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:

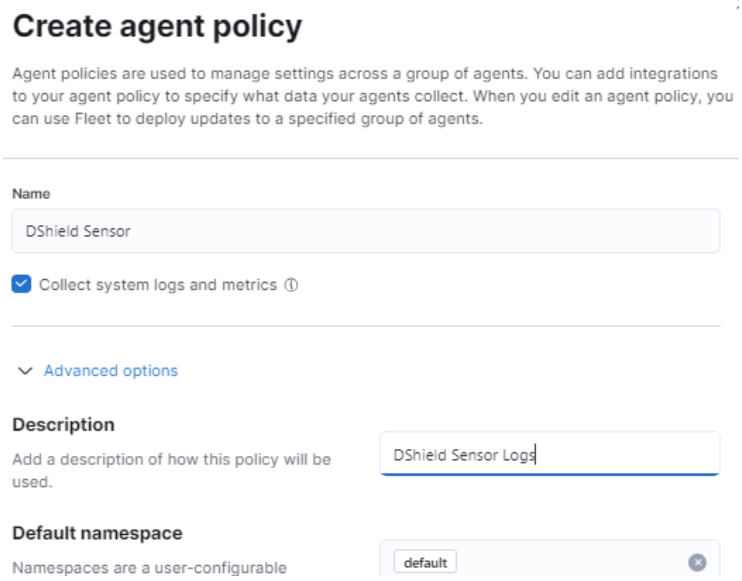
```
curl -L -O https://artifacts.elastic.co/downloads/beats/elastic-agent/elastic-agent-8.11.0-amd64.deb

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

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

To add elastic-agent to DShield sensor do:

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



Select: Create agent policy

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

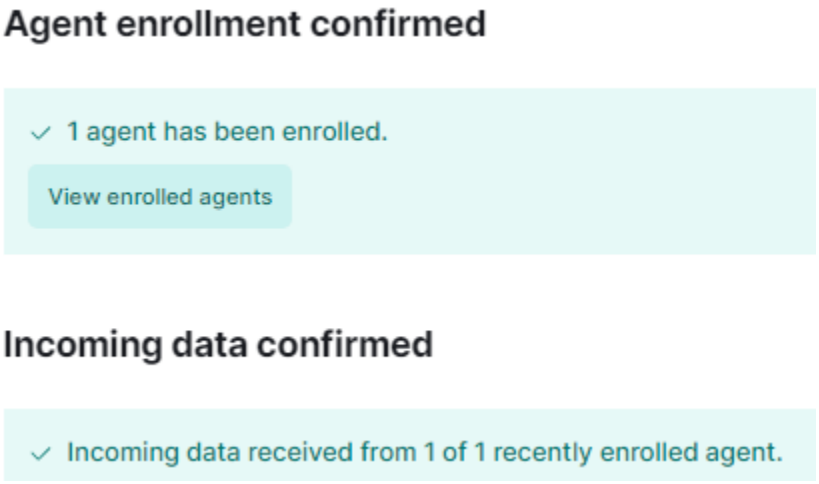
Pick RPM and copy line 3 and format it like this:

```
sudo elastic-agent enroll \
  --url=https://fleet-server:8220 \
  --certificate-authorities=/usr/local/share/ca-certificates/ca.crt \
  --enrollment-token=RVFIbEo0MEJKRzNBblNzWHJCb3U6dy1WemJnRnVRVzJJZTdDX29PR2Ftdw== \
  --insecure
```

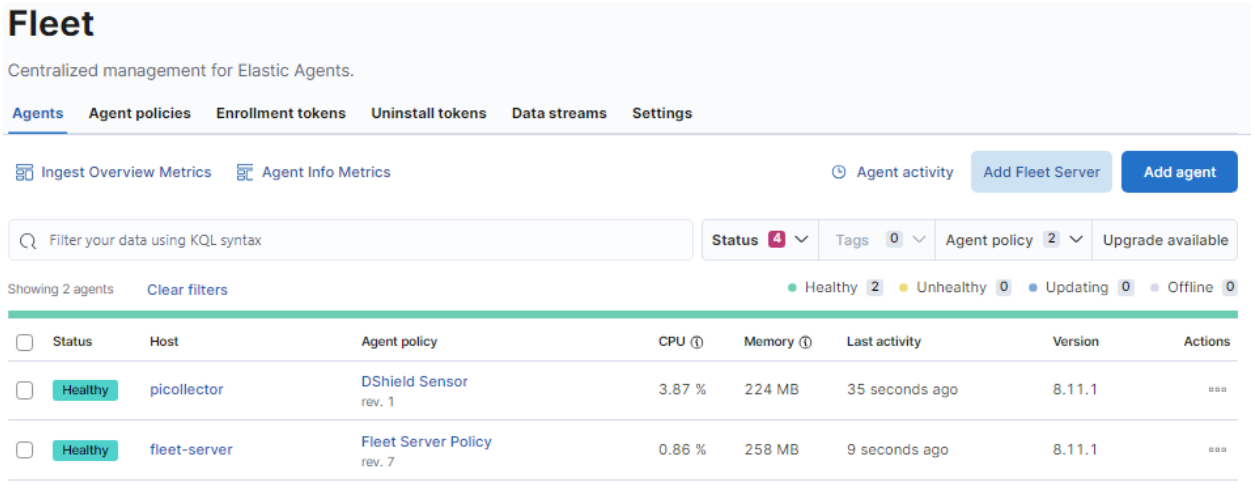
The DShield sensor should show this confirmation after it is added:

