Stellen Sie die ExtraHop ECA VM-Konsole auf Linux KVM bereit

Veröffentlicht: 2024-07-02

Dieses Dokument enthält Informationen zur Installation der virtuellen ExtraHop-Konsole auf einer Linux-Kernel-basierten virtuellen Maschine (KVM). In diesem Handbuch wird davon ausgegangen, dass Sie mit der grundlegenden KVM-Administration vertraut sind.

Falls Sie dies noch nicht getan haben, laden Sie die virtuelle ExtraHop-Konsolendatei für KVM von der ExtraHop Kundenportal.

Wichtig: Wenn Sie mehr als einen virtuellen ExtraHop-Sensor bereitstellen möchten, erstellen Sie die neue Instanz mit dem ursprünglichen Bereitstellungspaket oder klonen Sie eine vorhandene Instanz, die noch nie gestartet wurde.

Anforderungen

Bevor Sie die virtuelle ExtraHop-Konsole installieren können, stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

- Eine KVM-Hypervisor-Umgebung, die in der Lage ist, eine VM zu hosten, die Folgendes bietet:
  - 4 GB RAM
  - Zwei vCPUs.
  - Eine 4-GB-Startdiskette (Virtio-SCSI-Schnittstelle empfohlen)
  - Eine Datenspeicherfestplatte mit 40 GB oder mehr (Virtio-SCSI-Schnittstelle empfohlen)

  Die Hypervisor-CPU sollte Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Befehle unterstützen.
- Ein ExtraHop-Lizenzschlüssel für die virtuelle Konsole

Richtlinien zur Leistung

Die Performance des virtuellen ExtraHop Konsole hängt von der Anzahl der Sensoren ab, die Sie einsetzen, in Kombination mit der Anzahl der Geräte, die das System voraussichtlich in Ihrer Umgebung erkennen wird. Informationen zur Bestimmung der geeigneten Größe finden Sie in der Virtual ExtraHop Console Performance Guidelines.

Inhalt des Pakets

Das Installationspaket für KVM-Systeme ist ein `tar.gz` Datei, die die folgenden Elemente enthält:

eca.xml
: Die Domain-XML-Konfigurationsdatei

eca.xml.md5
: Eine MD5-Prüfsummendatei zur Überprüfung der Integrität der Datei eca.xml.

extrahop-boot.qcow2
: Die Bootdiskette

extrahop-boot.qcow2.md5
: Eine MD5-Prüfsummendatei zur Überprüfung der Integrität der Datei extrahop-boot.qcow2.

extrahop-data.qcow2

Die Datenspeicherfestplatte

extrahop-data.qcow2.md5

Eine MD5-Prüfsummendatei zur Überprüfung der Integrität der Datei extrahop-data.qcow2.

Bearbeiten Sie die Domain-XML-Konfigurationsdatei

Bearbeiten Sie die Konfigurationsdatei und erstellen Sie die virtuelle ExtraHop-Konsole.

1. Extrahieren Sie die `tar.gz` Datei, die das Installationspaket enthält.
2. Kopieren Sie die beiden Festplatten `extrahop-boot.qcow2` und `extrahop-data.qcow2` zu Ihrem KVM-System. Notieren Sie sich den Ort, an dem Sie diese Dateien speichern.
3. Öffnen Sie die Domain-XML-Konfigurationsdatei. Suchen und bearbeiten Sie die folgenden Werte:
   a) Ändern Sie den VM-Namen (`ExtraHop-ECA`) auf den Namen, den Sie Ihrer virtuellen ExtraHop-Konsole zuweisen möchten .

   ```
   <name>ExtraHop-ECA</name>
   ```

   b) Ändern Sie den Pfad der Quelldatei *[PFAD_ZUM_SPEICHER]* mit dem Speicherort, an dem Sie die virtuellen Festplattendateien in Schritt 1 gespeichert haben.

   ```
   <source file='[PATH_TO_STORAGE]/extrahop-boot.qcow2'/>
   <source file='[PATH_TO_STORAGE]/extrahop-data.qcow2'/>
   ```
4. Speichern Sie die XML-Datei.
5. Melden Sie sich bei der KVM-Konsole an.
6. Erstellen Sie die neue virtuelle ExtraHop-Konsole mit Ihrer überarbeiteten Domain-XML-Konfigurationsdatei, indem Sie den folgenden Befehl ausführen:

   ```
   virsh define eca.xml
   ```
7. Starten Sie die virtuelle Maschine, indem Sie den folgenden Befehl ausführen:

   ```
   virsh start <vm_name>
   ```

   Wo *<vm_name>* ist der Name der virtuellen Konsole, die Sie in Schritt 3 konfiguriert haben.

(Optional) Konfigurieren Sie eine statische IP-Adresse

Standardmäßig ist das ExtraHop-System mit aktiviertem DHCP konfiguriert. Wenn Ihr Netzwerk DHCP nicht unterstützt, müssen Sie eine statische Adresse manuell konfigurieren.

1. Melden Sie sich beim KVM-Host an.
2. Führen Sie den folgenden Befehl aus, um über die virtuelle serielle Konsole eine Verbindung zum ExtraHop-System herzustellen:

   ```
   virsh console <vm_name>
   ```

   Wo *<vm_name>* ist der Name Ihrer virtuellen Maschine.
3. Drücken Sie zweimal die EINGABETASTE, um zur Systemanmeldeaufforderung zu gelangen.

   ```
   ExtraHop Discover Appliance Version 7.8.2.2116
   IP: 192.0.2.81
   ```

```
exampleium login:
```

4. Geben Sie an der Anmeldeaufforderung ein `Schale`, und drücken Sie dann die EINGABETASTE.
5. Geben Sie an der Passwortaufforderung Folgendes ein `Standard`, und drücken Sie dann die EINGABETASTE.
6. Führen Sie die folgenden Befehle aus, um die statische IP-Adresse zu konfigurieren:
   a) Aktiviere privilegierte Befehle:

   ```
   enable
   ```

   b) Geben Sie an der Passwortaufforderung Folgendes ein `Standard`, und drücken Sie dann die EINGABETASTE.
   c) Rufen Sie den Konfigurationsmodus auf:

   ```
   configure
   ```

   d) Rufen Sie den Schnittstellenkonfigurationsmodus auf:

   ```
   interface
   ```

   e) Starte den `ip` Befehl und spezifizieren Sie die IP-Adresse und DNS Einstellungen im folgenden Format:

   `ip ipaddr <ip_address> <netmask> <gateway> <dns_server>`

   Zum Beispiel:

   ```
   ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
   ```

   f) Verlassen Sie den Schnittstellenkonfigurationsmodus:

   ```
   exit
   ```

   g) Speichern Sie die laufende Konfigurationsdatei:

   ```
   running_config save
   ```

   h) Typ y und drücken Sie dann ENTER.

Maßnahmen nach dem Einsatz

Öffnen Sie einen Webbrowser und geben Sie die IP-Adresse des ExtraHop-Systems in die Adressleiste ein und drücken Sie dann **EINGEBEN**. Akzeptieren Sie die EULA und geben Sie den Produktschlüssel ein , um die Konsole zu lizenzieren.

Loggen Sie sich in das ExtraHop-System ein mit dem `setup` Benutzerkonto und Typ `default` für das Passwort.

- Überprüfen Sie die Checkliste für Sensor und Konsole nach der Bereitstellung und konfigurieren Sie zusätzliche Einstellungen.
- Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden
- Verbinde die Konsole und die Sensoren mit ExtraHop Recordstores
- Sensoren und Konsole mit dem Packetstore verbinden