Stellen Sie einen ExtraHop Recordstore in AWS bereit

Veröffentlicht: 2024-09-25

In diesem Handbuch erfahren Sie, wie Sie das ExtraHop Recordstore AMI in Ihrer Amazon Web Services (AWS) -Umgebung starten und mehrere Recordstores verbinden, um einen Cluster zu erstellen.

Anforderungen an das System

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

- Ein AWS-Konto
- Zugriff auf das Amazon Machine Image (AMI) des ExtraHop Recordstore.
- Ein ExtraHop-Produktschlüssel
- Ein AWS-Instanztyp, der am ehesten dem entspricht Sensor VM-Größe wie folgt:

Plattenladen	Größe	Empfohlener Instanztyp
EXA 5100 v	Klein	m5.2xlarge (8 vCPU und 32 GB RAM)
	Mittel	m5.4xlarge (16 vCPU und 64 GB RAM)
	Groß	c5.9xlarge (36 vCPU und 72 GB RAM)

- Eine Datenspeichergröße zwischen 200 GB und 2 TB, abhängig vom ausgewählten Instance-Typ.

Instanztyp	Größe des Datenspeichers
m 5.2 x groß	Zwischen 200 GB und 500 GB
m 5,4 x groß	Zwischen 200 GB und 1 TB
c 5,9 x groß	Zwischen 200 GB und 2 TB

Erstellen Sie den Recordstore in AWS

Bevor Sie beginnen
Die Amazon Machine Images (AMIs) von ExtraHop-Recordstores werden nicht öffentlich geteilt. Bevor Sie mit dem Bereitstellungsverfahren beginnen können, müssen Sie Ihre AWS-Konto-ID an Ihren ExtraHop-Vertreter senden. Ihre Konto-ID wird mit den ExtraHop-AMIs verknüpft.

1. Melden Sie sich mit Ihrem Benutzernamen und Passwort bei AWS an.
2. klicken **EC2**.
3. Im linken Navigationsbereich, unter Bilder, klicken **AMIs**.
4. Ändern Sie über der AMI-Tabelle das **Filter** von **Gehört mir** zu **Private Bilder**.
5. Geben Sie in das Filterfeld ein `ExtraHop` und drücken Sie dann die EINGABETASTE.
6. Markieren Sie das Kontrollkästchen neben dem ExtraHop Recordstore AMI und klicken Sie auf **Starten**.
7. Auf dem Wählen Sie einen Instanztyp Seite, wählen Sie den Instance-Typ aus, der für Ihre Bereitstellung geeignet ist, und klicken Sie dann auf **Weiter: Instanzdetails konfigurieren**.

8. In der Anzahl der Instanzen Textfeld, geben Sie die Anzahl der Knoten in Ihrem Recordstore-Cluster ein.
9. Klicken Sie auf Netzwerk Dropdownliste und wählen Sie die Standardeinstellung oder eine der VPCs für Ihre Organisation aus.
10. Aus dem Verhalten beim Herunterfahren Dropdownliste, wählen **Stopp**.
11. Klicken Sie auf **Vor versehentlicher Kündigung schützen** Ankreuzfeld.
12. Optional: Aus dem IAM-Rolle Wählen Sie in der Dropdownliste eine IAM-Rolle aus.
13. Optional: Wenn Sie in eine VPC gestartet sind und mehr als eine Schnittstelle hinzufügen möchten, scrollen Sie nach unten zum Netzwerkschnittstellen Abschnitt und klick **Gerät hinzufügen** um der Instanz zusätzliche Schnittstellen hinzuzufügen.

    Hinweis: Wenn Sie mehr als eine Schnittstelle hinzufügen, stellen Sie sicher, dass sich jede Schnittstelle in einem anderen Subnetz befindet.

14. klicken **Weiter: Speicher hinzufügen**.

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

15. In der Größe (GiB) Feld für den Wurzel Volumen, geben Sie die Größe des Speichervolumens ein.

    Die Mindestgröße des Datenspeichers beträgt 186 GiB (200 GB).

