Stellen Sie einen ExtraHop-Recordstore auf Linux KVM bereit

Veröffentlicht: 2025-01-04

In diesem Handbuch erfahren Sie, wie Sie einen virtuellen ExtraHop-Recordstore auf einer Linux-Kernel-basierten virtuellen Maschine (KVM) bereitstellen und mehrere Recordstore verbinden, um einen Cluster zu erstellen. Sie sollten mit der grundlegenden KVM-Verwaltung vertraut sein, bevor Sie fortfahren.

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 das System

Ihre Umgebung muss die folgenden Anforderungen erfüllen, um einen virtuellen Recordstore bereitzustellen:

Wichtig: ExtraHop testet virtuelle Cluster auf lokalem Speicher auf optimale Leistung. ExtraHop empfiehlt dringend, virtuelle Cluster auf kontinuierlich verfügbaren Speichern mit niedriger Latenz bereitzustellen, z. B. auf einer lokalen Festplatte, einem Direct Attached Storage (DAS), einem Network Attached Storage (NAS) oder einem Storage Area Netzwerk (SAN).

- Eine KVM-Hypervisor-Umgebung, die den virtuellen Recordstore hosten kann. Der virtuelle Recordstore ist in den folgenden Konfigurationen verfügbar:

Nur Recordstore Manager-Node	5100 V, extra klein	5100v Klein	5100v Mittel	5100v Groß
4 CPUs	4 CPUs	8 CPUs	16 CPUs	32 CPUs
8 GB RAM	8 GB RAM	16 GB RAM	32 GB RAM	64 GB RAM
4 GB Bootdiskette	4-GB-Startdiskette	4-GB-Startdiskette	4-GB-Startdiskette	4-GB-Startdiskette
12 GB	250 GB oder kleinere Datenspeicherfestplatte	Datenspeicherfestplatte mit 500 GB oder weniger	Datenspeicherfestplatte mit 1 TB oder weniger	Datenspeicherfestplatte mit 2 TB oder weniger

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

Hinweis: Der Knoten nur für Recordstore Manager ist mit einer 12-GB-Datenspeicherfestplatte vorkonfiguriert. Sie müssen manuell ein zweites virtuelles Laufwerk für die anderen Recordstore-Konfigurationen konfigurieren, um Datensatzdaten zu speichern.

Wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter oder den technischen Support, um die für Ihre Anforderungen am besten geeignete Datenspeicher-Festplattengröße zu ermitteln.

Hinweis: Für KVM-Bereitstellungen wird die Virtio-SCSI-Schnittstelle für die Boot- und Datenspeicherfestplatten empfohlen.

- Ein virtueller Recordstore-Lizenzschlüssel.
- Die folgenden TCP-Ports müssen geöffnet sein:
  - TCP-Port 443: Ermöglicht den Browserzugriff auf die Administrationseinstellungen. Anfragen, die an Port 80 gesendet werden, werden automatisch an den HTTPS-Port 443 umgeleitet.

- TCP-Port 9443: Ermöglicht Recordstore-Knoten die Kommunikation mit anderen Knoten im selben Cluster.

Inhalt des Pakets

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

`EXA-5100v-<x>.xml`
: Die Domain-XML-Konfigurationsdatei

`EXA-5100v-<x>.xml.md5`
: Die Domain–XML–Prüfsummendatei

`extrahop-boot.qcow2`
: Die Bootdiskette

`extrahop-boot.qcow2.md5`
: Die Prüfsummendatei der Startdiskette

Stellen Sie den virtuellen Recordstore bereit

Gehen Sie wie folgt vor, um den virtuellen Recordstore bereitzustellen:

- Ermitteln Sie die beste virtuelle Bridge-Konfiguration für Ihr Netzwerk
- Bearbeiten Sie die Domain-XML-Konfigurationsdatei und erstellen Sie Ihre virtuelle Appliance
- Erstellen Sie die Datenspeicherfestplatte
- Starten Sie die VM
- Konfigurieren Sie die Explore-Appliance

Ermitteln Sie die beste Bridge-Konfiguration

Identifizieren Sie die Brücke, über die Sie auf die Verwaltungsschnittstelle Ihres Recordstore zugreifen.

