

Stellen Sie den ExtraHop Recordstore mit VMware bereit

Veröffentlicht: 2024-09-25

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

Der virtuelle Recordstore wird als OVA-Paket verteilt, das eine vorkonfigurierte virtuelle Maschine (VM) mit einem Linux-basierten 64-Bit-Betriebssystem (OS) 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 einen virtuellen ExtraHop-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 vorhandene Installation von VMware ESX oder ESXi Server Version 6.5 oder höher, 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 Unterstützung für Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Befehle bereitstellen.

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.

- Ein vSphere-Client
- Ein virtueller Recordstore-Lizenzschlüssel.

- Die folgenden TCP-Ports müssen geöffnet sein:
 - TCP-Ports 80 und 443: Ermöglicht die Verwaltung des Recordstore. Anfragen, die an Port 80 gesendet werden, werden automatisch an den HTTPS-Port 443 umgeleitet.
 - TCP-Port 9443: Ermöglicht es Recordstore-Knoten, mit anderen Recordstore-Knoten im selben Cluster zu kommunizieren.

Stellen Sie einen virtuellen ExtraHop-Recordstore bereit

Bevor Sie beginnen

Falls Sie dies noch nicht getan haben, laden Sie die virtuelle ExtraHop Recordstore OVA-Datei für VMware von der [ExtraHop Kundenportal](#).



Hinweis Wenn Sie die virtuelle Maschine (VM) nach der Bereitstellung auf einen anderen Host migrieren müssen, fahren Sie zuerst den virtuellen Recordstore 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. Aus dem **Datei** Menü, wählen **OVF-Vorlage bereitstellen**.
3. Folgen Sie den Anweisungen des Assistenten für virtuelle Maschinen, um die OVF-Vorlage bereitzustellen:

Für die meisten Bereitstellungen sind die Standardeinstellungen ausreichend.

- a) Navigieren Sie zum Speicherort der heruntergeladenen OVA-Datei, wählen Sie die Datei aus, und klicken Sie dann auf **Weiter**.
- b) Überprüfen und verifizieren Sie die Details der OVF-Vorlage und klicken Sie auf **Weiter**.
- c) Geben Sie den Namen und den Speicherort der VM ein. Geben Sie der VM einen eindeutigen und spezifischen Namen für das ESX-Inventar und klicken Sie dann auf **Weiter**.
- d) Für Festplattenformat, wählen **Thick Provision Lazy Zeroed** und klicken Sie dann auf **Weiter**.
- e) Ordnen Sie die OVF-konfigurierten Netzwerkschnittstellenbezeichnungen den richtigen ESX-konfigurierten Schnittstellenbezeichnungen zu und klicken Sie dann auf **Weiter**.
- a) Überprüfen Sie die Konfiguration, wählen Sie nicht die **Nach dem Einsatz einschalten** Kontrollkästchen, und klicken Sie dann auf **Fertig** um die Bereitstellung abzuschließen.


Wenn die Bereitstellung abgeschlossen ist, können Sie den eindeutigen Namen, den Sie der Recordstore-VM-Instanz zugewiesen haben, im Inventarbaum des ESX-Servers sehen, auf dem sie bereitgestellt wurde.

4. Klicken Sie im Verzeichnisbaum auf die neue Recordstore-VM-Instanz.
5. Aus dem Aktionen Dropdownliste, wählen **Einstellungen bearbeiten...** um die Festplatte zu konfigurieren, auf der die Recordstore-Daten gespeichert werden.
6. Aus dem Neues Gerät Dropdownliste, wählen **Neue Festplatte**, bestätige das **Thick Provision Lazy Zeroed** ist ausgewählt für Festplattenbereitstellung, und klicken Sie dann auf **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 Dropdownliste, wählen **Einschalten**.
9. Aus dem Aktionen Dropdownliste, wählen **Konsole öffnen**.
10. Loggen Sie sich ein mit dem `schale` Benutzerkonto und das Passwort `Standard`.
11. Starte den `zeige ipaddr` Befehl zur Anzeige der IP-Adresse des virtuellen Recordstore.
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.

Sie können eine statische IP-Adresse für das ExtraHop-System manuell über die CLI 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 an der Anmeldeaufforderung ein `schale` und drücken Sie dann die EINGABETASTE.
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) 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 ENTER.

