

1. LB2 - Beschreibung der Software OSQuery (10%)

1.1 Lernziele

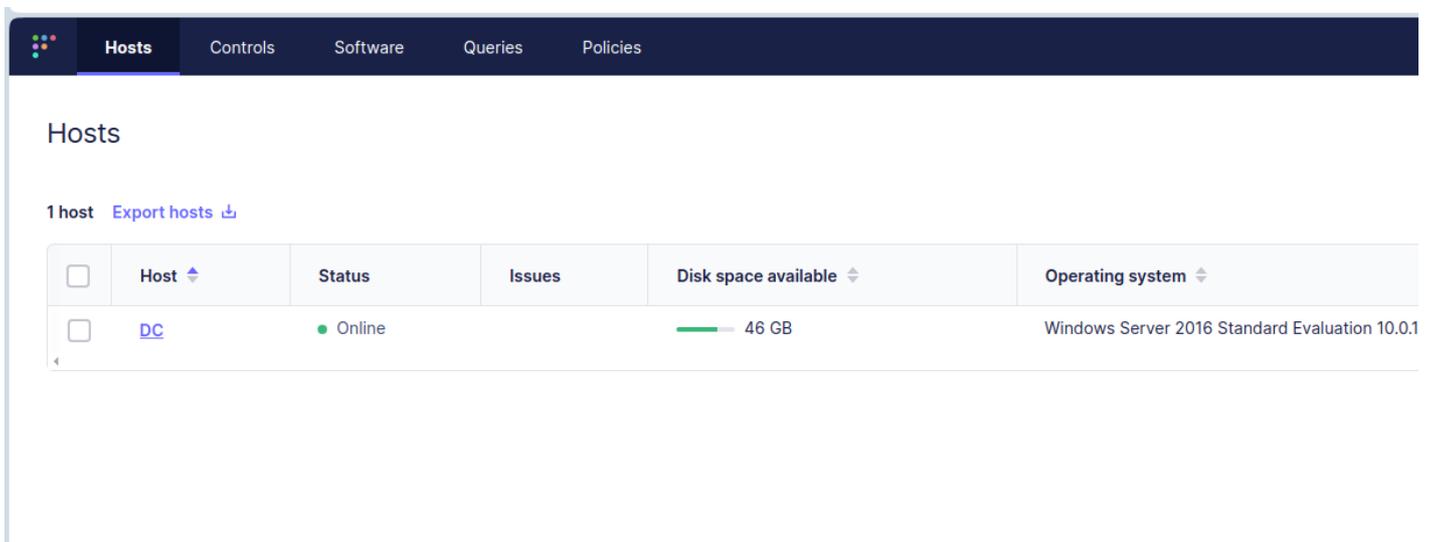
Jede/r Lernende:

- ...kann in eigenen Worten die Applikation OSQuery beschreiben
- ...kann OSQuery nach Vorgaben konfigurieren
- ...kann OSQuery anwenden (erste Tests durchführen)

1.2 Registrierung der Clients anstossen

Damit Sie mittels Osquery die Daten der Windows-VMs auslesen können, müssen die Geräte bei der Software *Fleet* registriert werden. Dies "sollte" eigentlich im normalen Bootup-Prozess der VMs geschehen sein...das ist allerdings kompliziert und aufgrund von verschiedenen Zertifikaten erfahrungsgemäss ziemlich fehleranfällig.

Idealerweise sollten Sie nach dem Login auf <http://192.168.56.105:8412> eigentlich die folgende View sehen:



The screenshot shows the OSQuery Fleet web interface. At the top, there is a navigation bar with tabs for 'Hosts', 'Controls', 'Software', 'Queries', and 'Policies'. The 'Hosts' tab is selected. Below the navigation bar, the page title is 'Hosts'. There is a sub-header '1 host' and a link 'Export hosts' with a download icon. Below this is a table with columns: Host, Status, Issues, Disk space available, and Operating system. The table contains one row for a host named 'DC' with status 'Online', 46 GB of disk space available, and operating system 'Windows Server 2016 Standard Evaluation 10.0.1'.

Host	Status	Issues	Disk space available	Operating system
DC	Online		46 GB	Windows Server 2016 Standard Evaluation 10.0.1

Kein Host ersichtlich?

Sollten Sie keinen Host sehen, hat die Registrierung nicht funktioniert und Sie müssen die folgenden Schritte durchführen.

1.2.1 Nochmals initialisieren

1. Stoppen Sie den osquery-Dienst auf Ihrer Windows-VM

- Öffnen Sie in der Windows VM die Webseite von Fleet `https://192.168.56.105:8412/` und klicken Sie auf `Add host`
- Laden Sie das `enrollment secret`, das `Fleet Certificate` und das `flagfile.txt` herunter

macOS

Windows

Linux (RPM)

Linux (deb)

ChromeOS

Advanced

Download your Fleet certificate:

[Download](#) ↓

Run this command with the [Fleet command-line tool](#) installed:

```
fleetctl package --type=YOUR_TYPE --fleet-url=https://192.168.56.105:8412
--enroll-secret=14/cEccvTxrpmFV9pZ4hifyAsr00jaT
--fleet-certificate=PATH_TO_YOUR_CERTIFICATE/fleet.pem
```

Distribute your package to add hosts to Fleet.

This works for macOS, Windows, and Linux hosts. To add Chromebooks, [click here](#).

[Plain osquery](#) ^

Download your enroll secret:

Osquery uses an enroll secret to authenticate with the Fleet server.

[Download](#) ↓

Download your Fleet certificate

Prove the TLS certificate used by the Fleet server to enable secure connections from osquery:

[Download](#) ↓

Download your flagfile:

If using the enroll secret and server certificate downloaded above, use the generated flagfile. In some configurations, modifications may need to be made.

[Download](#) ↓

- Ersetzen Sie im `flagfile.txt` den Host `192.168.56.105` mit dem Hostnamen `fleet`
- Führen Sie nun den Registrierungsbefehl (am Speicherort der Dateien, typischerweise im Downloads-Folder) nochmals aus: `osqueryd --flagfile=flagfile.txt --verbose`

Führen Sie jetzt diese Schritte auf beiden VMs durch - Achtung: Dieser Osqueryd-Befehl muss in einer Konsole laufen, damit Sie mit Osquery arbeiten können

1.3 Aufträge und Bewertungskriterien

Recherche - OSQuery 0-4P:

- Was ist OSQuery? Wofür wird es verwendet
- Was ist die aktuellste Version von OSQuery?
- Was sind Beispiel-Anwendungen/Use-Cases bei welchen OSQuery helfen kann?

Wichtig

Auf Ihrem System wurde OSQuery bereits installiert und konfiguriert (Best-Practices) - **Tipp:** Betrachten Sie das Script "scripts/install-osquery.ps1"

Konfiguration / Testing - OSQuery 0-4P:

- Dokumentieren Sie das Config-File welches auf Ihrem System für OSQuery installiert ist
- Dokumentieren Sie die Struktur des Config-Files
- Führen Sie einen ersten Test mittels OSQuery durch und dokumentieren Sie das Resultat