Stellen Sie einen ExtraHop-Sensor auf Linux KVM bereit

Veröffentlicht: 2024-01-22

Das folgende Verfahren führt Sie durch den Bereitstellungsprozess des virtuellen ExtraHop EDA 1100v. Sensor auf einer Linux-Kernel-basierten virtuellen Maschine (KVM). Sie sollten mit der grundlegenden KVM-Verwaltung vertraut sein, bevor Sie fortfahren.

Falls Sie dies noch nicht getan haben, laden Sie den virtuellen ExtraHop herunter Sensor Datei für KVM aus dem 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 an virtuelle Maschinen

Ihr KVM-Hypervisor muss in der Lage sein, die folgenden Spezifikationen für den virtuellen Sensor.

Fühler	vCPU	RAM	Festplatte
Reveal (x) EDA 1100v	2	4 GB	• 4-GB-Startdiskette (Virtio-SCSI-Schnittstelle empfohlen) • 40-GB-Datenspeicherfestplatte • (Optional) Festplatte mit 250 GB oder weniger für Paketerfassung (Thick-Provisioning)

Die Hypervisor-CPU sollte Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Befehle unterstützen.

Hinweis: Wenn Sie Paketerfassungen aktivieren möchten, konfigurieren Sie während der Bereitstellung eine zusätzliche Speicherfestplatte. Informationen zum Hinzufügen einer Festplatte finden Sie in der Dokumentation Ihres Anbieters.

Inhalt des Pakets

Das Installationspaket für KVM-Systeme ist eine Datei tar.gz, die die folgenden Dateien enthält:

Beschreibung	Enthüllen (x) 1100 V
Domain-XML-Konfigurationsdatei	eda-1100v.xml
Domain−XML-Prüfsummendatei	eda-1100v.xml.md5
Startdiskette	extrahop-boot.qcow2
Prüfsummendatei für die Startdiskette	extrahop-boot.qcow2.md5
Datenspeicher-Festplatte	extrahop-data.qcow2

Beschreibung	Enthüllen (x) 1100 V
Prüfsummendatei für die Datastore-Festplatte	extrahop-data.qcow2.md5

Stellen Sie den virtuellen Sensor bereit

Um das virtuelle bereitzustellen Sensor, führen Sie die folgenden Verfahren durch:

- Ermitteln Sie die beste virtuelle Bridge-Konfiguration für Ihr Netzwerk
- Erstellen Sie eine virtuelle Capture-Bridge, die den Datenverkehr enthält, den Sie überwachen möchten
- Bearbeiten Sie die Domain-XML-Konfigurationsdatei
- Konfigurieren Sie eine Spiegelsitzung auf der virtuellen Bridge

Ermitteln Sie die beste Bridge-Konfiguration

Sammeln Sie Informationen über Ihr Netzwerk, um die beste virtuelle Bridge-Konfiguration zu ermitteln.

1. Identifizieren Sie die Quelle Ihrer wire data und die Art der Daten, die Sie erfassen möchten.
   - Erstellen Sie für SPAN, RSPAN oder Portspiegelung die virtuelle Capture Bridge mit Open vSwitch.
   - Wählen Sie für ERSPAN oder rpcapd entweder Open vSwitch oder die integrierte Linux-Bridge, um die virtuelle Capture-Bridge zu erstellen.
2. Stellen Sie fest, ob Sie Datenverkehr von einer externen Netzwerkquelle erfassen möchten. Falls ja, konfigurieren Sie eine physische Schnittstelle auf der virtuellen Capture Bridge.
3. Identifizieren Sie die Bridge, über die Sie auf die Verwaltungsschnittstelle zugreifen möchten.
   - Wir empfehlen, separate Bridges für die Capture Bridge und die Management Bridge zu konfigurieren.
   - • Die Management-Bridge muss für den virtuellen Sensor und für alle Benutzer zugänglich sein, die auf die Verwaltungsschnittstelle zugreifen müssen.
   - Wenn Sie von einem externen Computer aus auf die Verwaltungsschnittstelle zugreifen müssen, konfigurieren Sie eine physische Schnittstelle auf der Virtual Capture Bridge.

Erstellen Sie die virtuelle Capture Bridge

Bevor Sie die PCAP durch einen virtuellen ExtraHop aktivieren Sensor, müssen Sie eine virtuelle Brücke erstellen, die auf den Promiscuous-Modus eingestellt ist. Wenn Sie Datenverkehr von einem externen Netzwerk erfassen möchten, müssen Sie der Bridge eine physische Schnittstelle hinzufügen, und diese Schnittstelle muss ebenfalls auf den Promiscuous-Modus eingestellt sein.

Das folgende Verfahren beschreibt, wie Sie mit Open vSwitch eine virtuelle Bridge erstellen. Informationen zum Erstellen einer virtuellen Bridge mit der integrierten Linux-Bridge finden Sie in der Dokumentation zu Ihrem KVM-System.