```
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:

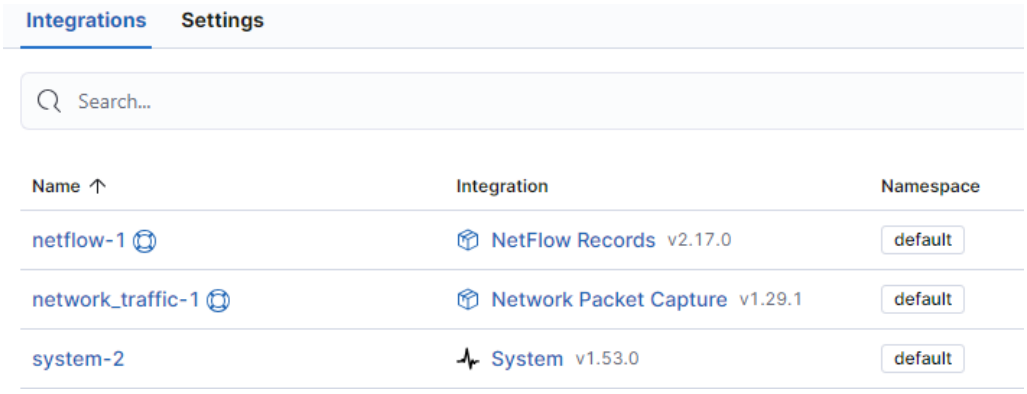


This confirm the DShield sensor is now added to ELK



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



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)

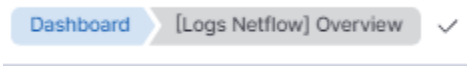
Set: options= "-v 9 -P udp -n 127.0.0.1:2055" (Must be double quotes)

Save the changes and restart the service

$ sudo systemctl restart softflowd

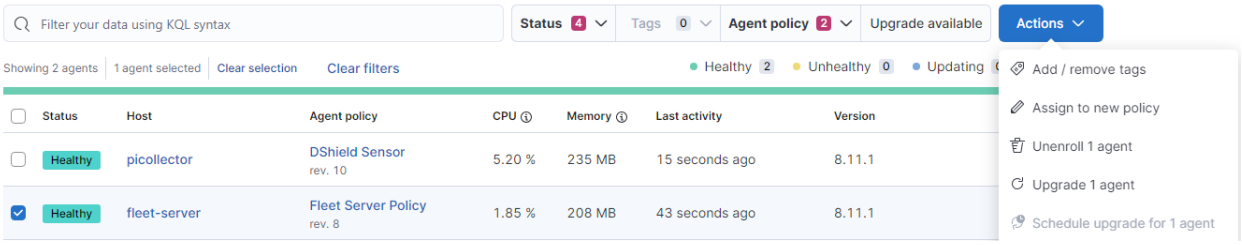
$ netstat -an | grep 2055 (Confirm softflowd is running)

The flows can be viewed with this dashboard:

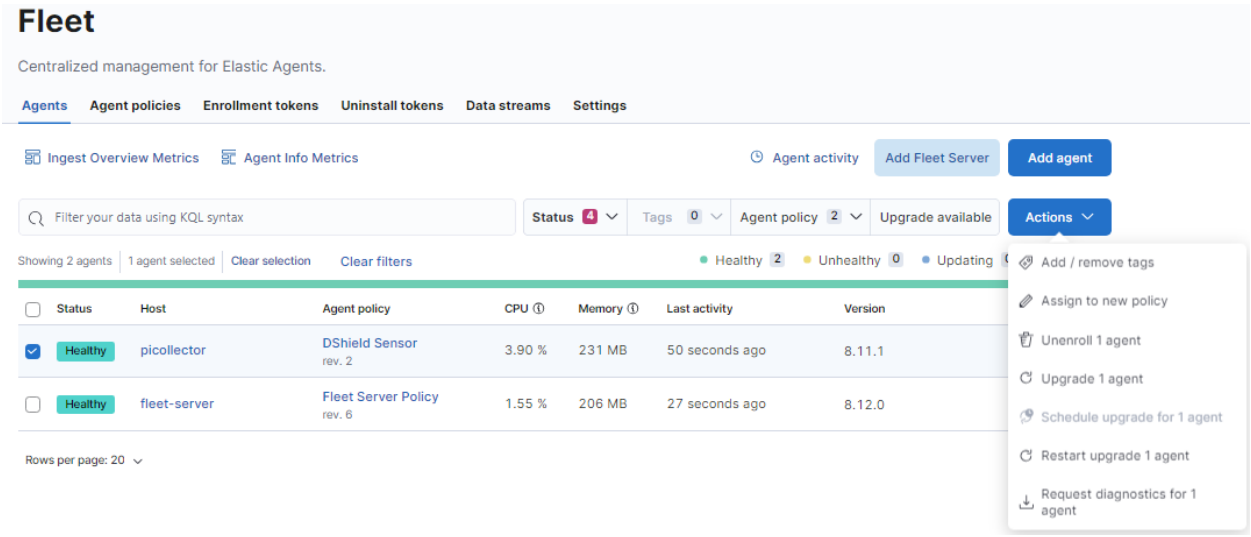


Upgrading elastic-agents

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.



The next version is 8.12.0 and proceed to Upgrade agent



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