16. Aus dem Datenträgertyp Drop-down-Menü, wählen Sie entweder **Magnetisch (Standard)** oder **Allzweck-SSD (gp2)**.

    Sie müssen wählen **Allzweck-SSD (gp2)** wenn Sie eine Größe von mehr als 1024 GiB angeben. GP2 bietet eine bessere Speicherleistung, allerdings zu höheren Kosten.

17. klicken **Weiter: Schlagworte hinzufügen**.
18. klicken **Tag hinzufügen**.
19. In der Schlüssel Feld, geben Sie einen Namen für das Tag ein.
20. In der Wert Feld, geben Sie einen Namen für die Instanz ein.
21. klicken **Weiter: Sicherheitsgruppe konfigurieren**.
22. Auf dem Sicherheitsgruppe konfigurieren Seite, erstellen Sie eine neue Sicherheitsgruppe oder fügen Sie Ports zu einer vorhandenen Gruppe hinzu.

    Wenn Sie bereits eine Sicherheitsgruppe mit den erforderlichen Ports für das ExtraHop-System haben, können Sie diesen Schritt überspringen.

    a) Wählen Sie entweder **Eine neue Sicherheitsgruppe erstellen** oder **Wählen Sie eine vorhandene Sicherheitsgruppe**.

       Wenn Sie eine bestehende Gruppe bearbeiten möchten, wählen Sie die Gruppe aus, die Sie bearbeiten möchten. Wenn Sie eine neue Gruppe erstellen möchten, geben Sie einen Namen für die Sicherheitsgruppe ein und geben Sie eine Beschreibung ein.

    b) Klicken Sie auf **Typ** Dropdownliste und wählen Sie ein Protokoll aus.

    c) Geben Sie die Portnummer in das **Port-Bereich** Feld.

    d) Für jeden weiteren benötigten Port klicken Sie auf **Regel hinzufügen**, und dann von der Typ Dropdownliste, wählen Sie ein Protokoll aus und geben Sie die Portnummer in das Port-Bereich Feld.

       Die folgenden Ports müssen für die Recordstore AWS-Instance geöffnet sein:

       - TCP-Port 443: Ermöglicht es Ihnen, den Recordstore von einem Webbrowser aus zu verwalten. Anfragen, die an Port 80 gesendet werden, werden automatisch an den HTTPS-Port 443 umgeleitet.
       - TCP-Port 9443: Ermöglicht es Recordstore-Knoten, innerhalb desselben Cluster zu kommunizieren.

23. klicken **Überprüfung und Markteinführung**.
24. Wählen **Allzweckmodell (SSD) herstellen... (empfohlen)** und klicken **Weiter**.

Hinweis: Wenn du auswählst **Allzweckmodell (SSD) herstellen... (empfohlen)**, Sie werden diesen Schritt bei nachfolgenden Instance-Starts nicht sehen.

25. Scrollen Sie nach unten, um die AMI-Details, den Instance-Typ und die Sicherheitsgruppeninformationen zu überprüfen, und klicken Sie dann auf **Starten**.
26. Klicken Sie im Popup-Fenster auf die erste Dropdownliste und wählen Sie **Fahren Sie ohne Schlüsselpaar fort**.
27. Klicken Sie auf **Ich erkenne an...** Ankreuzen und dann klicken **Instanz starten**.
28. klicken **Instanzen anzeigen** um zur AWS-Managementkonsole zurückzukehren.

    Von der AWS-Managementkonsole aus können Sie Ihre Instance auf der Initialisieren Bildschirm.

    Unter dem Tisch, auf dem **Beschreibung** Auf der Registerkarte finden Sie eine IP-Adresse oder einen Hostnamen für den Recordstore, auf den von Ihrer Umgebung aus zugegriffen werden kann.