1. Stellen Sie sicher, dass der virtuelle Recordstore und alle Benutzer, die auf die Verwaltungsschnittstelle zugreifen müssen, auf die Management Bridge zugreifen können.
2. Wenn Sie von einem externen Computer aus auf die Verwaltungsschnittstelle zugreifen müssen, konfigurieren Sie eine physische Schnittstelle auf der Management Bridge.

Bearbeiten Sie die Domain-XML-Konfigurationsdatei

Nachdem Sie die Management Bridge identifiziert haben, bearbeiten Sie die Konfigurationsdatei und erstellen Sie den virtuellen Recordstore.

1. Kontakt ExtraHop-Unterstützung um das Explore KVM-Paket zu erhalten und herunterzuladen.
2. Extrahieren Sie die Datei tar.gz, die das Installationspaket enthält.
3. Kopiere das `extrahop-boot.qcow2` Datei auf Ihr KVM-System.
4. Öffnen Sie die Domain-XML-Konfigurationsdatei in einem Texteditor und bearbeiten Sie die folgenden Werte:
   a) Ändern Sie den VM-Namen in einen Namen für Ihren virtuellen ExtraHop-Recordstore.
   Zum Beispiel:

```
<name>ExtraHop-EXA-S</name>
```

b) Ändern Sie den Quelldateipfad (`[PATH_TO_STORAGE]`) an den Ort, an dem Sie die virtuelle Festplattendatei in Schritt 3 gespeichert haben.

```
<source file='/images/extrahop-boot.qcow2'/>
```

c) Ändern Sie die Quellbrücke für das Verwaltungsnetzwerk (`ovsbr0`), um dem Namen Ihrer Management Bridge zu entsprechen.

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

d) Optional: Wenn Ihre virtuelle Bridge über die Open vSwitch Virtual Switch-Software konfiguriert ist, fügen Sie der Schnittstelle die folgende Einstellung für den virtuellen Porttyp hinzu (nach der Einstellung für die Quellbrücke):

```
<virtualport type='openvswitch'>
</virtualport>
```

5. Speichern Sie die XML-Datei.

Erstellen Sie die Datenspeicherfestplatte

Erstellen Sie die Datenspeicherfestplatte so, dass der zugewiesene Speicherplatz groß genug ist, um die Art von Datensätzen zu speichern, die Sie für die gewünschte Menge an Lookback speichern möchten.

Führen Sie den folgenden Befehl aus, um die Datenspeicherfestplatte zu erstellen:

```
qemu-img create -f qcow2 <path to storage location>
           <size>
```

Wo *<size>* ist die Größe der Festplatte in Gigabyte. In diesem Beispiel wird ein qcow2-Image mit einer maximalen Größe von 2 TB erstellt:

```
qemu-img create -f qcow2 /home/extrahop/extrahop-data.qcow2 2000G
```

Den Recordstore erstellen

Erstellen Sie den virtuellen Recordstore mit Ihrer überarbeiteten Domain-XML-Konfigurationsdatei, indem Sie den folgenden Befehl ausführen:

```
virsh define <EXA-5100v-<x>.xml>
```

Wo `<EXA-5100v-<x>.xml>` ist der Name Ihrer Domain-XML-Konfigurationsdatei.

Starten Sie die VM

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

```
virsh start <vm_name>
```

Wo *<vm_name>* ist der Name Ihres virtuellen ExtraHop-Recordstores, den Sie in Schritt 4 des Bearbeiten Sie die Domain−XML-Datei Abschnitt.

