ExtraHop 9.9
Leitfaden für die Admin-Benutzeroberfläche

Weitere Informationen finden Sie unter https://docs.extrahop.com.

Veröffentlicht: 2025-01-04

ExtraHop Networks
Seattle, WA 98101
877-333-9872 (US)
+44 (0)203 7016850 (EMEA)
+65-31585513 (APAC)
www.extrahop.com

Inhaltsübersicht

Einführung in die ExtraHop Admin-Benutzeroberfläche

Der Admin-UI-Leitfaden enthält detaillierte Informationen zu den Administratorfunktionen und -funktionen von ExtraHop. Sensoren und Konsolen. Dieses Handbuch bietet einen Überblick über die globale Navigation und Informationen zu den Steuerelementen, Feldern und Optionen, die in der gesamten Benutzeroberfläche verfügbar sind.

Nachdem Sie Ihre bereitgestellt haben Sensor oder Konsole, siehe Checkliste für Sensor und Konsole nach der Bereitstellung.

Video: Sehen Sie sich die entsprechende Schulung an: RevealX Enterprise Administrationsoberfläche

Wir schätzen Ihr Feedback. Bitte teilen Sie uns mit, wie wir dieses Dokument verbessern können. Senden Sie Ihre Kommentare oder Vorschläge an documentation@extrahop.com.

Unterstützte Browser

Die folgenden Browser sind mit allen ExtraHop-Systemen kompatibel. Wenden Sie die von Ihrem Browser bereitgestellten Barrierefreiheits- und Kompatibilitätsfunktionen an, um über technische Hilfsmittel auf Inhalte zuzugreifen.

- Firefox
- Google Chrome
- Microsoft Edge
- Safari

Wichtig: Internet Explorer 11 wird nicht mehr unterstützt. Wir empfehlen Ihnen, die neueste Version aller unterstützten Browser zu installieren.

Status und Diagnose

Das Status und Diagnose Der Abschnitt enthält Kennzahlen zum allgemeinen Zustand Ihres ExtraHop-Systems.

Gesundheit

Das Gesundheit Diese Seite bietet eine Sammlung von Metriken, die Ihnen helfen, den Betrieb Ihres ExtraHop-Systems zu überwachen, und ermöglicht es dem ExtraHop-Support, bei Bedarf Systemfehler zu beheben.

System

Meldet die folgenden Informationen zur CPU-Auslastung und zur Festplatte des Systems.

CPU-Benutzer

Der Prozentsatz der CPU-Auslastung, der dem ExtraHop-Systembenutzer zugeordnet ist.

CPU-System

Der Prozentsatz der CPU-Auslastung im Zusammenhang mit dem ExtraHop-System.

CPU im Leerlauf

Der Prozentsatz der CPU-Leerlaufzeit, der dem ExtraHop-System zugeordnet ist.

CPU-IO

Der Prozentsatz der CPU-Auslastung, der mit den I/O-Funktionen des ExtraHop-Systems verbunden ist.

Status der Brücke

Meldet die folgenden Informationen über die ExtraHop-System-Bridge-Komponente.

VM RSS

Der verwendete physische Speicher des Bridge-Prozesses.

VM-Daten

Der Bridge-Prozess speichert virtuellen Speicher, der gerade verwendet wird.

VM-Größe

Der Bridge-Prozess verarbeitet den gesamten verwendeten virtuellen Speicher.

Startzeit

Gibt die Startzeit für die ExtraHop-System-Bridge-Komponente an.

Status erfassen

Meldet die folgenden Informationen zum Netzwerkaufzeichnungsstatus des ExtraHop-Systems.

VM RSS

Der verwendete physische Speicher des Netzwerkaufzeichnungsprozesses.

VM-Daten

Der Netzwerkaufzeichnungsprozess heapt den verwendeten virtuellen Speicher.

VM-Größe

Der gesamte verwendete virtuelle Speicher des Netzwerkaufzeichnungsprozesses.

Startzeit

Die Startzeit für die ExtraHop-Netzwerkerfassung.

Status des Dienstes

Meldet den Status der ExtraHop-Systemdienste.

Exalarme
Die Zeitdauer, in der der ExtraHop-Systemwarnungsdienst ausgeführt wurde.

ausdehnen
Die Zeitdauer, in der der ExtraHop-Systemtrend-Service ausgeführt wurde.

exconfig
Die Zeit, in der der ExtraHop-Systemkonfigurationsdienst ausgeführt wurde.

exportale
Die Zeit, in der der Webportaldienst des ExtraHop-Systems ausgeführt wurde.

Exshell
Die Zeitdauer, in der der ExtraHop-System-Shell-Service ausgeführt wurde.

Schnittstellen
Meldet den Status der ExtraHop-Systemschnittstellen.

RX-Pakete
Die Anzahl der Pakete, die von der angegebenen Schnittstelle empfangen wurden das ExtraHop-System.

RX-Fehler
Die Anzahl der empfangenen Paketfehler auf dem angegebenen Schnittstelle.

RX Drops
Die Anzahl der empfangenen Pakete, die durch den angegebenen Wert gelöscht wurden Schnittstelle.

TX-Pakete
Die Anzahl der Pakete, die von der angegebenen Schnittstelle übertragen werden auf dem ExtraHop-System.

TX-Fehler
Die Anzahl der übertragenen Paketfehler auf dem angegebenen Schnittstelle.

TX Drops
Die Anzahl der übertragenen Pakete, die durch den angegebenen Wert gelöscht wurden Schnittstelle.

RX-Bytes
Die Anzahl der Byte, die von der angegebenen Schnittstelle auf dem ExtraHop-System.

TX-Bytes
Die Anzahl der Byte, die von der angegebenen Schnittstelle übertragen werden das ExtraHop-System.

Partitionen
Meldet den Speicher, der Systemkomponenten für das ExtraHop-System zugewiesen wurde.

Name
Die Systemkomponenten, die eine Speicherpartition im NVRAM haben.

Optionen
Die Lese- und Schreiboptionen für die Systemkomponenten.

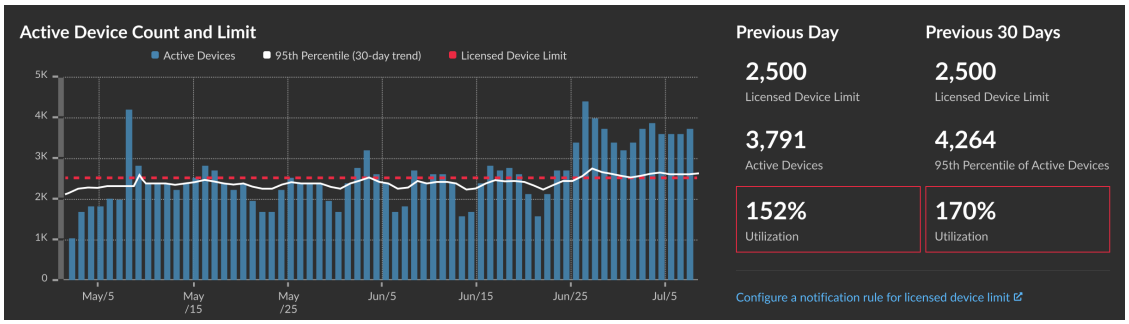
Größe
Die Partitionsgröße in Gigabyte, die der Systemkomponente zugewiesen ist.

Auslastung
Die Menge an Arbeitsspeicher, die derzeit von den Systemkomponenten verbraucht wird, als Menge und als Prozentsatz der gesamten Partition.

Anzahl und Limit der aktiven Gerät

Anhand des Diagramms Anzahl und Limit der aktiven Gerät können Sie überwachen, ob die Anzahl Ihrer aktiven Geräte das lizenzierte Limit überschritten hat. Beispielsweise sind für ein ExtraHop-System mit einem Frequenzband von 20.000 bis 50.000 Geräten bis zu 50.000 Geräte zulässig.

Klicken Sie **Systemeinstellungen** ⚙ und klicken Sie dann **Die gesamte Verwaltung**. Aus dem Status und Diagnose Abschnitt, klicken Sie **Anzahl und Limit der aktiven Geräte** um das Diagramm anzusehen.



Das Diagramm „Anzahl und Limit aktiver Geräte“ zeigt die folgenden Metriken an:

- Die gestrichelte rote Linie steht für Limit für lizenzierte Gerät.
- Die durchgezogene schwarze Linie steht für das 95. Perzentil der aktiven Geräte, die in den letzten 30 Tagen täglich beobachtet wurden.
- Die blauen Balken stellen die maximale Anzahl aktiver Geräte dar, die in den letzten 30 Tagen täglich beobachtet wurden.

Auf dieser Seite werden auch die folgenden Metriken angezeigt:

- Das lizenzierte Gerätelimit für den Vortag und die letzten 30 Tage.
- Die Anzahl der am Vortag beobachteten aktiven Geräte.
- Das 95. Perzentil der in den letzten 30 Tagen beobachteten aktiven Geräte.
- Der Nutzungsprozentsatz des lizenzierten Gerätelimits für den Vortag und die letzten 30 Tage. Die Nutzung ist die Anzahl der aktiven Gerät geteilt durch das lizenzierte Limit.

Sie können eine Systembenachrichtigungsregel erstellen, die Sie warnt, wenn sich die Auslastung der lizenzierten Geräte dem Limit nähert (über 80%) or over (exceeds 100%). Die prozentualen Grenzwerte können bei der Erstellung einer Regel angepasst werden. Wenn Sie feststellen, dass Sie sich ständig dem lizenzierten Limit nähern oder es überschreiten, empfehlen wir Ihnen, mit Ihrem Vertriebsteam zusammenzuarbeiten, um in den nächsten verfügbaren Kapazitätsbereich zu wechseln.

Anzahl der aktiven Gerät überprüfen

Sie können das Diagramm „Anzahl aktiver Gerät und Limit“ anzeigen, um zu überwachen, ob die Anzahl Ihrer aktiven Geräte das lizenzierte Limit überschritten hat.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Aus dem Status und Diagnose Abschnitt, klicken **Anzahl und Limit der aktiven Geräte** um das Diagramm anzusehen.