Den Recordstore konfigurieren

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

- Registrieren Sie die Explore-Appliance
- Erstellen Sie einen Explore-Cluster
- Konfigurieren Sie die Systemzeit
- E-Mail-Benachrichtigungen konfigurieren
- Koppeln Sie die Explore-Appliance mit allen Discover- und Command-Appliances
- Senden Sie Datensatzdaten an die Explore-Appliance

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.

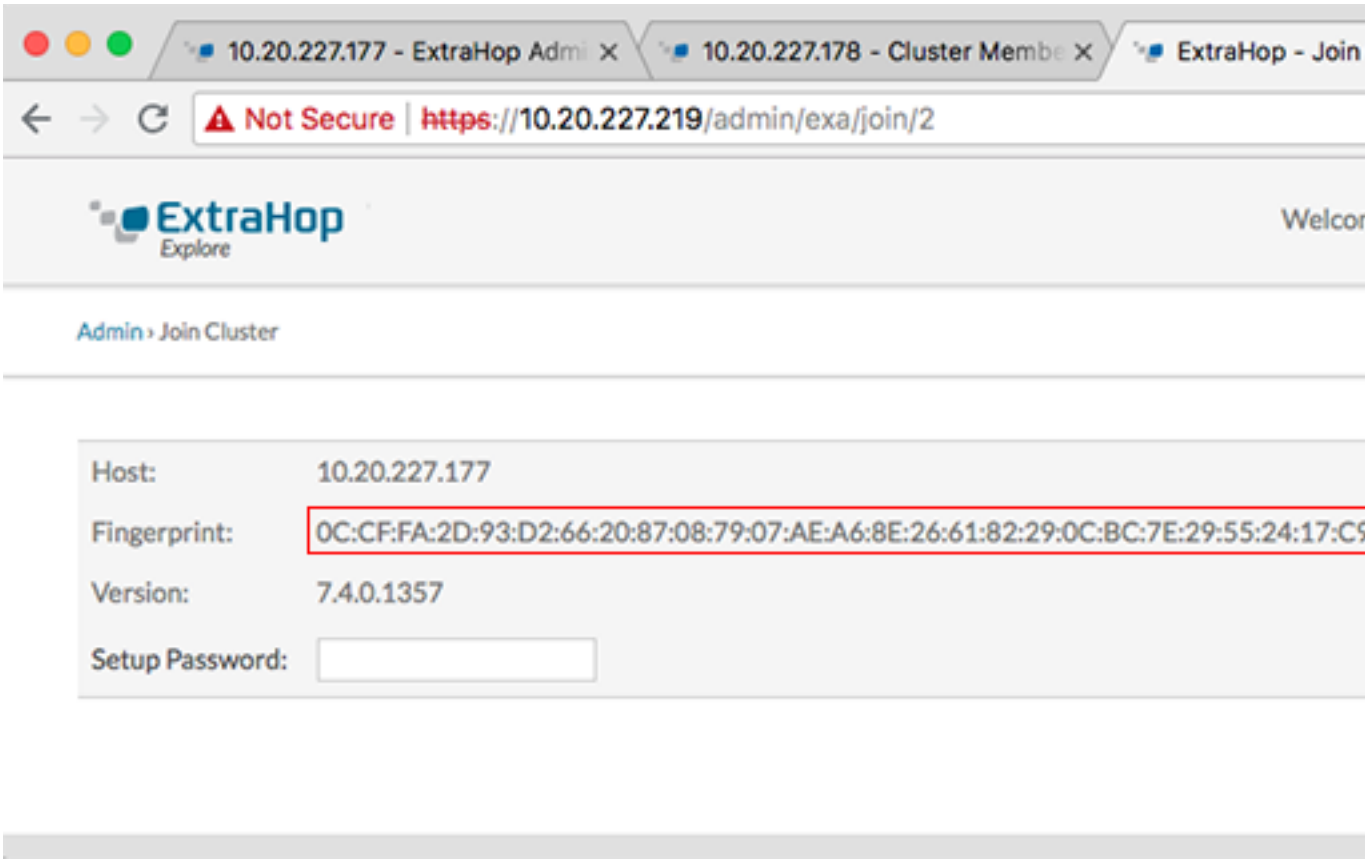
Wichtig: Jeder Knoten , dem Sie beitreten, muss dieselbe Konfiguration (physisch oder virtuell) und dieselbe ExtraHop-Firmware-Version haben.

