Stellen Sie die ExtraHop Explore Appliance mit VMware bereit

Veröffentlicht: 2024-02-12

In diesem Handbuch erfahren Sie, wie Sie die virtuelle ExtraHop Explore-Appliance bereitstellen, während der vSphere-Client auf einem Windows-Computer ausgeführt wird, und wie Sie mehrere Explore-Appliances verbinden, um einen Explore-Cluster zu erstellen. Sie sollten mit der Verwaltung von VMware ESX- und ESXi-Umgebungen vertraut sein, bevor Sie fortfahren.

Die virtuelle Explore-Appliance wird als OVA-Paket vertrieben, das eine vorkonfigurierte virtuelle Maschine (VM) mit einem Linux-basierten 64-Bit-Betriebssystem enthält, das für die Verwendung mit VMware ESX und ESXi Version 6.5 und höher optimiert ist.

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 eine virtuelle Explore-Appliance 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 bestehende Installation von VMware ESX oder ESXi Server Version 6.5 oder höher, die die virtuelle Explore-Appliance hosten kann. Die virtuelle Explore-Appliance ist in den folgenden Konfigurationen verfügbar:

Knoten nur für EXA Manager	EXA-XS	EXA-S	PRÜFUNG-M	EXA-L
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-Startdiskette	4-GB-Startdiskette	4-GB-Startdiskette	4-GB-Startdiskette	4-GB-Startdiskette
12 GB	250 GB oder kleinere Datenspeicherfestplatte	500 GB oder kleinere Datenspeicherfestplatte	1 TB oder kleinere Datenspeicherfestplatte	Datenspeicherfestplatte mit 2 TB oder kleiner

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

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

  Wenden Sie sich an Ihren ExtraHop-Vertriebsmitarbeiter oder den technischen Support, um die Festplattengröße des Datenspeichers zu ermitteln, die Ihren Anforderungen am besten entspricht.
- Ein vSphere-Client
- Ein Lizenzschlüssel für eine virtuelle Explore-Appliance.

- Die folgenden TCP-Ports müssen geöffnet sein:
  - TCP-Ports 80 und 443: Ermöglicht die Verwaltung der Explore-Appliance. Anfragen, die an Port 80 gesendet werden, werden automatisch an den HTTPS-Port 443 umgeleitet.
  - TCP-Port 9443: Ermöglicht Explore-Knoten die Kommunikation mit anderen Explore-Knoten im selben Cluster.

Stellen Sie die virtuelle Explore-Appliance bereit

Bevor Sie beginnen
Falls Sie dies noch nicht getan haben, laden Sie die OVA-Datei der virtuellen ExtraHop Explore-Appliance für VMware von der ExtraHop Kundenportal.

Hinweis: Wenn Sie die VM nach der Bereitstellung auf einen anderen Host migrieren müssen, fahren Sie zuerst die virtuelle Appliance herunter und migrieren Sie dann mit einem Tool wie VMware vMotion. Live-Migration wird nicht unterstützt.

1. Starten Sie den VMware vSphere-Client und stellen Sie eine Verbindung zu Ihrem ESX-Server her.
2. Gehe zum Datei Menü und wählen **OVF-Vorlage bereitstellen**.
3. Die Schritte zur Bereitstellung der OVF-Vorlage werden im Folgenden ausführlich beschrieben. Für die meisten Bereitstellungen sind die Standardeinstellungen ausreichend.
   a) Quelle: Navigieren Sie zum Speicherort der heruntergeladenen OVA-Datei und klicken Sie dann auf **Weiter**.
   b) Details zur OVF-Vorlage: Überprüfen Sie die Details und klicken Sie dann auf **Weiter**.
   c) Name und Standort: Konfigurieren Sie den Namen und den Speicherort der VM. Geben Sie der VM einen eindeutigen und spezifischen Namen für das ESX-Inventar und klicken Sie dann auf **Weiter**.
   d) Festplattenformat: Wählen **Thick Provision Lazy Zeroed** und dann klicken **Weiter**.
   e) Netzwerkkartierung: Ordnen Sie die OVF-konfigurierten Netzwerkschnittstellenbezeichnungen den richtigen ESX-konfigurierten Schnittstellenbezeichnungen zu und klicken Sie dann auf **Weiter**.
   f) Bereit zum Abschließen: Überprüfen Sie die Konfiguration, wählen Sie nicht Nach der Bereitstellung einschalten Checkbox, und klicken Sie dann auf **Fertig stellen** um die Bereitstellung abzuschließen.