Audit-Protokoll

Das Audit-Log enthält Daten über den Betrieb Ihres ExtraHop-Systems, aufgeschlüsselt nach Komponenten. Das Audit-Log listet alle bekannten Ereignisse nach Zeitstempel in umgekehrter chronologischer Reihenfolge auf.

Wenn Sie ein Problem mit dem ExtraHop-System haben, lesen Sie das Audit-Log, um detaillierte Diagnosedaten einzusehen, um festzustellen, was das Problem verursacht haben könnte.

Audit-Log-Daten an einen Remote-Syslog-Server senden

Das Audit-Log sammelt Daten über den Betrieb des ExtraHop-Systems, aufgeschlüsselt nach Komponenten. Das auf dem System gespeicherte Protokoll hat eine Kapazität von 10.000 Einträgen, und Einträge, die älter als 90 Tage sind, werden automatisch entfernt. Sie können diese Einträge in den Verwaltungseinstellungen einsehen oder die Audit-Log-Ereignisse zur Langzeitspeicherung, Überwachung und erweiterten Analyse an einen Syslog-Server senden. Alle protokollierten Ereignisse sind in der folgenden Tabelle aufgeführt.

Die folgenden Schritte zeigen Ihnen, wie Sie das ExtraHop-System so konfigurieren, dass Audit-Log-Daten an einen Remote-Syslog-Server gesendet werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Status und Diagnose Abschnitt, klicken Sie **Audit-Protokoll**.
3. Klicken Sie **Syslog-Einstellungen konfigurieren**.
4. In der Reiseziel Feld, geben Sie die IP-Adresse des Remote-Syslog-Servers ein.
5. Aus dem **Protokoll** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   - **TCP**
   - **TLS**
   - **UDP**

   Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.

   Hinweis: Wenn Sie TLS auswählen, muss das ExtraHop-System die Syslog-Serveridentität überprüfen, indem es das TLS-Zertifikat des Server validiert. Du kannst konfigurieren Sie das ExtraHop-System so, dass es der Zertifizierungsstelle (CA) vertraut, die das Zertifikat des Syslog-Servers signiert hat in den Administrationseinstellungen.
6. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Remote-Syslog-Server ein.

   Der Standardwert ist 514.
7. Klicken Sie **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollte in der Syslog-Datei auf dem Syslog-Server ein Eintrag ähnlich dem folgenden angezeigt werden:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
8. Klicken Sie **Speichern**.
9. Optional: Ändern Sie das Format der Syslog-Meldungen:

   Standardmäßig sind Syslog-Meldungen nicht mit RFC 3164 oder RFC 5424 kompatibel. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfiguration ändern.

   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie einen Eintrag hinzu unter `auditlog_rsyslog` wo der Schlüssel ist `rfc_compliant_format` und der Wert ist entweder `rfc5424` oder `rfc3164`.

   Das `auditlog_rsyslog` Der Abschnitt sollte dem folgenden Code ähneln:

   ```
   "auditlog_rsyslog": {
       "syslog_destination": "192.168.0.0",
       "syslog_ipproto": "udp",
   ```

```
        "syslog_port": 514,
        "rfc_compliant_format": "rfc5424"
    }
```

e) Klicken Sie **Aktualisieren**.
f) Klicken Sie **Erledigt**.

10. Optional: Ändern Sie die Zeitzone, auf die in den Syslog-Zeitstempeln verwiesen wird:

    Standardmäßig verweisen Syslog-Zeitstempel auf die UTC-Zeit. Sie können Zeitstempel jedoch so ändern, dass sie auf die ExtraHop-Systemzeit verweisen, indem Sie die laufende Konfiguration ändern.

    a) Klicken Sie **Admin**.
    b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
    c) Klicken Sie **Konfiguration bearbeiten**.
    d) Fügen Sie einen Eintrag hinzu unter `auditlog_rsyslog`, wo der Schlüssel ist `syslog_use_localtime` und der Wert ist `true`.