2. Melden Sie sich bei der KVM-Konsole an und zeigen Sie die IP-Adresse für Ihren neuen virtuellen ExtraHop-Recordstore an, indem Sie den folgenden Befehl ausführen:

```
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.

Konfiguriere den Recordstore

Nachdem Sie die IP-Adresse für den Recordstore erhalten haben, melden Sie sich bei den Administrationseinstellungen im Recordstore an über `https://<extrahop-hostname-or-IP-address>/admin` und führen Sie die folgenden empfohlenen Verfahren aus.

Hinweis: Der Standard-Login-Benutzername ist `setup`, und das Passwort ist `default`.

- Registrieren Sie Ihr ExtraHop-System
- Verbinden Sie den EXA 5200 mit dem ExtraHop-System
- Datensatzdaten an den Recordstore senden
- Überprüfen Sie die Recordstore-Checkliste nach der Bereitstellung und konfigurieren Sie zusätzliche Recordstore-Einstellungen.

Einen Recordstore-Cluster erstellen

Für die beste Leistung, Datenredundanz und Stabilität müssen Sie mindestens drei ExtraHop-Recordstores in einem Cluster konfigurieren.

Wenn Sie einen Recordstore-Cluster erstellen, stellen Sie sicher, dass Sie alle Knoten, einschließlich Manager-Knoten, am selben Standort oder Rechenzentrum bereitstellen. Weitere Informationen zu unterstützten Recordstore-Cluster-Konfigurationen finden Sie unter Richtlinien für Recordstore-Cluster.

Wichtig: Wenn Sie einen Recordstore-Cluster mit sechs bis neun Knoten erstellen, müssen Sie den Cluster mit mindestens drei Nur-Manager-Knoten konfigurieren. Weitere Informationen finden Sie unter Bereitstellung von Knoten nur für Manager.

Im folgenden Beispiel haben die Recordstores die folgenden IP-Adressen:

- Knoten 1:10.20.227.177