   Wenn die Bereitstellung abgeschlossen ist, können Sie den eindeutigen Namen, den Sie der Explore-Appliance-VM-Instanz zugewiesen haben, in der Inventarstruktur für den ESX-Server sehen , auf dem sie bereitgestellt wurde.
4. Klicken Sie in der Verzeichnisstruktur auf die neue Explore-Appliance-VM-Instanz.
5. Aus dem Aktionen Drop-down-Liste, wählen **Einstellungen bearbeiten...** um die Festplatte zu konfigurieren, auf der die Explore-Appliance-Daten gespeichert sind.
6. Aus dem Neues Gerät Drop-down-Liste, wählen **Neue Festplatte**, bestätige das **Thick Provision Lazy Zeroed** ist ausgewählt für Festplattenbereitstellung und dann klicken **Hinzufügen**.
7. In der Neue Festplatte Feld, geben Sie die Größe Ihrer virtuellen Speicherfestplatte ein und klicken Sie dann auf **OK**.
8. Aus dem Aktionen Drop-down-Liste, wählen **Einschalten**.
9. Aus dem Aktionen Drop-down-Liste, wählen **Konsole öffnen**.
10. Loggen Sie sich ein mit dem `Schale` Benutzerkonto. Typ `Standard` für das Passwort.
11. Führen Sie den `ipaddr anzeigen` Befehl zum Anzeigen der IP-Adresse der virtuellen Explore-Appliance.
12. Verlassen Sie das Konsolenfenster.

Konfigurieren Sie eine statische IP-Adresse über die CLI

Das ExtraHop-System ist standardmäßig konfiguriert mit DHCP aktiviert. Wenn Ihr Netzwerk DHCP nicht unterstützt, wird keine IP-Adresse abgerufen, und Sie müssen eine statische Adresse manuell konfigurieren.

Wichtig: Wir empfehlen dringend Konfiguration eines eindeutigen Hostnamens. Wenn sich die System-IP-Adresse ändert, kann die ExtraHop-Konsole die Verbindung zum System einfach über den Hostnamen wiederherstellen.

1. Greifen Sie über eine SSH-Verbindung auf die CLI zu, indem Sie eine USB-Tastatur und einen SVGA-Monitor an die physische ExtraHop-Appliance anschließen, oder über ein serielles RS-232-Kabel (Nullmodem) und ein Terminalemulatorprogramm. Stellen Sie den Terminalemulator auf 115200 Baud mit 8 Datenbits, ohne Parität, 1 Stoppbit (8N1) und deaktivierter Hardware-Flusskontrolle ein.
2. Geben Sie in der Anmeldeaufforderung Folgendes ein `Schale` und drücken Sie dann ENTER.
3. Geben Sie an der Passwortaufforderung Folgendes ein `Standard`, und drücken Sie dann die EINGABETASTE.
4. 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 geben Sie die IP-Adresse und die DNS-Einstellungen im folgenden Format an:

   ```
   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 die EINGABETASTE.

Den Recordstore konfigurieren

Nachdem Sie die IP-Adresse für den Recordstore erhalten haben, melden Sie sich an `https://<explore_ip_address>/admin` und führen Sie die folgenden empfohlenen Verfahren durch.

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

- Registrieren Sie Ihr ExtraHop-System
- Verbinde die Konsole und die Sensoren mit ExtraHop Recordstores

- Senden Sie Datensatzdaten an die Explore-Appliance
- Überprüfen Sie die Erkunden Sie die Checkliste nach der Bereitstellung und konfigurieren Sie zusätzliche Recordstore-Einstellungen.

Erstellen Sie einen Recordstore-Cluster

Für optimale Leistung, Datenredundanz und Stabilität müssen Sie mindestens drei Extrahop-Recordstore in einem Cluster konfigurieren.

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

In diesem 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

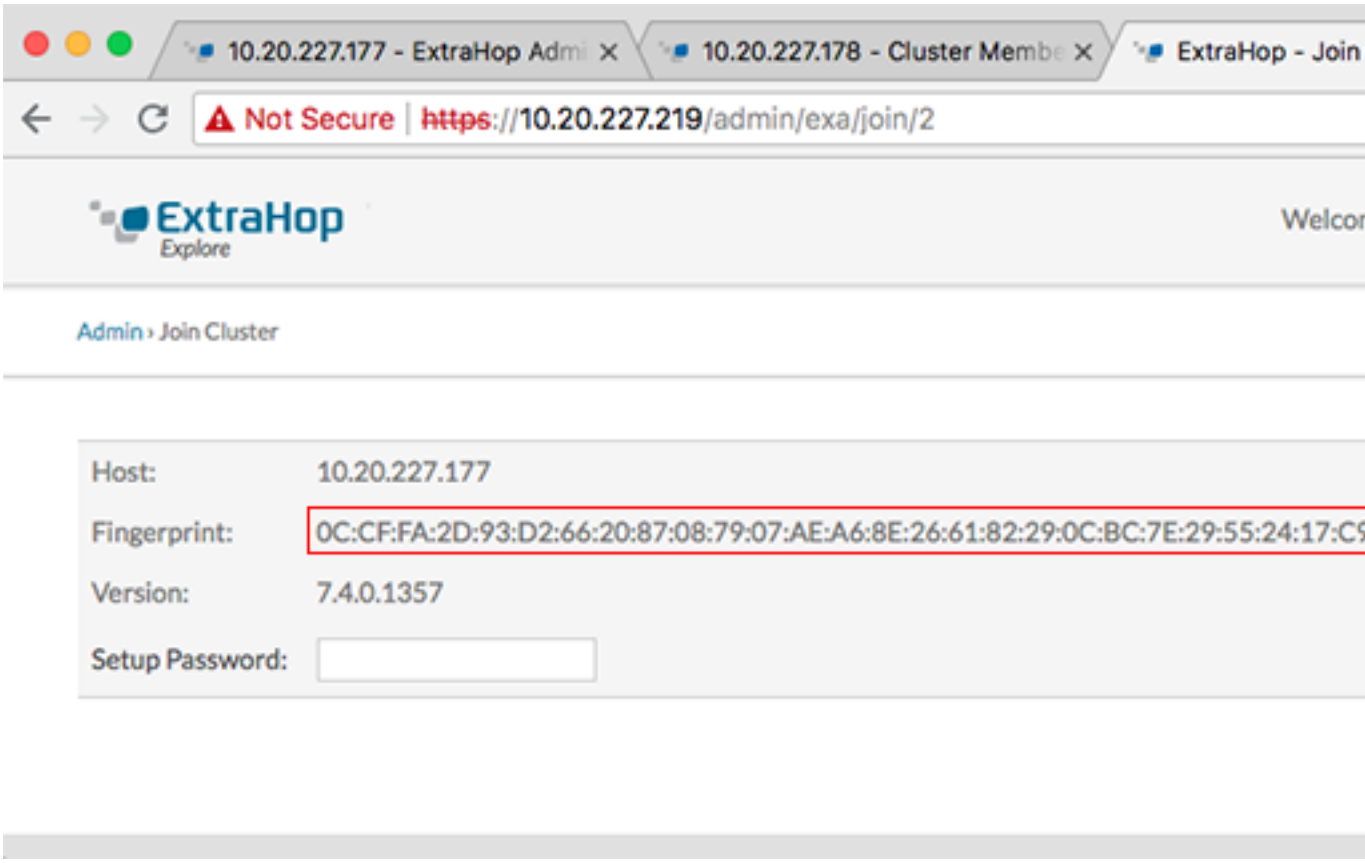
Sie verbinden die Knoten 2 und 3 mit Knoten 1, um den Recordstore-Cluster zu erstellen. Alle drei Knoten sind reine Datenknoten. Sie können einen reinen Datenknoten nicht mit einem Knoten verbinden, der nur für Manager bestimmt ist, oder einen Knoten, der nur für Manager bestimmt ist, mit einem Knoten verbinden, der nur Daten Knoten, um einen Cluster zu erstellen.