    Das `auditlog_rsyslog` Der Abschnitt sollte dem folgenden Code ähneln:

```
    "auditlog_rsyslog": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

    e) Klicken Sie **Aktualisieren**.
    f) Klicken Sie **Erledigt**.

Nächste Schritte
Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen wie erwartet funktionieren, behalten Sie Ihre Konfigurationsänderungen bei, indem Sie die laufende Konfigurationsdatei speichern.

Audit-Log-Ereignisse
Die folgenden Ereignisse auf einem ExtraHop-System generieren einen Eintrag im Audit-Log.

Kategorie	Ereignis
Vereinbarungen	• Eine EULA- oder POC-Vereinbarung wird vereinbart
API	• Ein API-Schlüssel wird erstellt • Ein API-Schlüssel wird gelöscht • Ein Benutzer wird erstellt. • Ein Benutzer wird geändert.
Sensormigration	• Eine Sensormigration wird gestartet • Eine Sensormigration war erfolgreich • Eine Sensormigration ist fehlgeschlagen
Browsersitzungen	• Eine bestimmte Browsersitzung wird gelöscht • Alle Browsersitzungen werden gelöscht
Cloud-Dienste	• Status eines angeschlossenen Sensor wird abgerufen
Konsole	• Ein Sensor wird mit einer Konsole verbunden • Ein Sensor wird von einer Konsole getrennt

Kategorie	Ereignis
	• Ein ExtraHop-Recordstore oder Packetstore stellt eine getunnelte Verbindung zu einer Konsole her • Die Konsoleninformationen sind festgelegt • Ein Konsolen-Spitzname ist festgelegt • Einen Sensor aktivieren oder deaktivieren • Der Sensor wird aus der Ferne betrachtet • Eine Lizenz für einen Sensor wird von einer Konsole überprüft • Eine Lizenz für einen Sensor wird von einer Konsole festgelegt
Armaturenbretter	• Ein Dashboard wird erstellt • Ein Dashboard wird umbenannt • Ein Dashboard wird gelöscht • Ein Dashboard-Permalink, auch Kurzcode genannt, wird geändert • Die Optionen zum Teilen von Dashboards wurden geändert
Datenspeicher	• Die erweiterte Datenspeicherkonfiguration wurde geändert • Der Datenspeicher ist zurückgesetzt • Ein Datenspeicher-Reset wurde abgeschlossen • Anpassungen werden gespeichert • Anpassungen werden wiederhergestellt • Anpassungen werden gelöscht
Erkennungen	• Ein Erkennungsstatus wird aktualisiert • Ein Erkennungsbeauftragter wird aktualisiert • Erkennungshinweise werden aktualisiert • Ein externes Ticket wird aktualisiert • Eine Tuning-Regel wird erstellt • Eine Tuning-Regel wird gelöscht • Eine Tuning-Regel wird geändert • Eine Beschreibung der Tuning-Regel wird aktualisiert • Eine Tuning-Regel ist aktiviert • Eine Tuning-Regel ist deaktiviert • Eine Tuning-Regel wird erweitert
Ausnahmedateien	• Eine Ausnahmedatei wird gelöscht
ExtraHop Recordstore Records	• Alle ExtraHop Recordstore-Datensätze werden gelöscht
ExtraHop-Recordstore-Cluster	• Ein neuer ExtraHop-Recordstore-Knoten wird initialisiert • Ein Knoten wird zu einem ExtraHop-Recordstore-Cluster hinzugefügt

Kategorie	Ereignis
	• Ein Knoten wird aus einem ExtraHop-Recordstore-Cluster entfernt • Ein Knoten tritt einem ExtraHop-Recordstore-Cluster bei • Ein Knoten verlässt einen ExtraHop-Recordstore-Cluster • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Recordstore verbunden • Ein Sensor oder eine Konsole ist von einem ExtraHop-Recordstore getrennt • Ein ExtraHop-Recordstore-Knoten wurde entfernt oder fehlt, aber nicht über eine unterstützte Schnittstelle
ExtraHop Aktualisierungsservice	• Eine Entdeckungskategorie wird aktualisiert • Eine Erkennungsdefinition wird aktualisiert • Ein Erkennungsauslöser wird aktualisiert • Eine Ransomware-Definition wird aktualisiert • Erkennungsmetadaten werden aktualisiert • Erweiterter Erkennungsinhalt wird aktualisiert
Firmware	• Die Firmware wurde aktualisiert
Globale Richtlinien	• Die globale Richtlinie für die Bearbeitungssteuerung von Gerätegruppe wurde aktualisiert
Integrationen	• Eine Integration wird aktualisiert
Lizenz	• Eine neue statische Lizenz wird angewendet • Die Lizenzserverkonnektivität wird getestet • Ein Produktschlüssel ist auf dem Lizenzserver registriert • Eine neue Lizenz wird beantragt
Loggen Sie sich in das ExtraHop-System ein	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
Loggen Sie sich über SSH oder REST API ein	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
Module	• Die Zugriffskontrolle für das NDR-Modul ist aktiviert • Die Zugriffskontrolle für das NPM-Modul ist aktiviert
Netzwerk	• Eine Netzwerkschnittstellenkonfiguration wird bearbeitet • Der Hostname oder DNS Einstellung wurde geändert

Kategorie	Ereignis
	• Eine Netzwerkschnittstellenroute wird geändert
Offline-Erfassung	• Eine Offline-Capture-Datei wird geladen
PCAP	• Eine Paketerfassungsdatei (PCAP) wird heruntergeladen
Fernzugriff	• Der Fernzugriff für das ExtraHop Support Team ist aktiviert • Der Fernzugriff für das ExtraHop Support Team ist deaktiviert • Fernzugriff für ExtraHop Support ist aktiviert • Der Fernzugriff für ExtraHop Support ist deaktiviert
RPCAP	• Eine RPCAP-Konfiguration wird hinzugefügt • Eine RPCAP-Konfiguration wird gelöscht
Konfiguration ausführen	• Die laufende Konfigurationsdatei ändert sich
SAML-Identitätsanbieter	• Ein Identitätsanbieter wird hinzugefügt • Ein Identitätsanbieter wird geändert • Ein Identitätsanbieter wird gelöscht
SAML-Anmeldung	• Eine Anmeldung ist erfolgreich • Eine Anmeldung schlägt fehl
SAML-Rechte	• Eine Privilegienstufe wird gewährt • Eine Privilegienstufe wurde verweigert
Sensor-Tags	• Ein Sensor-Tag wird erstellt • Ein Sensor-Tag wurde geändert • Ein Sensor-Tag wird gelöscht • Tags auf einem Sensor werden geändert
SSL-Entschlüsselung	• Ein TLS-Entschlüsselungsschlüssel wird gespeichert
SSL-Sitzungsschlüssel	• Ein PCAP-Sitzungsschlüssel wird heruntergeladen
Kundendienst-Konto	• Das Support-Konto ist deaktiviert • Das Support-Konto ist aktiviert • Der Support-SSH-Schlüssel wird neu generiert
Unterstützungsskript	• Ein Standard-Support-Skript wird ausgeführt • Ein früheres Unterstützungsskript-Ergebnis wird gelöscht • Ein Support-Skript wird hochgeladen

Kategorie	Ereignis
Syslog	• Remote-Syslog-Einstellungen werden aktualisiert
System- und Servicestatus	• Das System startet • Das System wird heruntergefahren • Das System wird neu gestartet • Der Bridge-, Capture- oder Portal-Prozess wird neu gestartet • Ein Systemdienst ist aktiviert (z. B. SNMP, Webshell, Management, SSH) • Ein Systemdienst ist deaktiviert (z. B. SNMP, Webshell, /management, SSH)
Systemzeit	• Die Systemzeit ist eingestellt • Die Systemzeit wurde geändert • Die Systemzeit ist rückwärts eingestellt • NTP-Server sind eingerichtet • Die Zeitzone ist eingestellt • Eine manuelle NTP-Synchronisierung wird angefordert
Systembenutzer	• Ein Benutzer wird hinzugefügt • Benutzermetadaten werden bearbeitet • Ein Benutzer wird gelöscht • Ein Benutzerkennwort ist gesetzt • Ein anderer Benutzer als der `setup` Benutzer versucht, das Passwort eines anderen Benutzers zu ändern • Ein Benutzerkennwort wird aktualisiert
TAXII-Feeds	• Ein TAXII-Feed wird hinzugefügt • Ein TAXII-Feed wird geändert • Ein TAXII-Feed wird gelöscht
Informationsgespräche über Bedrohungen	• Ein Bedrohungsübersicht wird archiviert • Eine Bedrohungsübersicht wird wiederhergestellt
ExtraHop Packetstore	• Ein neuer ExtraHop-Paketstore wird initialisiert • Ein Sensor oder eine Konsole ist mit einem ExtraHop-Packetstore verbunden • Ein Sensor oder eine Konsole ist von einem ExtraHop-Packetstore getrennt • Ein ExtraHop-Paketstore wird zurückgesetzt
Tendenzen	• Ein Trend wird zurückgesetzt
Trigger	• Ein Auslöser wird hinzugefügt • Ein Auslöser wird bearbeitet • Ein Auslöser wird gelöscht

Kategorie	Ereignis
Benutzergruppen	• Eine lokale Benutzergruppe wird erstellt • Eine lokale Benutzergruppe wird gelöscht • Eine lokale Benutzergruppe ist aktiviert • Eine lokale Benutzergruppe ist deaktiviert

Fingerabdruck

Fingerabdrücke helfen dabei, Appliances vor Machine-in-the-Middle-Angriffen zu schützen, indem sie eine eindeutige Kennung bereitstellen, die beim Verbinden von ExtraHop-Appliances verifiziert werden kann.

Wenn Sie einen ExtraHop-Recordstore oder Packetstore mit einem Paketsensor oder einer Konsole verbinden, stellen Sie sicher, dass der angezeigte Fingerabdruck genau dem Fingerabdruck entspricht, der auf der Join- oder Pairing-Seite angezeigt wird.

Wenn die Fingerabdrücke nicht übereinstimmen, wurde die Kommunikation zwischen den Geräten möglicherweise abgefangen und verändert.

Ausnahmedateien

Ausnahmedateien sind eine Kerndatei der im Speicher gespeicherten Daten. Wenn Sie die Einstellung Ausnahmedatei aktivieren, wird die Kerndatei auf die Festplatte geschrieben, wenn das System unerwartet stoppt oder neu gestartet wird. Diese Datei kann dem ExtraHop Support helfen, das Problem zu diagnostizieren.

Klicken Sie **Ausnahmedateien aktivieren** oder **Ausnahmedateien deaktivieren** um das Speichern von Ausnahmedateien zu aktivieren oder zu deaktivieren.

Unterstützungsskripte

ExtraHop Support stellt möglicherweise ein Support-Skript bereit, das eine spezielle Einstellung anwenden, eine kleine Anpassung am ExtraHop-System vornehmen oder Hilfe beim Fernsupport oder bei erweiterten Einstellungen bieten kann. Die Administrationseinstellungen ermöglichen es Ihnen, Support-Skripte hochzuladen und auszuführen.

Führen Sie das Standard-Support-Skript aus

Das Standard-Support-Skript sammelt Informationen über den Zustand des ExtraHop-Systems zur Analyse durch den ExtraHop Support.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Status und Diagnose Abschnitt, klicken **Unterstützungsskripte**.
3. klicken **Standard-Support-Skript ausführen**.
4. klicken **Lauf**.
   Wenn das Skript abgeschlossen ist, Ergebnisse des Support-Skripts Seite wird angezeigt.
5. Klicken Sie auf den Namen des Diagnose-Support-Pakets, das Sie herunterladen möchten.

   Die Datei wird am Standardspeicherort für Downloads auf Ihrem Computer gespeichert.

   Senden Sie diese Datei, normalerweise mit dem Namen `diag-results-complete.expk`, an den ExtraHop Support.

Das `.expk` Die Datei ist verschlüsselt und der Inhalt ist nur für den ExtraHop Support sichtbar. Sie können jedoch das herunterladen `diag-results-complete.manifest` Datei, um eine Liste der gesammelten Dateien anzuzeigen.