- Knoten 2:10.20.227.178
- Knoten 3:10.20.227.179

Sie verbinden die Knoten 2 und 3 mit Knoten 1, um den Recordstore-Cluster zu erstellen. Alle drei Knoten sind Datenknoten. Sie können keinen Datenknoten mit einem Manager-Knoten verbinden oder einen Manager-Knoten mit einem Datenknoten verbinden, um einen Cluster zu erstellen.

Wichtig: Jeder Knoten , dem Sie beitreten, muss dieselbe Konfiguration (physisch oder virtuell) und dieselbe ExtraHop-Firmware-Version haben.

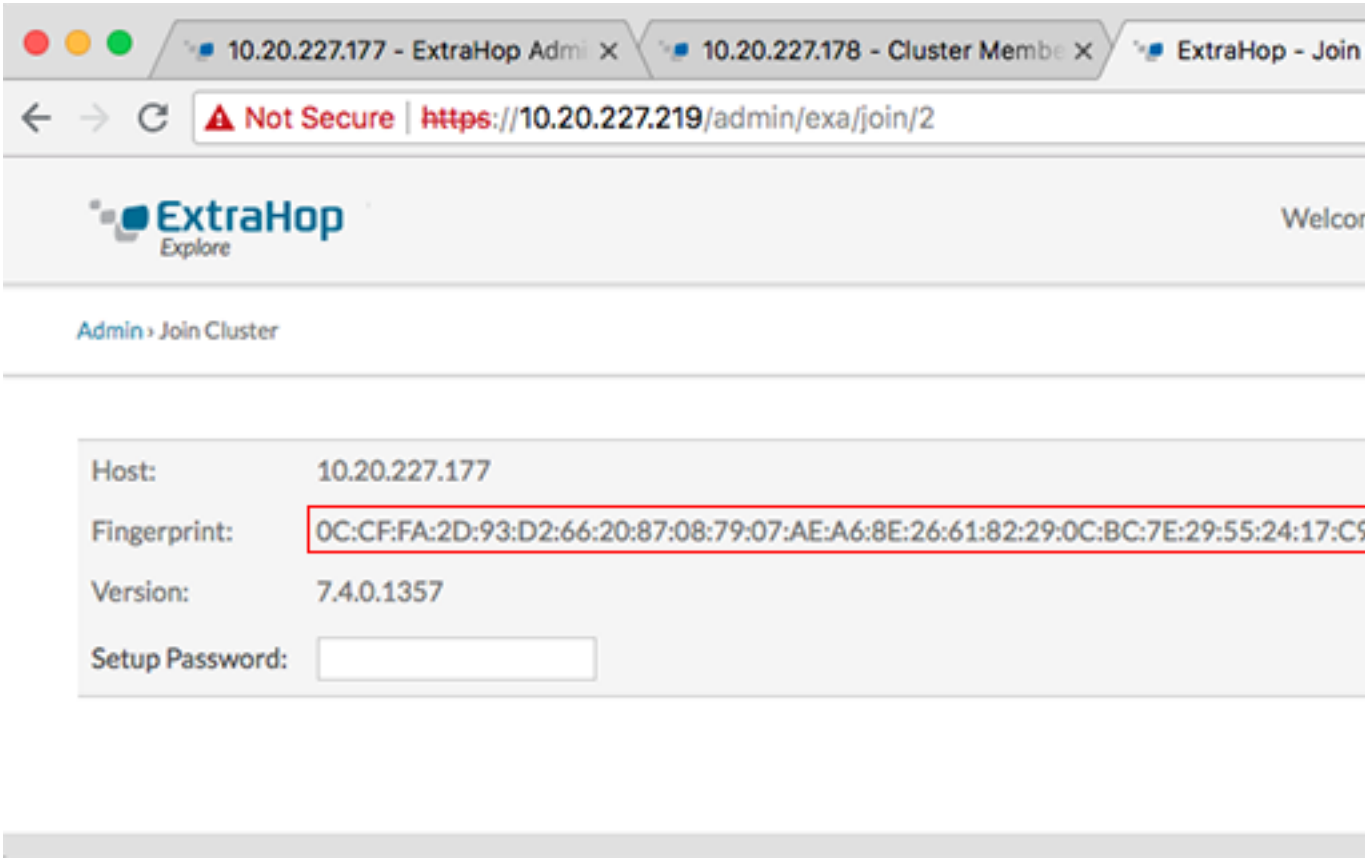
Bevor Sie beginnen
Sie müssen die Recordstores bereits in Ihrer Umgebung installiert oder bereitgestellt haben, bevor Sie fortfahren können.

1. Loggen Sie sich in die Administrationseinstellungen aller drei Recordstores ein mit dem `setup` Benutzerkonto in drei separaten Browserfenstern oder Tabs.
2. Wählen Sie das Browserfenster von Knoten 1 aus.
3. In der Status und Diagnose Abschnitt, klicken Sie **Fingerabdruck** und notieren Sie sich den Fingerabdruckwert.

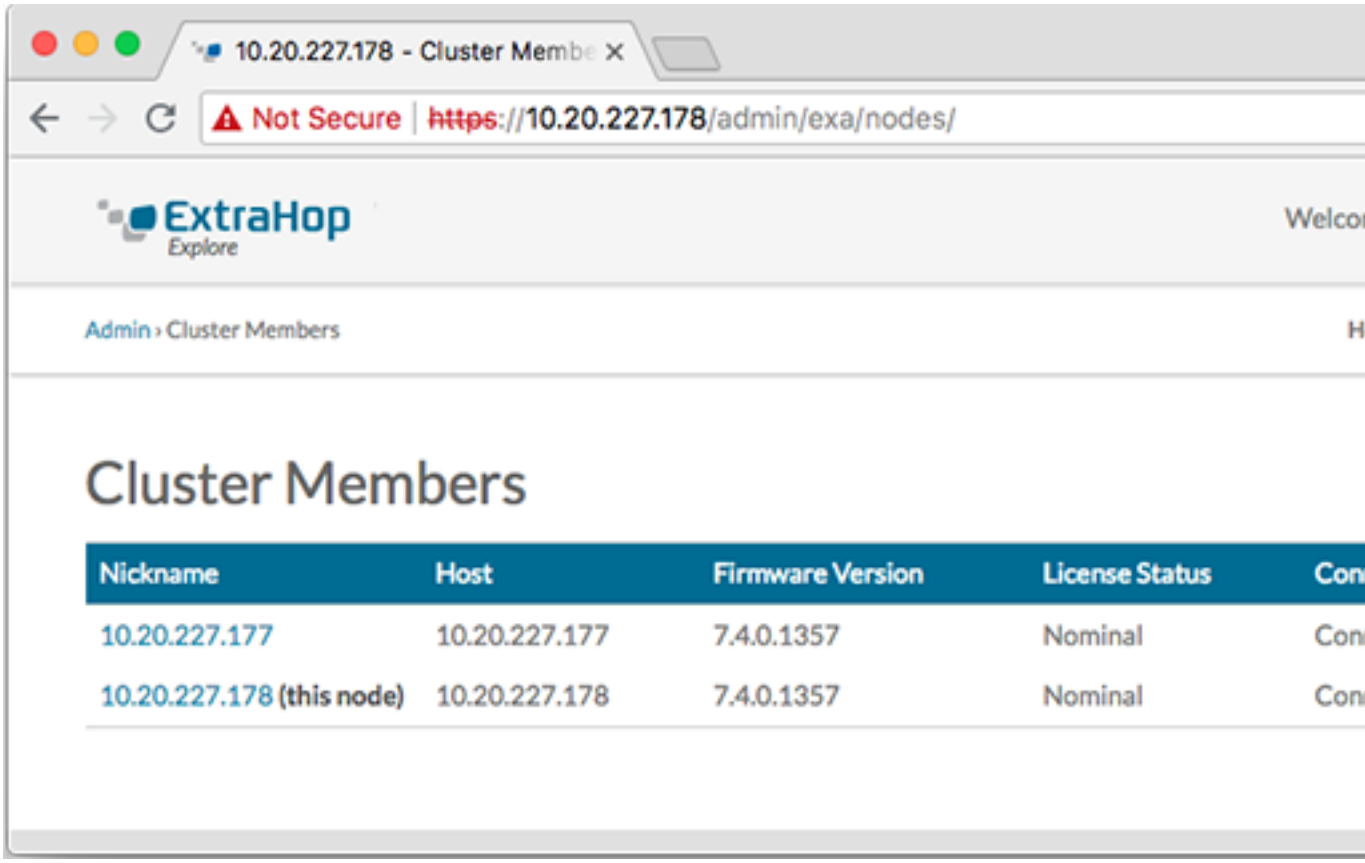
   Sie werden später bestätigen, dass der Fingerabdruck für Knoten 1 übereinstimmt, wenn Sie die verbleibenden zwei Knoten verbinden.

4. Wählen Sie das Browserfenster von Knoten 2 aus.
5. In der Recordstore-Cluster-Einstellungen Abschnitt, klicken Sie **Cluster beitreten**.
6. In der **Gastgeber** Feld, geben Sie den Hostnamen oder die IP-Adresse von Datenknoten 1 ein und klicken Sie dann auf **Fortfahren**.

   Hinweis: Geben Sie bei cloudbasierten Bereitstellungen unbedingt die IP-Adresse ein, die in der Schnittstellentabelle auf der Seite Konnektivität aufgeführt ist.
