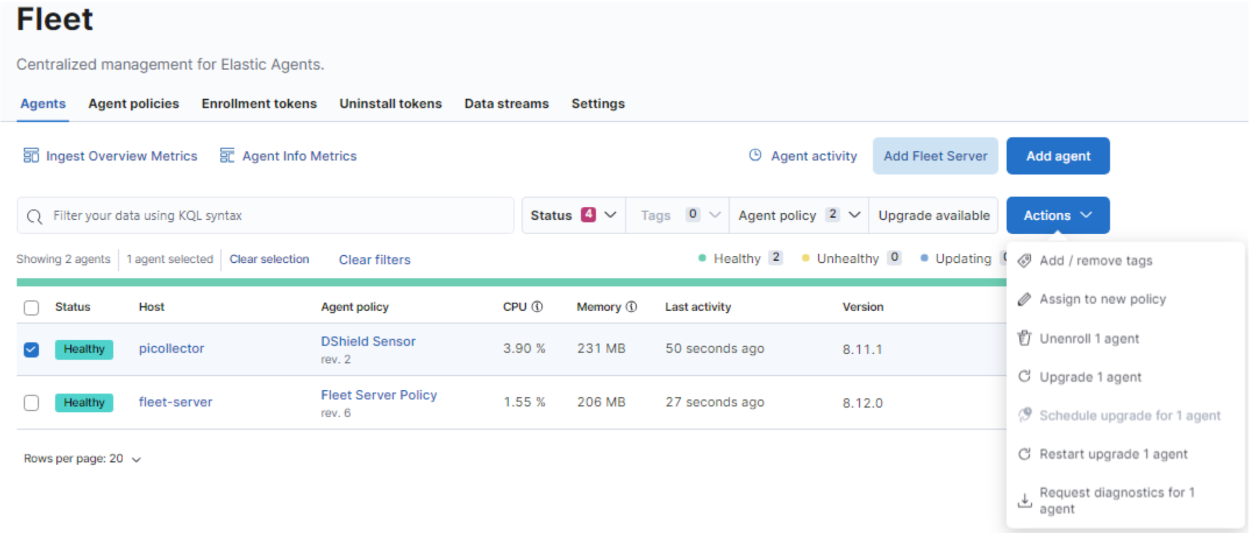
Upgrading elastic-agents

When you upgrade all the applications, elastic-agents must be upgraded via the interface. Selecting the fleet-server and action, the drop-down menu shows the agent can be upgraded. Proceed with the upgrade.



	Status	Host	Agent policy	CPU	Memory	Last activity	Version
☐	Healthy	picollector	DShield Sensor rev. 10	5.20 %	235 MB	15 seconds ago	8.11.1
☑	Healthy	fleet-server	Fleet Server Policy rev. 8	1.85 %	208 MB	43 seconds ago	8.11.1

The next version is 8.12.0 and proceed to Upgrade agent



	Status	Host	Agent policy	CPU	Memory	Last activity	Version
☑	Healthy	picollector	DShield Sensor rev. 2	3.90 %	231 MB	50 seconds ago	8.11.1
☐	Healthy	fleet-server	Fleet Server Policy rev. 6	1.55 %	206 MB	27 seconds ago	8.12.0

Upgrading the agent to 8.12.0 as per the above picture can only be done if available either from the GUI or from the command line. If available, this is the command to update the agent:

```
$ sudo apt-get upgrade elastic-agent
```