Führen Sie ein benutzerdefiniertes Support-Skript aus

Wenn Sie vom ExtraHop Support ein benutzerdefiniertes Support-Skript erhalten, gehen Sie wie folgt vor, um eine kleine Anpassung am System vorzunehmen oder erweiterte Einstellungen vorzunehmen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Status und Diagnose Abschnitt, klicken **Unterstützungsskripte**.
3. klicken **Benutzerdefiniertes Support-Skript ausführen**.
4. klicken **Wählen Sie Datei**, navigieren Sie zu dem Diagnosesupport-Skript, das Sie hochladen möchten, und klicken Sie dann auf **Offen**.
5. klicken **Upload** um die Datei auf dem ExtraHop-System auszuführen.
   Der ExtraHop Support bestätigt, dass das Support-Skript die gewünschten Ergebnisse erzielt hat.

Netzwerk-Einstellungen

Die Netzwerk-Einstellungen Dieser Abschnitt enthält Konfigurationseinstellungen für Ihr ExtraHop-System. Mit diesen Einstellungen können Sie einen Hostnamen festlegen, Benachrichtigungen konfigurieren und Verbindungen zu Ihrem System verwalten.

Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

ExtraHop Cloud Services bietet Zugriff auf die Cloud-basierten Dienste von ExtraHop über eine verschlüsselte Verbindung.

Ihre Systemlizenz bestimmt, welche Dienste für Ihre ExtraHop-Konsole oder Ihren ExtraHop-Sensor verfügbar sind. Eine einzelne Lizenz kann jeweils nur auf eine einzelne Appliance oder virtuelle Maschine (VM) angewendet werden. Wenn Sie eine Lizenz von einer Appliance oder VM auf eine andere übertragen möchten, können Sie Systemregistrierung verwalten von der ExtraHop Cloud Services-Seite.

Nachdem die Verbindung hergestellt wurde, werden Informationen zu den verfügbaren Diensten auf der Seite ExtraHop Cloud Services angezeigt.

- Durch das Teilen von Daten mit dem ExtraHop Machine Learning Service können Sie Funktionen aktivieren, die das ExtraHop-System und Ihre Benutzererfahrung verbessern.
  - Aktivieren Sie den AI-Suchassistenten, um Geräte mit Benutzeraufforderungen in natürlicher Sprache zu finden, die zur Produktverbesserung mit ExtraHop Cloud Services geteilt werden. Sehen Sie die Häufig gestellte Fragen zum AI-Suchassistenten für weitere Informationen. AI Search Assistant kann derzeit nicht für die folgenden Regionen aktiviert werden:
    - Asien-Pazifik (Singapur, Sydney, Tokio)
    - Europa (Frankfurt, Paris)
  - Melden Sie sich für Expanded Threat Intelligence an, damit der Machine Learning Service Daten wie IP-Adressen und Hostnamen anhand der von CrowdStrike bereitgestellten Bedrohungsinformationen, gutartigen Endpunkten und anderen Informationen zum Netzwerkverkehr überprüfen kann. Sehen Sie die Häufig gestellte Fragen zu erweiterten Bedrohungsinformationen für weitere Informationen.
  - Tragen Sie Daten wie Datei-Hashes und externe IP-Adressen zur Collective Threat Analysis bei, um die Erkennungsgenauigkeit zu verbessern. Sehen Sie die Häufig gestellte Fragen zur kollektiven Gefahrenanalyse für weitere Informationen.
- Der ExtraHop Update Service ermöglicht automatische Aktualisierungen von Ressourcen auf dem ExtraHop-System, wie z. B. Ransomware-Paketen.
- Mit ExtraHop Remote Access können Sie Mitgliedern des ExtraHop-Account-Teams und dem ExtraHop-Support erlauben, sich mit Ihrem ExtraHop-System zu verbinden, um Hilfe bei der Konfiguration zu erhalten. Sehen Sie die Häufig gestellte Fragen zum Fernzugriff für weitere Informationen über Benutzer mit Fernzugriff.

Video: Sehen Sie sich die entsprechende Schulung an: Stellen Sie eine Verbindung zu ExtraHop Cloud Services her

Bevor Sie beginnen

- RevealX 360-Systeme werden automatisch mit ExtraHop Cloud Services verbunden. Möglicherweise müssen Sie jedoch Zugriff über Netzwerkfirewalls zulassen.
- Sie müssen die entsprechende Lizenz auf dem ExtraHop-System anwenden, bevor Sie eine Verbindung zu ExtraHop Cloud Services herstellen können. Sehen Sie die Häufig gestellte Fragen zur Lizenz für weitere Informationen.
- Sie müssen eingerichtet haben oder System- und Zugriffsadministrationsrechte um auf die Administrationseinstellungen zuzugreifen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **ExtraHop Cloud-Dienste**.
3. Klicken Sie **Allgemeine Geschäftsbedingungen** um den Inhalt zu lesen.
4. Lesen Sie die Allgemeinen Geschäftsbedingungen und aktivieren Sie dann das Kontrollkästchen.
5. Klicken Sie **Stellen Sie eine Verbindung zu ExtraHop Cloud Services her**.

   Nachdem Sie eine Verbindung hergestellt haben, wird die Seite aktualisiert und zeigt Status- und Verbindungsinformationen für jeden Dienst an.
6. Optional: In der Service für maschinelles Lernen Abschnitt, wählen Sie eine oder mehrere erweiterte Funktionen aus:
   - Aktiviere den AI Search Assistant, indem du auswählst **Ich bin damit einverstanden, den KI-Suchassistenten zu aktivieren und Suchanfragen in natürlicher Sprache an ExtraHop Cloud Services zu senden**. (NDR-Modul erforderlich)
   - Aktivieren Sie Expanded Threat Intelligence, indem Sie **Ich bin damit einverstanden, IP-Adressen, Domainnamen, Hostnamen, Datei-Hashes und URLs an ExtraHop Cloud Services zu senden**.
   - Aktivieren Sie die kollektive Bedrohungsanalyse, indem Sie **Ich bin damit einverstanden, Domainnamen, Hostnamen, Datei-Hashes und externe IP-Adressen zu ExtraHop Cloud Services beizutragen**.

Wenn die Verbindung fehlschlägt, liegt möglicherweise ein Problem mit Ihren Firewallregeln vor.

Konfigurieren Sie Ihre Firewallregeln

Wenn Ihr ExtraHop-System in einer Umgebung mit einer Firewall eingesetzt wird, müssen Sie den Zugriff auf ExtraHop Cloud Services öffnen. Für RevealX 360-Systeme, die mit selbstverwalteten Systemen verbunden sind Sensoren, müssen Sie auch den Zugriff auf den Cloud-basierten Recordstore öffnen, der in RevealX Standard Investigation enthalten ist

Offener Zugang zu Cloud-Diensten

Für den Zugriff auf ExtraHop Cloud Services ist Ihr Sensoren muss in der Lage sein, DNS-Abfragen für*.extrahop.com aufzulösen und auf TCP 443 (HTTPS) unter einer der folgenden IP-Adressen zuzugreifen , die Ihrem entsprechen Sensor Lizenz. Wir empfehlen, den Zugriff auf beide IP-Adressen zu öffnen, um sich vor Betriebsunterbrechungen zu schützen.

Region	IP-Adressen
Nord-, Mittel- und Südamerika (AMER)	35,161,154,247 54,191,189,22
Asien, Pazifik (APAC)	54,66,242,25 13,239,224,80
Europa, Naher Osten, Afrika (EMEA)	52,59,110,168 18,198,13,99
Bundesstaat der Vereinigten Staaten (US-FED)	3,135,6,11 3,139,1111,240

Offener Zugang zu RevealX 360 Premium Investigation

Für den Zugriff auf RevealX 360 Premium Investigation ist Ihr Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf bestimmte vollqualifizierte Domainnamen zuzugreifen.

In den Vereinigten Staaten befindliche Sensoren müssen auf diese Domainnamen zugreifen können:

- `eh.oem-2-1.logscale.us-2.crowdstrike.com`
- `eh.oem-2-2.logscale.us-2.crowdstrike.com`

Sensoren, die sich in der Europäischen Union befinden, müssen auf diesen Domänenname zugreifen können:

- `eh.oem-2-3.logscale.eu-1.crowdstrike.com`

Zusätzlich zur Konfiguration des Zugriffs auf diese Domänen müssen Sie auch die globale Proxyserver-Einstellungen.

Offener Zugang zu RevealX 360 Standard Investigation

Für den Zugriff auf RevealX 360 Standard Investigation ist Ihr Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf diese vollständig qualifizierten Domainnamen zuzugreifen:

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`
- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Sie können auch die öffentlichen Leitlinien von Google zu folgenden Themen lesen Berechnung möglicher IP-Adressbereiche für googleapis.com.

Zusätzlich zur Konfiguration des Zugriffs auf diese Domänen müssen Sie auch die globale Proxy-Servereinstellungen.

Stellen Sie über einen Proxy eine Verbindung zu ExtraHop Cloud Services her

Wenn Sie keine direkte Internetverbindung haben, können Sie versuchen, über einen expliziten Proxy eine Verbindung zu ExtraHop Cloud Services herzustellen.

Bevor Sie beginnen
Überprüfen Sie, ob Ihr Proxyanbieter so konfiguriert ist, dass er Machine-in-the-Middle (MITM) ausführt, wenn SSH über HTTP CONNECT zu localhost:22 getunnelt wird. ExtraHop Cloud Services stellt einen verschlüsselten inneren SSH-Tunnel bereit, sodass der Datenverkehr für die MITM-Inspektion nicht sichtbar ist. Wir empfehlen, eine Sicherheitsausnahme zu erstellen und die MITM-Inspektion für diesen Verkehr zu deaktivieren.

Wichtig: Wenn Sie MITM auf Ihrem Proxy nicht deaktivieren können, müssen Sie die Zertifikatsvalidierung in der Konfigurationsdatei des ExtraHop-Systems deaktivieren. Weitere Informationen finden Sie unter Zertifikatsvalidierung umgehen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. klicken **ExtraHop Cloud Proxy aktivieren**.
4. In der Hostname Feld, geben Sie den Hostnamen für Ihren Proxyserver ein, z. B. `Proxyhost`.
5. In der Hafen Feld, geben Sie den Port für Ihren Proxyserver ein, z. B. `8080`.
6. Optional: Falls erforderlich, in der Nutzername und Passwort Felder, geben Sie einen Benutzernamen und ein Passwort für Ihren Proxyserver ein.
7. Klicken Sie **Speichern**.

Zertifikatsvalidierung umgehen

Einige Umgebungen sind so konfiguriert, dass verschlüsselter Datenverkehr das Netzwerk nicht verlassen kann, ohne von einem Drittanbietergerät überprüft zu werden. Dieses Gerät kann als TLS-Endpunkt fungieren, der den Datenverkehr entschlüsselt und erneut verschlüsselt, bevor die Pakete an ExtraHop Cloud Services gesendet werden.

Wenn ein System über einen Proxyserver eine Verbindung zu ExtraHop Cloud Services herstellt und die Zertifikatsvalidierung fehlschlägt, deaktivieren Sie die Zertifikatsvalidierung und versuchen Sie erneut, die Verbindung herzustellen. Die Sicherheit der ExtraHop-Systemauthentifizierung und -verschlüsselung stellt sicher, dass die Kommunikation zwischen Systemen und ExtraHop Cloud-Diensten nicht abgefangen werden kann.

Hinweis: Für das folgende Verfahren müssen Sie mit der Änderung der laufenden ExtraHop-Konfigurationsdatei vertraut sein.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Konfiguration ausführen**.
3. Klicken Sie **Konfiguration bearbeiten**.
4. Fügen Sie am Ende der laufenden Konfigurationsdatei die folgende Zeile hinzu:

```
"hopcloud": { "verify_outer_tunnel_cert": false }
```

5. Klicken Sie **Aktualisieren**.
6. Klicken Sie **Änderungen anzeigen und speichern**.
7. Überprüfe die Änderungen.
8. Klicken Sie **Speichern**.
9. Klicken Sie **Erledigt**.

Trennen Sie die Verbindung zu den ExtraHop Cloud Services

Sie können ein ExtraHop-System von den ExtraHop Cloud Services trennen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **ExtraHop Cloud-Dienste**.
3. In der Verbindung zu Cloud-Diensten Abschnitt, klicken Sie **Trennen**.

Registrierung für ExtraHop Cloud Services verwalten

Wenn Sie eine bestehende Lizenz von einem ExtraHop-System auf ein anderes übertragen möchten, können Sie die Systemregistrierung auf der Seite ExtraHop Cloud Services verwalten. Durch die Aufhebung der Registrierung eines Systems werden alle Daten und historischen Analysen für den Machine Learning Service aus dem System gelöscht und sind nicht mehr verfügbar.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **ExtraHop Cloud-Dienste**.
3. In der Verbindung zu Cloud-Diensten Abschnitt, klicken **Abmelden**.

Konnektivität

Das Konnektivität Die Seite enthält Steuerelemente für Ihre Appliance-Verbindungen und Netzwerkeinstellungen.

Status der Schnittstelle

Auf physischen Appliances wird ein Diagramm der Schnittstellenverbindungen angezeigt, das basierend auf dem Portstatus dynamisch aktualisiert wird.

- Der blaue Ethernet-Port dient der Verwaltung
- Ein schwarzer Ethernet-Port weist auf einen lizenzierten und aktivierten Port hin, der derzeit ausgefallen ist
- Ein grüner Ethernet-Port weist auf einen aktiven, verbundenen Port hin
- Ein grauer Ethernet-Port weist auf einen deaktivierten oder nicht lizenzierten Port hin

Netzwerkeinstellungen

- Klicken Sie **Einstellungen ändern** um einen Hostnamen für Ihre ExtraHop-Appliance hinzuzufügen oder DNS-Server hinzuzufügen.

Proxy-Einstellungen

- Aktiviere eine globaler Proxy um eine Verbindung zu einer ExtraHop-Konsole herzustellen
- Aktiviere eine Cloud-Proxy um eine Verbindung zu ExtraHop Cloud Services herzustellen

Einstellungen für die Bond-Schnittstelle

- Erstellen Sie eine Bond-Schnittstelle um mehrere Schnittstellen zu einer logischen Schnittstelle mit einer einzigen IP-Adresse zu verbinden.

Schnittstellen

Sehen Sie sich Ihre Verwaltungs- und Überwachungsschnittstellen an und konfigurieren Sie sie. Klicken Sie auf eine beliebige Schnittstelle, um die Einstellungsoptionen anzuzeigen.

- Erfassen Sie den Datenverkehr von NetFlow- und sFlow-Geräten
- Paketweiterleitung mit RPCAP

Einstellungen für die Paketaufnahme

- Konfigurieren Sie die Quelle der Pakete, die von diesem Sensor aufgenommen werden. Sie können den Sensor so einrichten, dass er Pakete aus einem direkten Feed oder Pakete, die von einem Drittanbieter weitergeleitet wurden, aufnimmt.

Eine Schnittstelle konfigurieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, von der **Schnittstellen-Modus** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   Deaktiviert

   Die Schnittstelle ist deaktiviert.

   Überwachung (nur Empfang)

   Überwacht den Netzwerkverkehr.

   Verwaltung

   Verwaltet den ExtraHop-Sensor.

   Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target

   Verwaltet den ExtraHop-Sensor und erfasst den von einem Paketweiterleiter weitergeleiteten Verkehr, ERSPAN*, VXLAN** oder GENEVE***.

   Während die 10-GbE-Management+-Erfassungsschnittstellen auf diesem Sensor Verwaltungsfunktionen mit Geschwindigkeiten von 10 Gbit/s ausführen können, ist die Verarbeitung von Datenverkehr wie ERSPAN, VXLAN und GENEVE auf 1 Gbit/s begrenzt.

Hinweis: In Umgebungen mit asymmetrischem Routing neben den Hochleistungsschnittstellen gelangen Ping-Antworten möglicherweise nicht an den Absender zurück.

Leistungsstarkes ERSPAN/VXLAN/GENEVE-Ziel

Erfasst den von ERSPAN *, VXLAN** oder GENEVE*** weitergeleiteten Datenverkehr. Dieser Schnittstellenmodus ermöglicht es dem Port, mehr als 1 Gbit/s zu verarbeiten. Stellen Sie diesen Schnittstellenmodus ein, wenn der ExtraHop-Sensor über einen 10-GbE-Anschluss verfügt. Für diesen Schnittstellenmodus müssen Sie nur eine IPv4-Adresse konfigurieren.

* Das ExtraHop-System unterstützt die folgenden ERSPAN-Implementierungen:

- ERSPAN Typ I
- ERSPAN Typ II
- ERSPAN Typ III
- Transparentes Ethernet-Bridging. ERSPAN-ähnliche Kapselung, die häufig in virtuellen Switch-Implementierungen wie dem VMware VDS und Open vSwitch zu finden ist.

**Virtual Extensible LAN (VXLAN) -Pakete werden auf dem UDP-Port 4789 empfangen.

***Generic Network Virtualization Encapsulation (GENEVE) -Pakete werden auf dem UDP-Port 6081 empfangen. Informationen zur Konfiguration von Geneve-gekapseltem Datenverkehr, der von einem AWS Gateway Load Balancer (GWLB) weitergeleitet wird, der als VPC Traffic Mirroring-Ziel fungiert, finden Sie im AWS-Dokumentation.

Hinweis: Für Amazon Web Services (AWS) -Bereitstellungen mit einer Schnittstelle müssen Sie auswählen **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1. Wenn Sie zwei Schnittstellen konfigurieren, müssen Sie auswählen **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 1 und **Verwaltung + RPCAP/ERSPAN/VXLAN/GENEVE Target** für Interface 2.

Hinweis: Bei Azure-Bereitstellungen unterstützen einige Instanzen, auf denen ältere NICs ausgeführt werden, möglicherweise den Hochleistungs-ERSPAN-/VXLAN-/GENEVE-Zielmodus nicht.

5. Optional: Wählen Sie eine Schnittstellengeschwindigkeit aus.

   Automatisch aushandeln ist standardmäßig ausgewählt; Sie sollten jedoch manuell eine Geschwindigkeit auswählen, wenn sie von Ihrem Sensor, Netzwerk-Transceiver und Netzwerk-Switch unterstützt wird.

   - **Automatisch aushandeln**
   - **10 Gbit/s**
   - **25 Gbit/s**
   - **40 Gbit/s**
   - **100 Gbit/s**

   Wichtig: Wenn Sie die Schnittstellengeschwindigkeit ändern auf **Automatisch aushandeln**, Sie müssen den Sensor möglicherweise neu starten, bevor die Änderung wirksam wird.

6. Optional: Wählen Sie einen FEC-Typ (Forward Error Correction).

   Wir empfehlen Auto-Negotiate, das für die meisten Umgebungen optimal ist.

   • **Automatisch aushandeln:** Aktiviert automatisch entweder RS-FEC oder Firecode FEC oder deaktiviert FEC basierend auf den Funktionen der verbundenen Schnittstellen.

   • **RS-FEC:** Aktiviert Reed-Solomon FEC immer.

   • **Firecode:** Aktiviert immer Firecode (FC) FEC, auch bekannt als BaseR FEC.

   • **Deaktiviert:** Deaktiviert FEC.

7. Konfigurieren Sie DCHP.

DHCPv4 ist standardmäßig aktiviert. Wenn Ihr Netzwerk DHCP nicht unterstützt, können Sie das löschen **DHCPv4** Kontrollkästchen, um DHCP zu deaktivieren und dann eine statische IP-Adresse, eine Netzmaske und ein Standard-Gateway einzugeben.

Hinweis: Nur eine Schnittstelle sollte mit einem Standard-Gateway konfiguriert werden. Statische Routen konfigurieren wenn Ihr Netzwerk das Routing über mehrere Gateways erfordert.

8. Konfigurieren Sie den TCP-Health-Check-Port.

   Diese Einstellung ist nur für Hochleistungsschnittstellen konfigurierbar und wird benötigt, wenn GENEVE-Datenverkehr von einem AWS Gateway Load Balancer (GWLB) aufgenommen wird. Der Wert der Portnummer muss mit dem in AWS konfigurierten Wert übereinstimmen. Weitere Informationen finden Sie unter Weiterleiten von geneve-gekapseltem Datenverkehr von einem AWS Gateway Load Balancer.
9. Optional: Aktiviere IPv6.

   Weitere Hinweise zur Konfiguration von IPv6 finden Sie unter IPv6 für eine Schnittstelle aktivieren.
10. Optional: Fügen Sie manuell Routen hinzu.
11. Klicken Sie **Speichern**.

Stellen Sie eine statische Route ein

Bevor Sie beginnen
Sie müssen DHCPv4 deaktivieren, bevor Sie eine statische Route hinzufügen können.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, stellen Sie sicher, dass die **IPv4-Adresse** und **Netzmaske** Die Felder sind vollständig und gespeichert und klicken Sie auf **Routen bearbeiten**.
5. In der Route hinzufügen Abschnitt, geben Sie einen Netzwerkadressbereich in CIDR-Notation in das **Netzwerk** Feld und IPv4-Adresse im **Über IP** Feld und dann klicken **Hinzufügen**.
6. Wiederholen Sie den vorherigen Schritt für jede Route, die Sie hinzufügen möchten.
7. Klicken Sie **Speichern**.

IPv6 für eine Schnittstelle aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle, die Sie konfigurieren möchten.
4. Auf dem Netzwerkeinstellungen für die Schnittstelle *<interface number>* Seite, auswählen **IPv6 aktivieren**.
   IPv6-Konfigurationsoptionen werden unten angezeigt **IPv6 aktivieren**.
5. Optional: Konfigurieren Sie IPv6-Adressen für die Schnittstelle.
   - Um IPv6-Adressen automatisch über DHCPv6 zuzuweisen, wählen Sie **DHCPv6 aktivieren**.

     Hinweis: Wenn diese Option aktiviert ist, wird DHCPv6 zur Konfiguration der DNS-Einstellungen verwendet.
   - Um IPv6-Adressen durch die automatische Konfiguration zustandsloser Adressen automatisch zuzuweisen, verwenden Sie das **Automatische Konfiguration zustandsloser Adressen** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

MAC-Adresse verwenden

Konfiguriert die Appliance so, dass IPv6-Adressen automatisch auf der Grundlage der MAC-Adresse der Appliance zugewiesen werden.

Verwenden Sie eine stabile private Adresse

Konfiguriert die Appliance so, dass sie automatisch private IPv6-Adressen zuweist, die nicht auf Hardwareadressen basieren. Diese Methode ist in RFC 7217 beschrieben.

- Um eine oder mehrere statische IPv6-Adressen manuell zuzuweisen, geben Sie die Adressen in das Statische IPv6-Adressen Feld.

6. Damit die Appliance Informationen zum rekursiven DNS-Server (RDNSS) und zur DNS-Suchliste (DNSSL) gemäß den Router-Ankündigungen konfigurieren kann, wählen Sie **RDNSS/DNSSL**.
