# 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 .

From the DShield sensor, copy the certificate to this directory

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

\$ 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

# To add elastic-agent to DShield sensor do

Management -> Fleet -> Agent policies -> 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 Advanced options Description Add a description of how this policy will be used. Default namespace Namespaces are a user-configurable

Select: Create agent policy

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

Pick RPM and copy line 2 & 3 and add configure your request like this:

sudo elastic-agent enroll \

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

If the agent confirmed that it is added, the following will show:

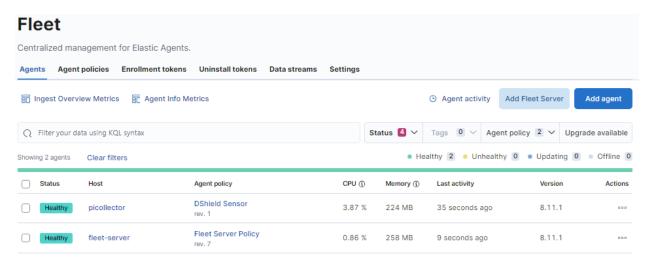
## Agent enrollment confirmed



# Incoming data confirmed

 $\,\,\checkmark\,\,$  Incoming data received from 1 of 1 recently enrolled agent.

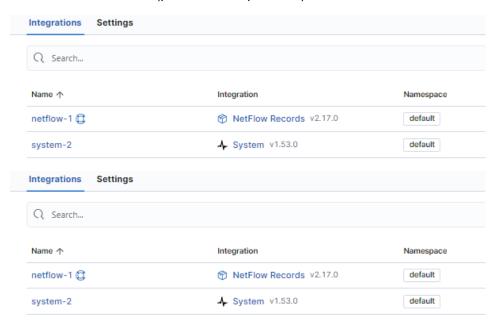
This confirm the DShield sensor is now added to ELK



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
- Elastic Defend (Protection level → Detect)

Network Traffic (packetbeat equivalent)



# Configure softflowd Application

\$ 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