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

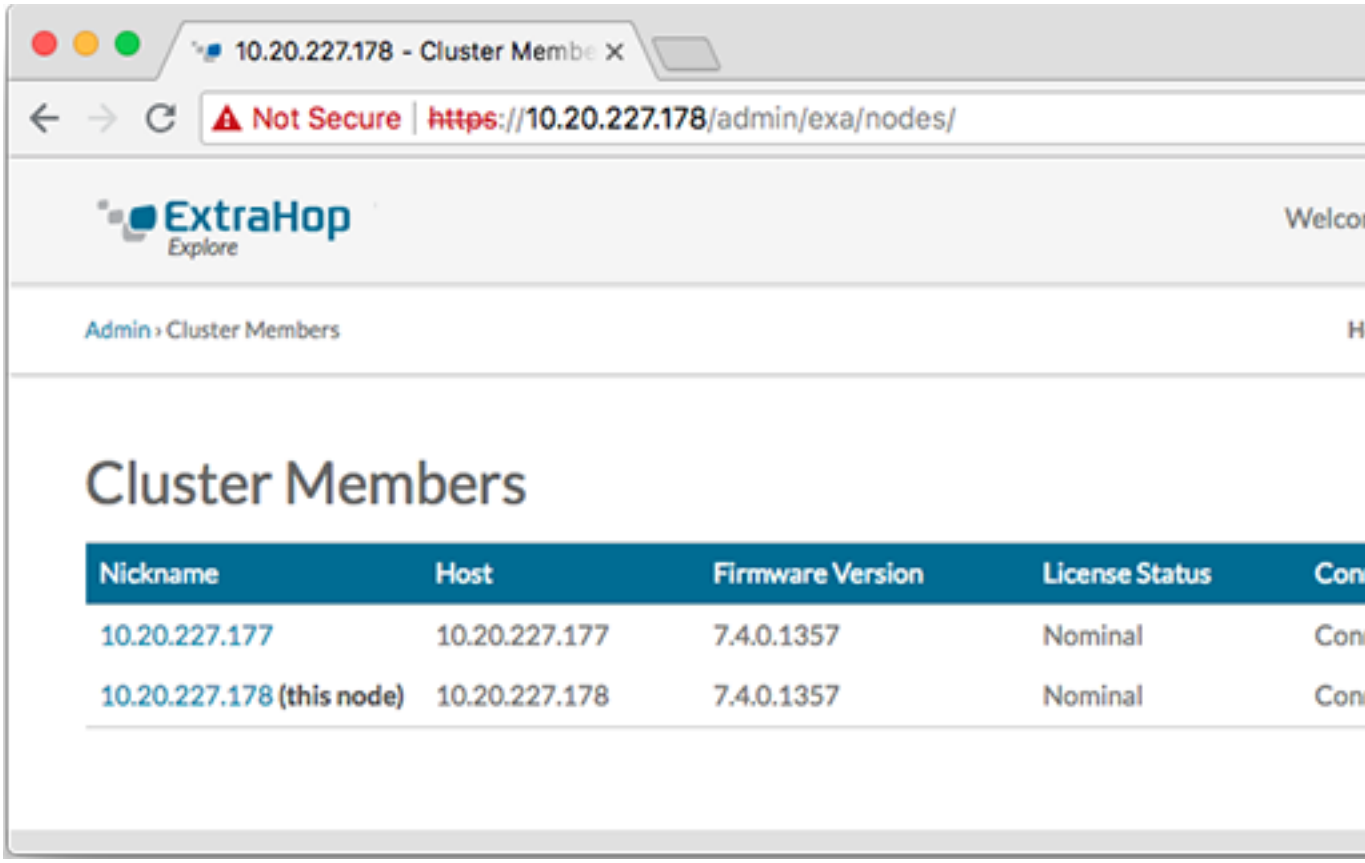
Bevor Sie beginnen
Sie müssen die Recordstores bereits in Ihrer Umgebung installiert oder bereitgestellt haben, bevor Sie fortfahren können.

1. Melden Sie sich mit dem Setup-Benutzerkonto in drei separaten Browserfenstern oder Tabs bei den Administrationseinstellungen aller drei Recordstores an.
2. Wählen Sie das Browserfenster von Knoten 1 aus.
3. In der Status und Diagnose Abschnitt, klicken **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 Cluster-Einstellungen erkunden Abschnitt, klicken **Cluster beitreten**.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse von Datenknoten 1 ein und klicken Sie dann auf **Weiter**.

   Hinweis: Geben Sie bei cloudbasierten Bereitstellungen unbedingt die IP-Adresse ein, die in der Tabelle Schnittstellen 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.



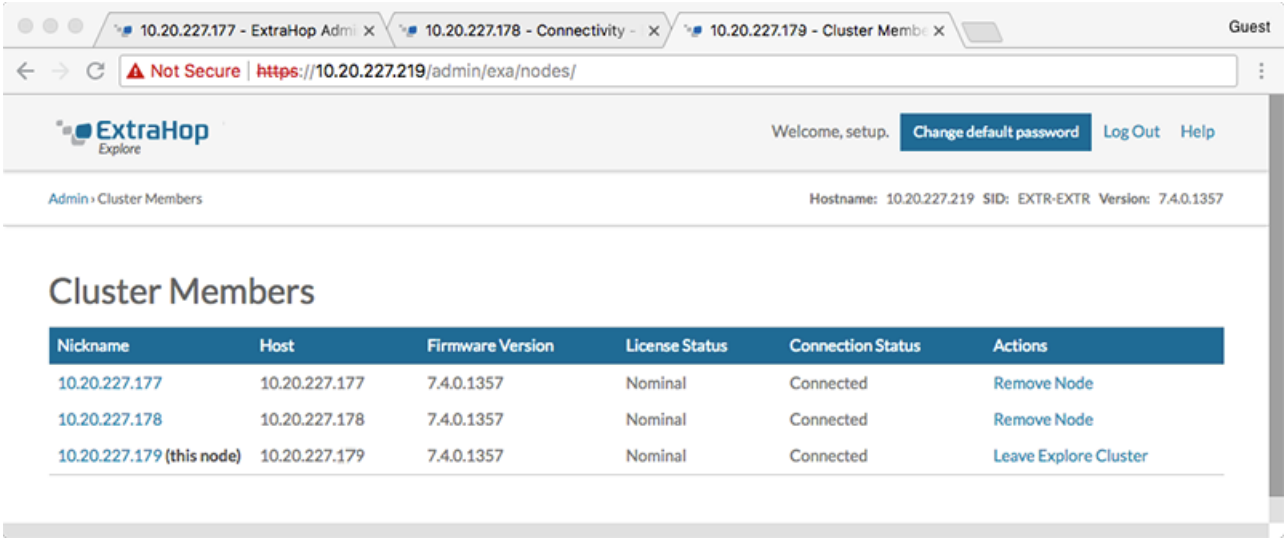
8. In der Passwort einrichten Feld, geben Sie das Passwort für den Knoten 1 ein `setup` Benutzerkonto und klicken Sie dann auf **Beitreten**.
   Wenn der Join abgeschlossen ist, Erkunden Sie die Cluster-Einstellungen Abschnitt hat zwei neue Einträge: **Cluster-Mitglieder** und **Cluster-Datenmanagement**.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



10. In der Status und Diagnose Abschnitt, klicken **Erkunden Sie den Cluster-Status**. Warte auf den Status Feld, in das geändert werden soll `Green` bevor der nächste Knoten hinzugefügt wird.
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, verbinden Sie einen neuen Knoten immer mit einem vorhandenen Cluster und nicht mit einer anderen einzelnen Appliance.

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 wie in der folgenden Abbildung.



13. In der Cluster-Einstellungen erkunden Abschnitt, klicken **Cluster-Datenmanagement** und vergewissere dich, dass **Replikationsebene** ist eingestellt auf **1** und **Neuzuweisung von Shards** ist **AUF**.

Nächste Schritte
Verbinde die Konsole und die Sensoren mit ExtraHop Recordstores

Verbinde den Recordstore mit einer Konsole und allen Sensoren

Nachdem Sie den Recordstore bereitgestellt haben, müssen Sie eine Verbindung von der Konsole und allen 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 dieses Verfahren 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 **Synchronisiere Recordstore**.
3. klicken **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 **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 **Verbinde**.
9. Wenn die Explore 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 Rekorde für weitere Informationen zu Konfigurationseinstellungen, zum Generieren und Speichern von Datensätzen und zum Erstellen von Datensatzabfragen.