Konfigurieren Sie 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

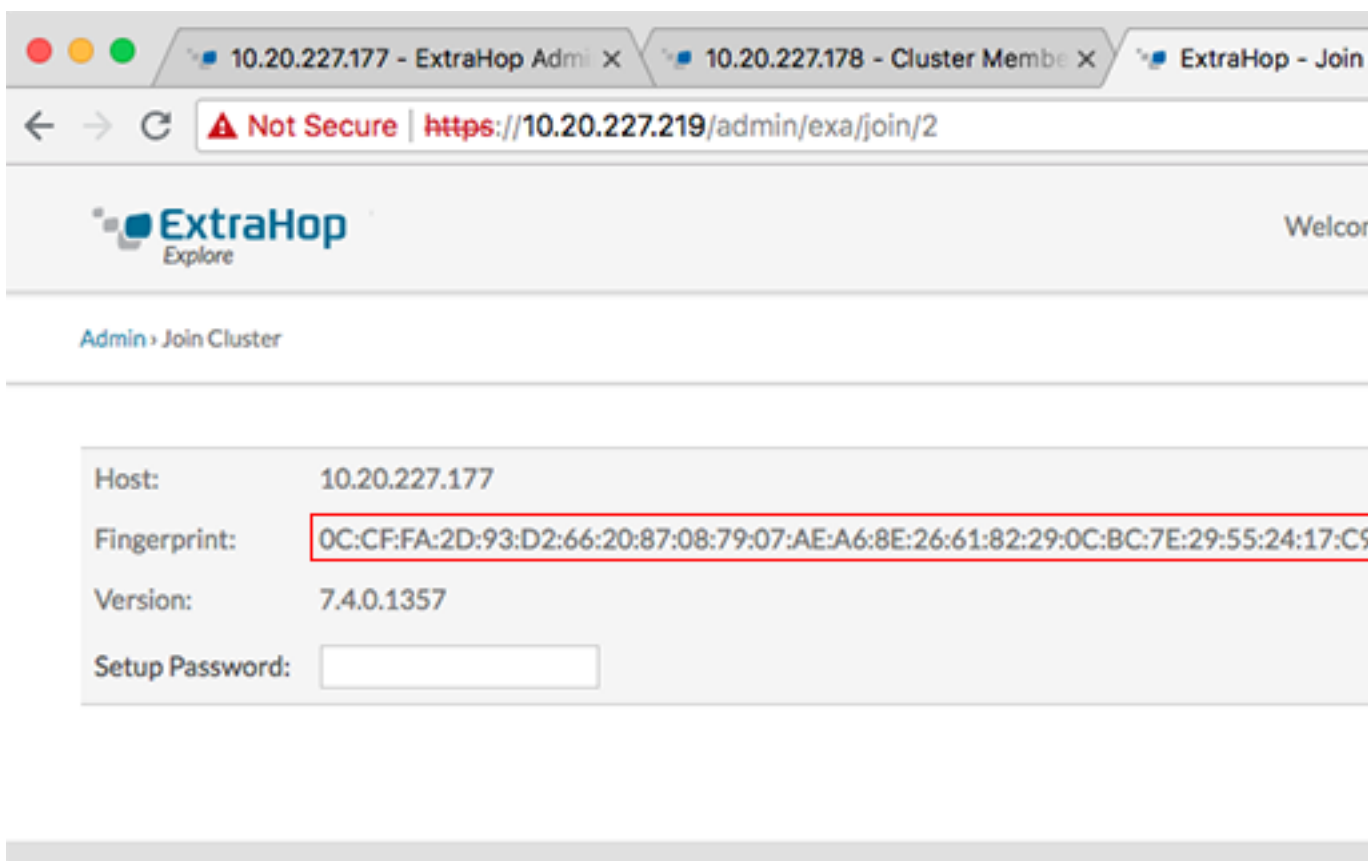
Sie müssen die Recordstores bereits in Ihrer Umgebung installiert oder bereitgestellt haben, bevor Sie fortfahren können.

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 **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 Erkunden Sie die 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 **Weiter**.



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.

10.20.227.178 - Cluster Membe X


Not Secure | https://10.20.227.178/admin/extra/nodes/

ExtraHop Explore

Admin > Cluster Members

Cluster Members

Nickname	Host	Firmware Version	License Status	Con
10.20.227.177	10.20.227.177	7.4.0.1357	Nominal	Con
10.20.227.178 (this node)	10.20.227.178	7.4.0.1357	Nominal	Con

- In der Status und Diagnose Abschnitt, klicken **Erkunden Sie den Cluster-Status**.
Warten Sie, bis das Statusfeld auf Grün wechselt, bevor Sie den nächsten Knoten hinzufügen.
- 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.
- 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.

10.20.227.177 - ExtraHop Admi X | 10.20.227.178 - Connectivity - X | 10.20.227.179 - Cluster Membe X

Not Secure | https://10.20.227.219/admin/extra/nodes/

ExtraHop Explore

Welcome, setup. [Change default password](#) [Log Out](#) [Help](#)

Admin > Cluster Members

Hostname: 10.20.227.219 SID: EXTR-EXTR Version: 7.4.0.1357

Cluster Members

Nickname	Host	Firmware Version	License Status	Connection Status	Actions
10.20.227.177	10.20.227.177	7.4.0.1357	Nominal	Connected	Remove Node
10.20.227.178	10.20.227.178	7.4.0.1357	Nominal	Connected	Remove Node
10.20.227.179 (this node)	10.20.227.179	7.4.0.1357	Nominal	Connected	Leave Explore Cluster


- In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken **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.