7. Klicken Sie **Speichern**.

Schnittstellendurchsatz

ExtraHop Sensor Die Modelle EDA 6100, EDA 8100 und EDA 9100 sind für die Erfassung des Datenverkehrs ausschließlich an 10-GbE-Ports optimiert.

Die Aktivierung der 1-GbE-Schnittstellen für die Überwachung des Datenverkehrs kann sich je nach ExtraHop auf die Leistung auswirken Sensor. Sie können diese zwar optimieren Sensoren Um den Datenverkehr gleichzeitig an den 10-GbE-Anschlüssen und den drei nicht verwaltbaren 1-GbE-Ports zu erfassen, empfehlen wir Ihnen, sich an den ExtraHop-Support zu wenden, um Unterstützung zu erhalten, um einen verringerten Durchsatz zu vermeiden.

Hinweis: Die Sensoren EDA 6200, EDA 8200, EDA 9200 und EDA 10200 sind nicht anfällig für einen reduzierten Durchsatz, wenn Sie 1-GbE-Schnittstellen für die Überwachung des Datenverkehrs aktivieren.

ExtraHop-Sensor	Durchsatz	Einzelheiten
SEIT 1900	Standarddurchsatz von 40 Gbit/s	Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, können Sie bis zu vier der 10-GbE-Schnittstellen für einen kombinierten Durchsatz von bis zu 40 Gbit/s verwenden.
SEIT 1800	Standarddurchsatz von 20 Gbit/s	Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, können Sie entweder eine oder beide der 10-GbE-Schnittstellen für einen kombinierten Durchsatz von bis zu 20 Gbit/s verwenden.
AB 6100	Standarddurchsatz von 10 Gbit/s	Wenn die nicht verwaltbaren 1-GbE-Schnittstellen deaktiviert sind, beträgt der maximale kombinierte Gesamtdurchsatz 10 Gbit/s.
SEIT 3100	Standarddurchsatz von 3 Gbit/s	Keine 10GbE-Schnittstelle
SEIT 1100	Standarddurchsatz von 1 Gbit/s	Keine 10GbE-Schnittstelle

Sensordurchsatz für mehrere Module

Etwas ExtraHop Sensor Modelle unterstützen die Aktivierung des IDS-Moduls, sofern der Sensor für das NDR-Modul lizenziert ist. Die Aktivierung von Intrusion Detection System auf diesen Sensoren kann sich auf den Sensordurchsatz auswirken.

ExtraHop Sensormodell	IDS-Unterstützung	Durchsatz ohne Intrusion Detection System (Gbit/s)	Durchsatz mit Intrusion Detection System (Gbit/s)
1200	Nein	1	N/A
4200	Nein	5	N/A
6200	Ja	10	4
8200	Ja	25	10
8320	Ja	25	25
9200	Ja	50	20
9300	Ja	50	30
10200	Ja	100	40
10300	Ja	100	TBD

Globaler Proxyserver

Wenn Ihre Netzwerktopologie einen Proxyserver benötigt, damit Ihr ExtraHop-System entweder mit einem Konsole oder mit anderen Geräten außerhalb des lokalen Netzwerks können Sie Ihr ExtraHop-System so einrichten, dass es eine Verbindung zu einem Proxyserver herstellt, den Sie bereits in Ihrem Netzwerk haben. Für den globalen Proxyserver ist keine Internetverbindung erforderlich.

Einen globalen Proxy konfigurieren

Wichtig: Sie können nur einen globalen Proxyserver pro ExtraHop-System konfigurieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Proxy-Einstellungen Abschnitt, klicken Sie **Globalen Proxy aktivieren**.
4. In der Hostname Feld, geben Sie den Hostnamen oder die IP-Adresse für Ihren globalen Proxyserver ein
5. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Proxyserver ein.
6. In der Nutzername Geben Sie in dieses Feld den Namen eines Benutzers ein, der privilegierten Zugriff auf Ihren globalen Proxyserver hat.
7. In der Passwort Feld, geben Sie das Passwort für den oben angegebenen Benutzer ein.

ExtraHop Cloud-Proxy

Wenn Ihr ExtraHop-System nicht über eine direkte Internetverbindung verfügt, können Sie über einen Proxy-Server, der speziell für die Konnektivität von ExtraHop-Cloud-Diensten vorgesehen ist, eine Verbindung zum Internet herstellen . Pro System kann nur ein Proxy konfiguriert werden.

Füllen Sie die folgenden Felder aus und klicken Sie auf **Speichern** um einen Cloud-Proxy zu aktivieren.

- **Hostname :** Der Hostname oder die IP-Adresse für Ihren Cloud-Proxyserver.
- **Hafen :** Die Portnummer für Ihren Cloud-Proxyserver.
- **Nutzername :** Der Name eines Benutzers, der Zugriff auf Ihren Cloud-Proxyserver hat.
- **Passwort :** Das Passwort für den oben angegebenen Benutzer.

Bond-Schnittstellen

Sie können mehrere Schnittstellen auf Ihrem ExtraHop-System zu einer einzigen logischen Schnittstelle verbinden, die eine IP-Adresse für die kombinierte Bandbreite der Mitgliedsschnittstellen hat. Verbindungsschnittstellen ermöglichen einen größeren Durchsatz mit einer einzigen IP-Adresse. Diese Konfiguration wird auch als Link-Aggregation, Port-Channeling, Linkbündelung, Ethernet-/Netzwerk-/NIC-Bonding oder NIC-Teaming bezeichnet. Bond-Schnittstellen können nicht in den Überwachungsmodus versetzt werden.

Hinweis: Wenn Sie die Einstellungen der Bond-Schnittstelle ändern, verlieren Sie die Konnektivität zu Ihrem ExtraHop-System. Sie müssen Änderungen an Ihrer Netzwerk-Switch-Konfiguration vornehmen, um die Konnektivität wiederherzustellen. Die erforderlichen Änderungen hängen von Ihrem Switch ab. Wenden Sie sich an den ExtraHop-Support, um Unterstützung zu erhalten, bevor Sie eine Bond-Schnittstelle erstellen.

- Bonding ist nur auf Management- oder Management +-Schnittstellen konfigurierbar.
- Port-Channeling auf den ExtraHop-Sensoren werden keine Anschlüsse zur Verkehrsüberwachung unterstützt.

Schnittstellen, die als Mitglieder einer Bond-Schnittstelle ausgewählt wurden, sind nicht mehr unabhängig konfigurierbar und werden angezeigt als Deaktiviert (Bond-Mitglied) im Abschnitt Schnittstellen der Seite Konnektivität. Nachdem eine Bond-Schnittstelle erstellt wurde, können Sie keine weiteren Mitglieder hinzufügen oder vorhandene Mitglieder löschen. Die Bond-Schnittstelle muss zerstört und neu erstellt werden.

- Erstellen Sie eine Bond-Schnittstelle
- Modifizieren Sie eine Bond-Schnittstelle
- Zerstöre eine Bond-Schnittstelle

Erstellen Sie eine Bond-Schnittstelle

Sie können eine Bond-Schnittstelle mit mindestens einem Schnittstellenelement und bis zu der Anzahl von Elementen erstellen, die für das Bonding verfügbar sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Einstellungen für die Bond-Schnittstelle Abschnitt, klicken Sie **Bond-Schnittstelle erstellen**.
4. Wählen Sie das Kontrollkästchen neben jeder Schnittstelle aus, die Sie in das Bonding einbeziehen möchten.

   Es werden nur Ports angezeigt, die derzeit für eine Bond-Mitgliedschaft verfügbar sind.
5. Aus dem **Einstellungen übernehmen von** Wählen Sie in der Dropdownliste die Schnittstelle aus, die die Einstellungen enthält, die Sie auf die Bond-Schnittstelle anwenden möchten.

   Die Einstellungen für alle nicht ausgewählten Schnittstellen gehen verloren.
6. Für **Art der Anleihe**, wählen Sie eine der folgenden Optionen:
   - **Statisch**, wodurch eine statische Bindung entsteht.
   - **802.3ad (LACP)**, das durch IEEE 802.3ad Link Aggregation (LACP) eine dynamische Verbindung herstellt.
7. Aus dem **Hash-Richtlinie** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:
   - **Schicht 3+4** Richtlinie, die die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger verteilt. Diese Richtlinie entspricht jedoch nicht vollständig den 802.3ad-Standards.
   - **Ebene 2+3** Richtlinie, die den Datenverkehr weniger gleichmäßig verteilt und den 802.3ad-Standards entspricht.
8. Klicken Sie **Erstellen**.

Aktualisieren Sie die Seite, um das anzuzeigen Bond-Schnittstellen Abschnitt. Jedes Mitglied der Bond-Schnittstelle, dessen Einstellungen nicht in der ausgewählt wurden **Einstellungen übernehmen von** Dropdownlisten werden angezeigt als **Deaktiviert (Bond-Mitglied)** in der Schnittstellen Abschnitt.

Ändern Sie die Einstellungen für die Bond-Schnittstelle
Nachdem eine Bond-Schnittstelle erstellt wurde, können Sie die meisten Einstellungen so ändern, als ob die Bond-Schnittstelle eine einzelne Schnittstelle wäre.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Bond-Schnittstellen Abschnitt, klicken Sie auf die Bond-Schnittstelle, die Sie ändern möchten.
4. Auf dem Netzwerkeinstellungen für Bond Interface <*Schnittstellennummer*> Seite, ändern Sie die folgenden Einstellungen nach Bedarf:

   • **Mitglieder :** Die Schnittstellenmitglieder der Bond-Schnittstelle. Mitglieder können nicht geändert werden, nachdem eine Bond-Schnittstelle erstellt wurde. Wenn Sie die Mitglieder ändern müssen, müssen Sie die Bond-Schnittstelle zerstören und neu erstellen.

   • **Bond-Modus:** Geben Sie an, ob eine statische Bindung oder eine dynamische Bindung über IEEE 802.3ad Link Aggregation (LACP) erstellt werden soll.

   • **Schnittstellen-Modus :** Die Art der Anleihemitgliedschaft. Eine Bond-Schnittstelle kann **Verwaltung** oder **Management+RPCAP/ERSPAN-Ziel** nur.

   • **DHCPv4 aktivieren :** Wenn DHCP aktiviert ist, wird automatisch eine IP-Adresse für das Bond-Interface abgerufen.

   • **Hash-Richtlinie:** Geben Sie die Hash-Richtlinie an. Das **Schicht 3+4** Die Richtlinie gleicht die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger aus, entspricht jedoch nicht vollständig den 802.3ad-Standards. Das **Ebene 2+3** Die Richtlinie verteilt den Verkehr weniger gleichmäßig, entspricht jedoch den 802.3ad-Standards.

   • **IPv4-Adresse :** Die statische IP-Adresse der Bond-Schnittstelle. Diese Einstellung ist nicht verfügbar, wenn DHCP aktiviert ist.

   • **Netzmaske :** Die Netzwerk-Netzmaske für die Bond-Schnittstelle.

   • **Tor :** Die IP-Adresse des Netzwerk-Gateways.

   • **Strecken :** Die statischen Routen für die Bond-Schnittstelle. Diese Einstellung ist nicht verfügbar, wenn DHCP aktiviert ist.

   • **IPv6 aktivieren :** Aktivieren Sie die Konfigurationsoptionen für IPv6.
5. Klicken Sie **Speichern**.

Zerstöre eine Bond-Schnittstelle