7. Vergewissern Sie sich, dass der Fingerabdruck auf dieser Seite mit dem Fingerabdruck übereinstimmt, den Sie in Schritt 3 notiert haben.



8. In der **Passwort einrichten** Feld, geben Sie das Passwort für den Knoten 1 ein `setup` Benutzerkonto und klicken Sie dann auf **Beitreten**.
   Wenn der Join abgeschlossen ist, wird Erkunden Sie die Cluster-Einstellungen Abschnitt hat zwei neue Einträge: **Cluster-Mitglieder** und **Cluster-Datenmanagement**.
9. Klicken Sie **Cluster-Mitglieder**.
   Sie sollten Knoten 1 und Knoten 2 in der Liste sehen.

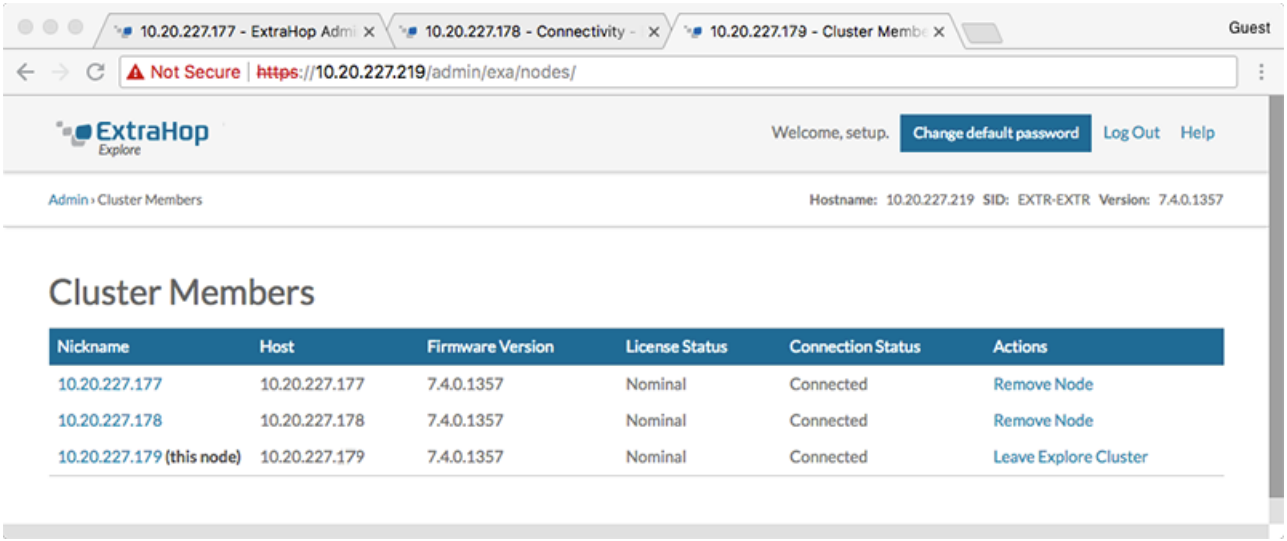


10. In der Status und Diagnose Abschnitt, klicken Sie **Erkunden Sie den Cluster-Status**.

    Warten Sie, bis das Statusfeld auf Grün wechselt, bevor Sie den nächsten Knoten hinzufügen.
11. Wiederholen Sie die Schritte 5 bis 10, um jeden weiteren Knoten mit dem neuen Cluster zu verbinden.

    Hinweis: Um zu vermeiden, dass mehrere Cluster erstellt werden, fügen Sie immer einen neuen Knoten einem vorhandenen Cluster und nicht einer anderen einzelnen Appliance hinzu.
12. Wenn Sie alle Ihre Recordstores zum Cluster hinzugefügt haben, klicken Sie auf **Cluster-Mitglieder** in der Erkunden Sie die Cluster-Einstellungen Abschnitt.

    Sie sollten alle verbundenen Knoten in der Liste sehen, ähnlich der folgenden Abbildung.



13. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken Sie **Cluster-Datenmanagement** und stellen Sie sicher, dass **Replikationsstufe** ist eingestellt auf **1** und **Neuzuweisung von Shards** ist **AUF**.

Nächste Schritte
Verbinden Sie den EXA 5200 mit dem ExtraHop-System.

Verbinden Sie den Recordstore mit einer Konsole und allen Sensoren

