Elastic Agent

Friday, August 23, 2024 9:12 AM

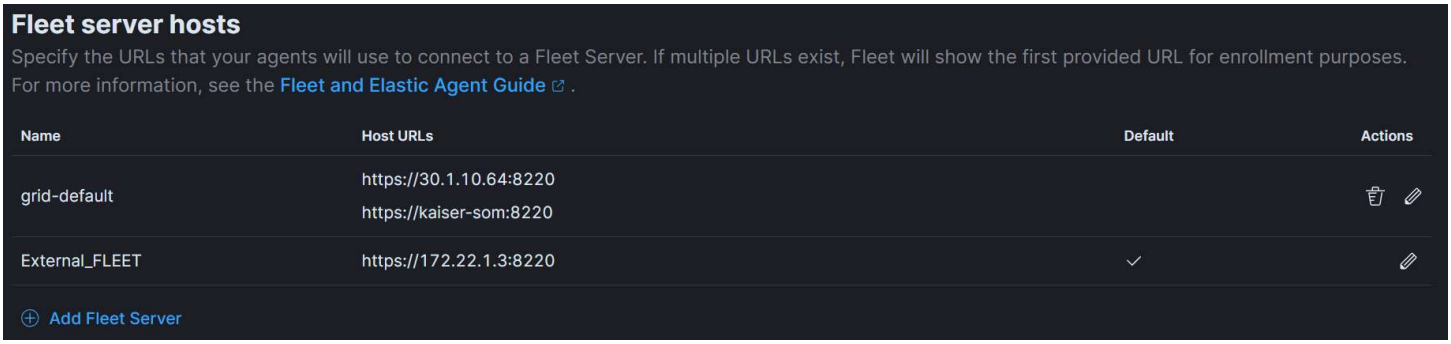
Download the elastic agent from online, not from the downloads page from security onion.
Unzip the folder and place in splunk in your deployment app.

elastic-agen
t-8.10.4-...
(here is the 8.10.4 zip of the elastic agent)

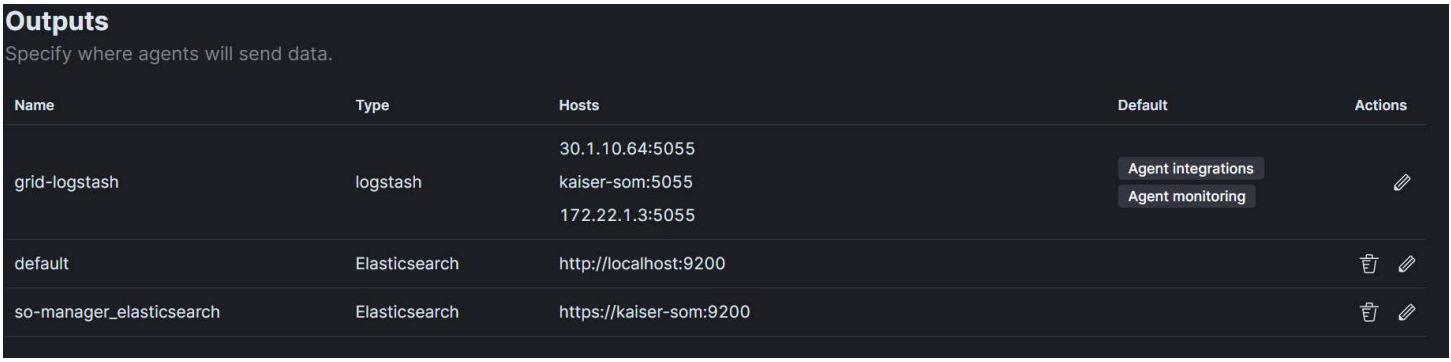
```
root@splunk:/opt/splunk/etc/deployment-apps/dco_tools/bin# ls
deploy.bat  elastic-agent-8.10.4-windows-x86_64  README  Sysmon64.exe  sysmonconfig-with-filedelete.xml
```

(here is where that unzip file goes in splunk)

Now go to Fleet in security onion > go to settings tab.
For Fleet Server Host, select add fleet server and make it your external IP. Make it default.



For Outputs, go to security onion CLI and stop the logstash service
Sudo so-logstash-stop
Click on the the pencil for grid-logstash and add a host (your external IP)



Start the Logstash service in security onion
Sudo so-logstash-start

Make changes to the deploy.dat in splunk as needed

```
if "%ElasticAgentStatus%"=="" (
    cd %ElasticAgentDir%
    .\elastic-agent.exe install --insecure --force --url=https://172.22.1.3:8220 --enrollment-token=SG5yMmRaRUJHSl9wZHo4LWttbV
A6OUJQSzM4RkdSV3lheXRkV1laV0tGUQ==
    net start 'Elastic Agent'
```

Here is an example of what would be in the deploy.bat (change the enrollment key to what is in your security onion, this is found in add agent > select endpoint initial > go to windows and the shown command will be present with the right enrollment key)