1. Loggen Sie sich in das KVM-System ein.
2. Erstellen Sie eine virtuelle Brücke, indem Sie den folgenden Befehl ausführen:

```
sudo ovs-vsctl add-br <bridge_name>
```

Wo *<bridge_name>* ist der Name Ihrer virtuellen Brücke.

3. Versetzen Sie die virtuelle Brücke in den Promiscuous-Modus, indem Sie den folgenden Befehl ausführen:

```
sudo ifconfig <bridge_name> promisc
```

Wo *<bridge_name>* ist der Name Ihrer virtuellen Brücke.

4. Wenn Sie auf den Verkehr in einem externen Netzwerk zugreifen möchten, fügen Sie der Bridge eine physische Schnittstelle hinzu, indem Sie den folgenden Befehl ausführen:

```
sudo ovs-vsctl add-port <bridge_name>
            <port_name>
```

Wo *<bridge_name>* ist der Name deiner virtuellen Brücke und *<port_name>* ist der Name des Ports, den Sie der Bridge hinzufügen möchten.

5. Wenn Sie der Bridge eine physische Schnittstelle hinzugefügt haben, versetzen Sie diese Schnittstelle in den Promiscuous-Modus, indem Sie den folgenden Befehl ausführen:

```
sudo ifconfig <port_name> promisc
```

Wo *<port_name>* ist der Name des Hafens.

Hinweis: Wenn Sie möchten, dass die Änderungen an der Benutzeroberfläche nach einem Neustart bestehen bleiben, fügen Sie die ifconfig-Befehle zu Ihrem `/etc/network/interfaces` datei.

Bearbeiten Sie die Domain-XML-Konfigurationsdatei

Nachdem Sie Ihre virtuelle Bridge erstellt haben, bearbeiten Sie die Konfigurationsdatei und erstellen Sie den virtuellen ExtraHop-Sensor.

1. Extrahieren Sie die Datei tar.gz, 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 XML-Konfigurationsdatei der Domain. Suchen und bearbeiten Sie die folgenden Werte:
   a) Ändern Sie den VM-Namen (ExtraHop-EDA-1100V) in den Namen, den Sie für Ihren virtuellen ExtraHop-Sensor festlegen möchten.

```
<name>ExtraHop-EDA-1100v</name>
```

   b) Ändern Sie den Quelldateipfad (*[PFAD_ZUM_SPEICHER]*) an den Ort, 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'/>
```

   c) Ändern Sie die Quellbrücke für Ihr Capture-Netzwerk (mirrorbr0) so, dass sie dem Namen Ihrer Capture-Bridge entspricht.

```
<interface type='bridge'>
<source bridge='mirrorbr0'/>
<virtualport type='openvswitch'>
</virtualport>
<model type='virtio'/>
<alias name='net1'/>
<address type='pci' domain='0x0000' bus='0x00' slot='0x06'
 function='0x0'/>
```

```
</interface>
```

Hinweis: Wenn Sie die integrierte Linux-Bridge konfigurieren, entfernen Sie die `virtualport type` Einstellung.

d) Ändern Sie die Quellbrücke für das Verwaltungsnetzwerk (ovsbr0) so, dass sie dem Namen Ihrer Management-Bridge entspricht.

```
<interface type='bridge'>
    <source bridge='ovsbr0'/>
    <virtualport type='openvswitch'>
    </virtualport>
    <model type='virtio'/>
    <alias name='net0'/>
    <address type='pci' domain='0x0000' bus='0x00' slot='0x03'
 function='0x0'/>
</interface>
```

Hinweis: Wenn Sie die integrierte Linux-Bridge konfigurieren, entfernen Sie die `virtualport type` Einstellung.

4. Speichern Sie die XML-Datei.
5. Melden Sie sich bei der KVM-Konsole an.
6. Erstellen Sie den neuen virtuellen ExtraHop-Sensor mit Ihrer überarbeiteten Domain-XML-Konfigurationsdatei, indem Sie den folgenden Befehl ausführen:

   ```
   virsh define <domain_XML_file>
   ```

   Wo *<domain_XML_file>* ist der Name Ihrer Domain-XML-Konfigurationsdatei (`eda-1100v.xml`
7. Führen Sie den folgenden Befehl aus, um die VM zu starten:

   ```
   virsh start <vm_name>
   ```

   Wo *<vm_name>* ist der Name Ihrer VM.

Konfigurieren Sie eine Spiegelsitzung auf der Capture Bridge

In diesem Verfahren wird erklärt, wie eine Spiegelsitzung auf einer virtuellen Open vSwitch-Bridge konfiguriert wird.

Bevor Sie beginnen

Wichtig: Um die beste Leistung bei der ersten Gerätesynchronisierung zu gewährleisten, schließen Sie alle Sensoren an die Konsole an und konfigurieren Sie dann die Weiterleitung des Netzwerkverkehrs zu den Sensoren.

1. Melden Sie sich bei der KVM-Konsole an.
2. Exportieren Sie die Konfigurationsdatei für Ihren neuen virtuellen ExtraHop-Sensor, indem Sie den folgenden Befehl ausführen:

   ```
   sudo virsh dumpxml <vm_name>
   ```
3. Suchen Sie in der XML-Ausgabe nach dem Namen Ihrer Capture Bridge. Suchen Sie die Zeile, die den Zielentwickler für diese Brücke bezeichnet (`<target dev = 'virtual port name'>`). Notieren Sie sich den Namen des virtuellen Ports, der dem Zielentwickler zugewiesen wurde.
4. Fügen Sie der Bridge den virtuellen Port hinzu, indem Sie den folgenden Befehl ausführen:

   ```
   sudo ovs-vsctl add-port <bridge_name> <virtual_port_name>
   ```

Wo <*bridge_name*> ist der Name deiner Capture Bridge und <*virtual_port_name*> ist der Name des virtuellen Ports aus der Zielentwicklungseinstellung, die Sie in Schritt 3 notiert haben.

5. Versetzen Sie diesen virtuellen Port in den Promiscuous-Modus, indem Sie den folgenden Befehl ausführen:

```
sudo ifconfig <virtual_port_name> promisc
```

6. Gehen Sie wie folgt vor, um den Verkehr von einem externen Netzwerk aus zu überwachen, um einen Mirror auf der Bridge zu konfigurieren.
   a) Erstellen Sie den Port-Mirror auf der Capture Bridge, indem Sie den folgenden Befehl ausführen:

```
sudo ovs-vsctl -- --id=@m create mirror name=<your_mirror_name> -- add
 bridge <bridge_name> mirrors @m
```

   Wo <*your_mirror_name*> ist dein Wunschname für den Spiegel und <*bridge_name*> ist der Name deiner Capture Bridge.
   b) Fügen Sie dem Spiegel eine physische Schnittstelle hinzu, indem Sie den folgenden Befehl ausführen:

```
sudo ovs-vsctl -- --id=@<mirror_port_name> get port <mirror_port_name>
 -- set mirror <your_mirror_name> select_src_port=@<mirror_port_name>
 select_dst_port=@<mirror_port_name>
```

   Wo <*mirror_port_name*> ist der Name des Ports, den Sie spiegeln möchten und <your_mirror_name> ist der Name, den Sie in Schritt 6a angegeben haben.

   Hinweis: In diesem Beispiel wird der Port sowohl als Quellport (zum Erfassen von ausgehendem Verkehr) als auch als Zielport (zum Erfassen von eingehendem Verkehr) hinzugefügt. Wenn Sie den Verkehr auf dem Port nur in eine Richtung erfassen möchten, fügen Sie den Port nur als Quellport (select_src_port) oder als Zielport (select_dst_port) hinzu.

   Hinweis: Wenn Sie nur den internen Verkehr überwachen möchten, ersetzen Sie <*mirror_port_name*> mit dem Namen der Capture Bridge, die Sie überwachen möchten.

   c) Fügen Sie den Namen des virtuellen Ports (aus Schritt 3) als Ausgabeport für den Spiegel hinzu, indem Sie den folgenden Befehl ausführen:

```
sudo ovs-vsctl -- --id=@<virtual_port_name> get port
 <virtual_port_name> -- set mirror <your_mirror_name> output-
port=@<virtual_port_name>
```

Starten Sie die VM

Nachdem Sie Ihren virtuellen ExtraHop erstellt haben Sensor, Sie können sich über einen Webbrowser bei der Verwaltungsschnittstelle anmelden, um Ihren Lizenzschlüssel anzuwenden, den Netzwerkverkehr zu sehen und Ihre Sensor Konfigurationen.

1. Starten Sie die VM, indem Sie den folgenden Befehl ausführen:

   virsh start <vm_name>

   Wo <vm_name> ist der Name Ihres ExtraHop-Sensors.
2. Melden Sie sich bei der KVM-Konsole an und zeigen Sie die IP-Adresse Ihres neuen ExtraHop-Sensors an, indem Sie den folgenden Befehl ausführen:

```
sudo virsh console <vm_name>
```

(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.

Den Sensor konfigurieren

Nachdem Sie eine IP-Adresse für die konfiguriert haben Sensor, öffnen Sie einen Webbrowser und navigieren Sie über die konfigurierte IP-Adresse zum ExtraHop-System. Akzeptieren Sie die Lizenzvereinbarung und melden Sie sich an. Der Standard-Anmeldename ist `setup` und das Passwort ist `default`. Folgen Sie den Anweisungen, um den Produktschlüssel einzugeben, die Standard-Setup- und Shell-Benutzerkontokennwörter zu ändern, eine Verbindung zu ExtraHop Cloud Services herzustellen und eine Verbindung zu einer ExtraHop-Konsole herzustellen.

Nachdem das System lizenziert wurde und Sie sich vergewissert haben, dass Datenverkehr erkannt wurde, führen Sie die empfohlenen Verfahren in der Checkliste für die Zeit nach der Bereitstellung.