Nachdem Sie den Recordstore bereitgestellt haben, müssen Sie von der ExtraHop-Konsole aus eine Verbindung herstellen und alle Sensoren bevor Sie Datensätze abfragen können.

Wichtig: Verbinden Sie den Sensor mit jedem Recordstore-Knoten, sodass der Sensor die Arbeitslast auf den gesamten Recordstore-Cluster verteilen kann.

Hinweis: Wenn Sie alle Ihre Sensoren von einer Konsole aus verwalten, müssen Sie diesen Vorgang nur von der Konsole aus ausführen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der ExtraHop Recordstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Recordstore**.
3. Klicken Sie **Neues hinzufügen**.
4. Geben Sie im Abschnitt Node 1 den Hostnamen oder die IP-Adresse eines beliebigen Recordstore im Cluster ein.
5. Klicken Sie für jeden weiteren Knoten im Cluster auf **Neues hinzufügen** und geben Sie den individuellen Hostnamen oder die IP-Adresse für den Knoten ein.
6. Klicken Sie **Speichern**.
7. Vergewissern Sie sich, dass der Fingerabdruck auf dieser Seite mit dem Fingerabdruck von Knoten 1 des Recordstore-Clusters übereinstimmt.
8. In der Entdecke das Setup-Passwort Feld, geben Sie das Passwort für den Knoten 1 ein `setup` Benutzerkonto und klicken Sie dann auf **Verbinden**.
9. Wenn die Recordstore-Cluster-Einstellungen gespeichert sind, klicken Sie auf **Erledigt**.

Datensatzdaten an den Recordstore senden

Nachdem Ihr Recordstore mit Ihrem verbunden ist Konsole und Sensoren, Sie müssen die Art der Datensätze konfigurieren, die Sie speichern möchten.

siehe Aufzeichnungen für weitere Informationen zu Konfigurationseinstellungen, zum Generieren und Speichern von Datensätzen und zum Erstellen von Datensatzabfragen.