If the host does not appear in fleet, use the following to troubleshoot.

With admin boosted cmd prompt:

C:\Program Files\osquey\osqueryd\osqueryd.exe --flagfile=C:\Program Files\osquery\osquery.flags --verbose --tls\_dump

Fleet Credentials:

IP addr: 192.168.50.156

Email: nccs\_fleet@gmail.com

Password: nccs\_fleet123@

First, we will download msi file on windows for osquery by using this link and then install it.

https://osquery.io/downloads/official/4.5.1

After installation, now create notepad files as admin and fetch enroll\_secret and fleet\_cert.pem and then paste into the files respectively. These two files should be created in the path “C:\Program Files\osquery\certs\”.

make entry in osquery.flags file whose path is “C:\Program Files\osquery”.

--enroll\_secret\_path=C:\Program Files\osquery\certs\enroll\_secret.txt

--tls\_server\_certs=C:\Program Files\osquery\certs\fleet\_cert.pem

--tls\_hostname=192.168.50.156:8080

--host\_identifier=uuid

--enroll\_tls\_endpoint=/api/v1/osquery/enroll

--config\_plugin=tls

--config\_tls\_endpoint=/api/v1/osquery/config

--config\_tls\_refresh=10

--disable\_distributed=false

--distributed\_plugin=tls

--distributed\_interval=10

--distributed\_tls\_max\_attempts=3

--distributed\_tls\_read\_endpoint=/api/v1/osquery/distributed/read

--distributed\_tls\_write\_endpoint=/api/v1/osquery/distributed/write

--logger\_plugin=tls

--logger\_tls\_endpoint=/api/v1/osquery/log

--logger\_tls\_period=10

Now restart the osquery services. And then you will see the host.

Enroll-secret:

4uotZxAYBGDhFETIi+00/02MvhVj4Fd/

Certificate:

-----BEGIN CERTIFICATE-----

MIIFQzCCAysCFB7k6aaf0maAuMA6puJnWnB6nZj/MA0GCSqGSIb3DQEBCwUAMF4x

CzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb21lLVN0YXRlMSEwHwYDVQQKDBhJbnRl

cm5ldCBXaWRnaXRzIFB0eSBMdGQxFzAVBgNVBAMMDjE5Mi4xNjguNTAuMTU2MB4X

DTIwMTExNzA2MjI0NloXDTIxMTExODA2MjI0NlowXjELMAkGA1UEBhMCQVUxEzAR

BgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5

IEx0ZDEXMBUGA1UEAwwOMTkyLjE2OC41MC4xNTYwggIiMA0GCSqGSIb3DQEBAQUA

A4ICDwAwggIKAoICAQCzVFIEjVCr8t9Pyzamu5Qpk7PLp1uMaOrMUDMZenXXVa5v

onevP9+H3ufB6CGO1TSEaA0cqEGahboisevyT1LkVEWTL4XRMtwdsilVjjYJNydV

MZS83TQUl3KdqiCXMo9s/1XCl/QOaB5enONufTLDQraATwSENdjRRwgHagonULkr

xIDsWIHpVIlYMq3gr2iBMHGyLP9J4qybHvY7Sd3HGiiugJCqMqiUdC8CdvKv34VT

EaIcSl0IqkFSwKcsv/Mwqrmtqo6HiQxjBj6SJaQPEq0inPbnZBEUBW6Y9yjCUDLB

sTYA8iAoytikZsq6InuUn2R5yBvnUmhZJME+WCU54WA8jl+00P8Gjx60jl8bkLK0

Q+83g9/7PDiQIKLWkWq3AIcxwKxJPikhv9uVzTMe1HqISkR0x0OgV+rl5dJd33vw

Hw7OCLZDTDYlH3vXO0ELawD6WuIUrvzIwLEDMACm/06FFN8UNr1RJuh0JOCCTE/X

4yt/AE5dw2q35uUNVNc4oWDnqAFq3b6DuyilijZ/HofK/3ysgocvWrNQ+gkFNQrR

Gf9bnZYKQ+t5ovb91YA/m70Gb+vNTjDkY7syOfE3tMUDBO8B6PWfGYkRp+ymxpQA

vLhU+KjfafRERX52kNkrG3yJOcJ8cqDMFp4vadDhsOhhIbvPOcluOhaOFKIsvwID

AQABMA0GCSqGSIb3DQEBCwUAA4ICAQAV0U3NToxNuvxa/q3cruCAzQ5aqjMMHayD

foxjFGCPq9b1dAxXlybnMMg+PYShPxhiucF8zEXlK+R5l9bw2lXibonp65ELJWhg

OKSBqXSBpOXIE11tgYlyS7SsQ3khpNpRhPCoaW028KIQrNFjQEbFSamYgvTdeMLn

1m2VeMbICRNz2V8gP90E2KhWA+t8K3bvAcUFavRJpyDAsOQHr0/kCygbVJaZXBmh

1lb54OpY9D9DASoVCMFqlpTCCULva3O5vqu9IEPfjXk1FbqLYs05CYyaTkMxjStY

Hvwar5pz2bMWuxMIM0Os5BBIzNAdgQ3n901o6l3Mn3oJc2yB+M0HFaASesWGKQc0

nqeoyCc2YJdCHIJ3eP+RjkONKSq1nXSa35+G+oigFbtxB4jXASrq2TAoIMjZgTnk

1RnaRjFNPudKy3J4jy46SHL+itnwHX568FXUnGk+KxdtV3D9F1ZzOxIBEixcCor1

tB96KMBxaOZOMKZsZTHp4IYVK7mCRE0c1BYSoftLkgksmlInjcD1PftOcq0+AwJ1

041799dLgc35ETq4G3aMkvSKtiH2P5Nlp5Pwjp/WpSMXCqPACFQkenZUAayb4wGI

gEQ9DY1GVx89TQW6yK0XlJw07FOjhq2PJoYkhiXHD/6c/+GE9ZVT7hftfO+/qJ5H

P0vqW371NQ==

-----END CERTIFICATE-----

https://osquery.readthedocs.io/en/stable/deployment/file-integrity-monitoring/#:~:text=File%20Integrity%20Monitoring%20with%20osquery,files%20populate%20the%20file\_events%20table.

<https://blog.kolide.com/how-to-set-up-windows-file-integrity-monitoring-using-osquery-and-kolide-d5ac09db046b>

* <https://osquery.io/downloads/official/4.5.1>
* <https://osquery.readthedocs.io/en/stable/deployment/file-integrity-monitoring/#:~:text=File%20Integrity%20Monitoring%20with%20osquery,files%20populate%20the%20file_events%20table.>
* <https://blog.kolide.com/how-to-set-up-windows-file-integrity-monitoring-using-osquery-and-kolide-d5ac09db046b>