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.

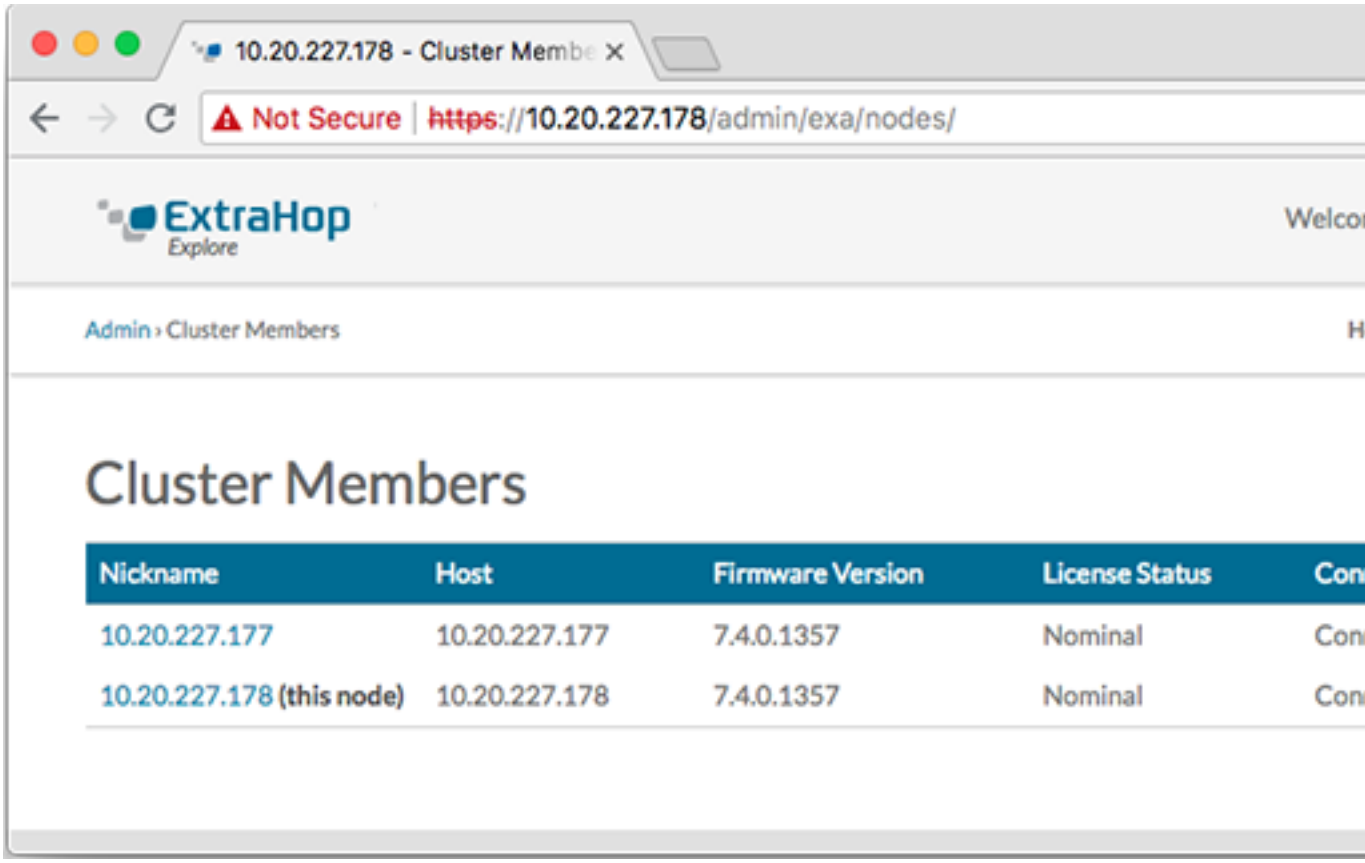
   Sie werden später bestätigen, dass der Fingerabdruck für Knoten 1 übereinstimmt, wenn Sie die verbleibenden zwei Knoten verbinden.
4. Wählen Sie das Browserfenster von Knoten 2 aus.
5. In der Erkunden Sie die Cluster-Einstellungen Abschnitt, klicken Sie **Cluster beitreten**.
6. In der **Gastgeber** 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.

