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:

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

✓ 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.

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**

	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
- 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