Wenn eine Bond-Schnittstelle zerstört wird, kehren die einzelnen Schnittstellenelemente der Bond-Schnittstelle zur unabhängigen Schnittstellenfunktionalität zurück. Eine Mitgliedsschnittstelle wird ausgewählt, um die Schnittstelleneinstellungen für die Bond-Schnittstelle beizubehalten, und alle anderen Mitgliedsschnittstellen sind deaktiviert. Wenn keine Mitgliedsoberfläche ausgewählt wird, um die Einstellungen beizubehalten, gehen die Einstellungen verloren und alle Mitgliedsoberflächen werden deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Abschnitt „Bond-Interfaces“, klicken Sie auf das rote **X** neben der Schnittstelle, die Sie zerstören möchten.
4. Auf dem Zerstöre die Bond-Schnittstelle < *Schnittstellennummer*> Wählen Sie auf dieser Seite die Mitgliedsoberfläche aus, auf die Sie die Einstellungen für die Bond-Schnittstelle verschieben möchten.

Nur die Mitglieds-Schnittstelle, die ausgewählt wurde, um die Bond-Schnittstelleneinstellungen beizubehalten, bleibt aktiv, und alle anderen Mitglieds-Schnittstellen sind deaktiviert.

5. Klicken Sie **Zerstören**.

Einstellungen für die Paketaufnahme

Sie können einen ExtraHop-Sensor so konfigurieren, dass er Pakete aus einem direkten Feed oder Pakete aufnimmt, die von einem Drittanbieter weitergeleitet wurden.

Bevor Sie beginnen

- Ihr Benutzerkonto muss volle Schreibrechte oder höher auf RevealX Enterprise oder System- und Zugriffsadministrationsrechte auf RevealX 360.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Einstellungen für die Paketaufnahme Abschnitt, wählen Sie eine der folgenden Optionen:

Option	Description
Pakete aus dem direkten Traffic-Feed aufnehmen	Nur verfügbar, wenn du mindestens eine Schnittstelle konfigurieren mit einem Modus, der GENEVE-Kapselung beinhaltet.
Von Netskope weitergeleitete Pakete aufnehmen	Nur verfügbar, wenn du mindestens eine Schnittstelle konfigurieren mit einem Modus, der GENEVE-Kapselung beinhaltet. Weitere Informationen finden Sie im Netskope-Integrationsleitfaden für RevealX Enterprise oder RevealX 360 um die Paket von Ihrer Netskope-Lösung aus zu konfigurieren.

4. Klicken Sie **Speichern**.

Flow-Netzwerke

Sie müssen die Netzwerkschnittstelle und die Porteinstellungen auf dem ExtraHop-System konfigurieren, bevor Sie NetFlow- oder sFlow-Daten aus Remote-Flow-Netzwerken (Flow-Exportern) sammeln können. Flow-Netzwerke können auf RevealX Enterprise-Systemen nicht konfiguriert werden. Das ExtraHop-System unterstützt die folgenden Flow-Technologien: Cisco NetFlow Version 5 (v5) und Version 9 (v9), AppFlow, IPFIX und sFlow.

Zusätzlich zur Konfiguration des ExtraHop-Systems müssen Sie Ihre Netzwerkgeräte so konfigurieren, dass sie sFlow- oder NetFlow-Verkehr senden. Schlagen Sie in der Dokumentation Ihres Anbieters nach oder sehen Sie sich ein Beispiel an Cisco-Konfigurationen im Anhang.

Erfassen Sie den Datenverkehr von NetFlow- und sFlow-Geräten

Sie müssen die Netzwerkschnittstelle und die Porteinstellungen auf dem ExtraHop-System konfigurieren, bevor Sie NetFlow- oder sFlow-Daten aus Remote-Flow-Netzwerken (Flow-Exportern) sammeln können. Flow-Netzwerke können auf RevealX Enterprise-Systemen nicht konfiguriert werden. Das ExtraHop-System unterstützt die folgenden Flow-Technologien: Cisco NetFlow v5 und v9, AppFlow, IPFIX und sFlow.

Hinweis: Informationen zur virtuellen EFC 1292v NetFlow-Sensor-Appliance finden Sie unter Stellen Sie den ExtraHop EFC 1292v NetFlow Sensor bereit.

Sie müssen sich als Benutzer anmelden mit System- und Zugriffsadministrationsrechte um die folgenden Schritte abzuschließen.

Konfigurieren Sie die Schnittstelle auf Ihrem ExtraHop-System

Zusätzlich zur Konfiguration des ExtraHop-Systems müssen Sie Ihre Netzwerkgeräte so konfigurieren, dass sie sFlow- oder NetFlow-Verkehr senden. Schlagen Sie in der Dokumentation Ihres Anbieters nach oder sehen Sie sich das Beispiel an Cisco-Konfigurationen am Ende dieses Dokuments. Beachten Sie, dass Cisco ASA-Firewalls mit NetFlow Secure Event Logging (NSEL) nicht unterstützt werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf den Namen der Schnittstelle , die die Flow-Daten erhalten soll.
4. Aus dem Schnittstellen-Modus Dropdownliste, wählen **Management + Flow-Ziel**.

   Hinweis: Der EDA 1100v muss entweder für Fluss- oder wire data konfiguriert werden, da dieser Sensor Fluss- und wire data nicht gleichzeitig verarbeiten kann. Wenn der Sensor für Durchflussdaten konfiguriert ist, müssen Sie den Überwachungsport auf einstellen **Deaktiviert**.
5. Wenn DHCPv4 aktivieren ist ausgewählt, klicken Sie **Speichern**.

   Andernfalls konfigurieren Sie die verbleibenden Netzwerkeinstellungen und klicken Sie dann auf **Speichern**.

Konfigurieren Sie den Flow-Typ und den UDP-Port

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Flow-Netzwerke**.
3. In der Häfen Abschnitt, in der Hafen Feld, geben Sie die UDP-Portnummer ein.

   Der Standardport für Net Flow ist `2055`, und der Standardport für sFlow ist `6343`. Sie können bei Bedarf weitere Ports für Ihre Umgebung hinzufügen.

   Hinweis: Die Portnummern müssen 1024 oder höher sein
4. Aus dem Durchflusstyp Dropdownliste, wählen **NetFlow** oder **sFlow**.

   Wählen Sie für AppFlow-Verkehr **NetFlow**.
5. Klicken Sie auf das Plus-Symbol (**+**), um den Port hinzuzufügen.
6. Speichern Sie die laufende Konfigurationsdatei, um Ihre Änderungen beizubehalten, indem Sie auf **Änderungen anzeigen und speichern** oben auf der Flow Networks-Seite.
7. Klicken Sie **Speichern**.

Fügen Sie die ausstehenden Flow-Netzwerke hinzu

Sie können jetzt ausstehende Flow-Netzwerke hinzufügen.

Bevor Sie beginnen

Sie müssen sich als Benutzer anmelden mit System- und Zugriffsadministrationsrechte um die folgenden Schritte abzuschließen.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Flow-Netzwerke**.
3. In der Ausstehende Flow-Netzwerke Abschnitt, klicken **Flow-Netzwerk hinzufügen**.
4. In der Flow-Netzwerk-ID Feld, geben Sie einen Namen ein, um dieses Flussnetz zu identifizieren.
5. Wählen Sie die **Automatische Aufzeichnungen** Kontrollkästchen, um Datensätze aus diesem Flussnetz an einen verbundenen Recordstore zu senden.
6. Wählen Sie die **SNMP-Polling aktivieren** Checkbox, um SNMP-Polling zu aktivieren.

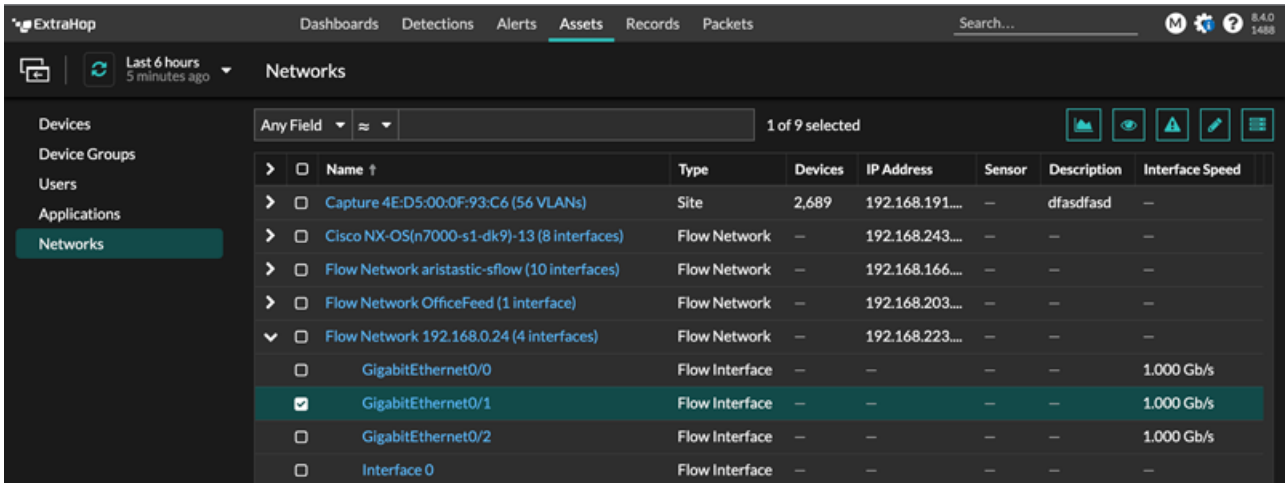
7. Wenn Sie SNMP-Polling aktivieren, wählen Sie eine der folgenden Optionen aus der Dropdownliste SNMP-Anmeldeinformationen aus:
   - **Von CIDR erben**. Wenn Sie diese Option auswählen, werden die SNMP-Anmeldeinformationen auf der Grundlage der Einstellungen für gemeinsame SNMP-Anmeldeinformationen angewendet.
   - **Benutzerdefinierte Anmeldedaten**. Wählen Sie v1, v2 oder v3 aus der Dropdownliste SNMP-Version aus, und konfigurieren Sie dann die verbleibenden Einstellungen für den spezifischen Abfragetyp.
8. Klicken Sie **Speichern**.

Das Flussnetz wird in der Tabelle Genehmigte Flussnetzwerke angezeigt. Wenn Sie das Flussnetz nicht sehen, können Sie es manuell hinzufügen, indem Sie auf **Flow-Netzwerk hinzufügen** in der Zugelassene Flow-Netzwerke Abschnitt und Vervollständigung der Informationen wie oben beschrieben.

Konfigurierte Flow-Netzwerke anzeigen
Nachdem Sie Ihre Flow-Netzwerke konfiguriert haben, melden Sie sich beim ExtraHop-System an, um die integrierten Diagramme anzusehen und Einstellungen und Konfigurationen zu ändern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Vermögenswerte**, und klicken Sie dann auf **Netzwerke**.
3. Klicken Sie auf den Dropdown-Pfeil neben dem Namen des Flussnetz, um eine Liste der Flow-Schnittstellen und ihrer Attribute anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen neben dem Namen des Flussnetz oder der Schnittstelle.

   In der oberen Leiste können Sie ein Diagramm erstellen, einen Auslöser zuweisen, eine Alarm zuweisen, die Flussschnittstelle umbenennen und die Schnittstellengeschwindigkeit festlegen.



Hinweis: Jeder NetFlow-Datensatz enthält den Schnittstellenindex (ifIndex) der Berichtsschnittstelle. Die Schnittstellentabelle (ifTable) wird dann vom ExtraHop-System abgefragt, um die Schnittstellengeschwindigkeit (ifSpeed) zu ermitteln.

5. Klicken Sie auf den Namen des Flussnetz oder die Flussschnittstelle, um die integrierten Diagramme auf den Übersichtsseiten anzuzeigen.

   Auf den Übersichtsseiten können Sie auf die Regionen und Diagramme klicken und sie einem neuen oder vorhandenen Dashboard hinzufügen.

Cisco NetFlow-Geräte konfigurieren

Die folgenden Beispiele für die grundlegende Cisco-Router-Konfiguration für NetFlow. NetFlow wird pro Schnittstelle konfiguriert. Wenn NetFlow auf der Schnittstelle konfiguriert ist, werden IP-Paketflussinformationen in das ExtraHop-System exportiert.

Wichtig: NetFlow nutzt den SNMP ifIndex-Wert, um Eingangs- und Ausgangsschnittstelleninformationen in Flow-Datensätzen darzustellen. Um die Konsistenz der Schnittstellenberichte zu gewährleisten, aktivieren Sie die SNMP ifIndex-Persistenz auf Geräten, die NetFlow an das ExtraHop-System senden. Weitere Informationen zur Aktivierung der SNMP ifIndex-Persistenz auf Ihren Netzwerkgeräten finden Sie in der vom Gerätehersteller bereitgestellten Konfigurationsanleitung.

Weitere Informationen zur Konfiguration von NetFlow auf Cisco Switches finden Sie in der Dokumentation zu Ihrem Cisco Router oder auf der Cisco-Website unter www.cisco.com.

Konfigurieren Sie einen Exporter auf dem Cisco Nexus-Switch
Definieren Sie einen Flow-Exporter, indem Sie das Exportformat, das Protokoll und das Ziel angeben.

1. Melden Sie sich bei der Switch-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.
2. Rufen Sie den globalen Konfigurationsmodus auf.