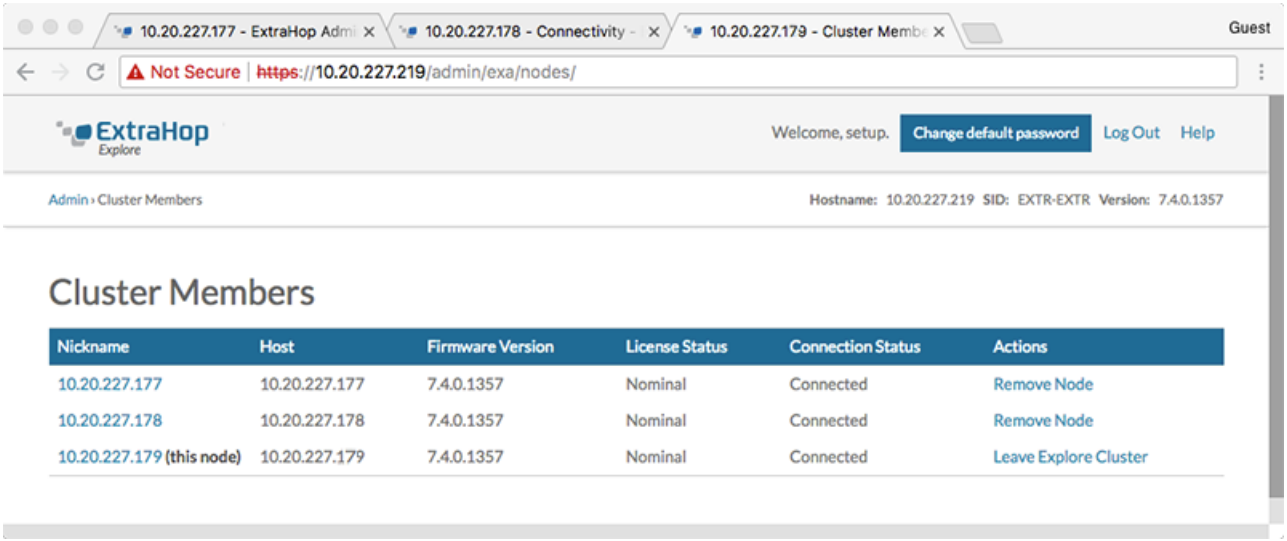


10. In der Status und Diagnose Abschnitt, klicken **Erkunden Sie den Cluster-Status**.

    Warten Sie, bis das Statusfeld auf Grün wechselt, bevor Sie den nächsten Knoten hinzufügen.
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 **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.

E-Mail-Benachrichtigungen konfigurieren

Sie müssen einen E-Mail-Server und einen Absender konfigurieren, bevor der Recordstore Benachrichtigungen über das System senden kann Warnungen per E-Mail.

Sie können die folgenden Benachrichtigungen vom System erhalten:

- Ein virtuelles Laufwerk befindet sich in einem heruntergestuften Zustand.
- Eine physische Festplatte befindet sich in einem heruntergekommenen Zustand.
- Eine physische Festplatte weist eine steigende Anzahl von Fehlern auf.
- Ein registrierter Recordstore-Knoten fehlt im Cluster. Der Knoten ist möglicherweise ausgefallen oder er ist ausgeschaltet.

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.