```
config t
```

3. Erstellen Sie einen Fluss Exporter und wechseln Sie in den Fluss Exporter-Konfigurationsmodus.

```
flow exporter <name>
```

Zum Beispiel:

```
flow exporter Netflow-Exporter-1
```

4. (Optional) Geben Sie eine Beschreibung ein.

```
description <string>
```

Zum Beispiel:

```
description Production-Netflow-Exporter
```

5. Legen Sie die IPv4- oder IPv6-Zieladresse für den Exporter fest.

```
destination <eda_mgmt_ip_address>
```

Zum Beispiel:

```
destination 192.168.11.2
```

6. Geben Sie die Schnittstelle an, die benötigt wird, um den NetFlow-Collector am konfigurierten Ziel zu erreichen.

```
source <interface_type> <number>
```

Zum Beispiel:

```
source ethernet 2/2
```

7. Geben Sie die NetFlow-Exportversion an.

```
version 9
```

Konfiguration von Cisco Switches über die Cisco IOS CLI

1. Melden Sie sich bei der Cisco IOS-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.

2. Rufen Sie den globalen Konfigurationsmodus auf.

```
config t
```

3. Geben Sie die Schnittstelle an, und wechseln Sie dann in den Schnittstellenkonfigurationsmodus.
   - Cisco Router der Serie 7500:

     ```
     interface <type> <slot>/<port-adapter>/<port>
     ```

     Zum Beispiel:

     ```
     interface fastethernet 0/1/0
     ```

   - Cisco Router der Serie 7200:

     ```
     interface <type> <slot>/<port>
     ```

     Zum Beispiel:

     ```
     interface fastethernet 0/1
     ```

4. Aktivieren Sie NetFlow.

```
ip route-cache flow
```

5. NetFlow-Statistiken exportieren, wobei *<ip-address>* ist die Management + Flow Target-Schnittstelle auf dem ExtraHop-System und *<udp-port>* ist die konfigurierte Collector-UDP-Portnummer.

```
ip flow-export <ip-address> <udp-port> version 5
```

Richten Sie gemeinsame SNMP-Anmeldeinformationen für Ihre NetFlow- oder sFlow-Netzwerke ein

Wenn Sie SNMP-Polling in Ihrer Flow-Netzwerkkonfiguration aktivieren, müssen Sie die Anmeldedaten angeben, mit denen Sie das Netzwerkgerät abfragen können. Die SNMP-Authentifizierungsdaten gelten für alle Flow-Netzwerke in einem CIDR-Block und werden automatisch auf jedes erkannte Flussnetz angewendet, sofern keine benutzerdefinierten Anmeldedaten konfiguriert sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Flow-Netzwerke**.
3. In der Geteilte SNMP-Anmeldeinformationen Abschnitt, klicken Sie **SNMP-Anmeldeinformationen hinzufügen**.
4. In der APFELWEIN Feld, geben Sie den IPv4-CIDR-Block ein.

   Geben Sie beispielsweise ein `10.0.0.0/8` um einer beliebigen IP-Adresse zu entsprechen , die mit 10 beginnt oder `10.10.0.0/16` um einer beliebigen IP-Adresse zu entsprechen, die mit 10.10 beginnt. Sie können keine IP-Adresse so konfigurieren, dass sie dem gesamten Datenverkehr entspricht.
5. Aus dem SNMP-Version Dropdownliste, wählen **v1**, **v2c**, oder **v3**.
6. Konfigurieren Sie zusätzliche Felder, die für die ausgewählte SNMP-Version spezifisch sind:
   - Wenn Sie v1 oder v2c ausgewählt haben, in der Gemeinschaftszeichenfolge Feld, geben Sie den Community-Namen ein.
   - Wenn Sie v3 ausgewählt haben, füllen Sie die folgenden Felder nach Bedarf aus:

     Name der Sicherheit

     Geben Sie den für die Authentifizierung bereitgestellten Benutzernamen ein. Dieses Feld ist erforderlich.

Sicherheitsstufe

Wählen Sie das SNMPv3-Sicherheitsmodell und die Sicherheitsstufe aus einer der folgenden Optionen aus:

- AuthPriv - Unterstützt einen SNMPv3-Benutzer mit Authentifizierung und Verschlüsselung
- AuthnoPriv - Unterstützt einen SNMPv3-Benutzer nur mit Authentifizierung und ohne Verschlüsselung
- NoAuthnoPriv — Unterstützt einen SNMPv3-Benutzer ohne Authentifizierung und Verschlüsselung

Art der Authentifizierung

Wählen Sie den Authentifizierungstyp aus einer der folgenden Optionen aus:

- MD5
- SHA

Authentifizierungsschlüssel

Geben Sie das Authentifizierungskennwort oder den Digest für den Benutzer ein.

Art des Datenschutzes

Wählen Sie den Datenverschlüsselungsstandard aus einer der folgenden Optionen aus:

- AES
- DES

Datenschutzschlüssel

Geben Sie den Verschlüsselungsschlüssel für den Benutzer ein.

7. Klicken Sie **Speichern**.

SNMP-Informationen manuell aktualisieren

Sie können Daten bei Bedarf vom SNMP-Agenten auf einem Flow-Netzwerkgerät abfragen und abrufen. Anstatt nach jeder Konfigurationsänderung auf die automatische Abfrage zu warten, um zu bestätigen, dass die Änderung korrekt ist (die automatische Abfrage erfolgt alle 24 Stunden), können Sie sofort eine Abfrage durchführen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie in der Spalte Aktionen für das genehmigte Flussnetz auf **Umfrage**.
   Das ExtraHop-System fragt nach den folgenden Informationen:
   - Der Systemname des SNMP-Agenten. Diese Kennung wird dem Flussnetz von SNMP zugewiesen. OID: `1.3.6.1.2.1.1.5.0`.
   - Der Schnittstellenname jeder Schnittstelle auf dem SNMP-Agenten. Diese Identifikatoren gelten für jede Flussschnittstelle im Flussnetz. OID: `1.3.6.1.2.1.2.2.1.2`.
   - Die Schnittstellengeschwindigkeit jeder Schnittstelle auf dem SNMP-Agenten. OID: `1.3.6.1.2.1.2.2.1.5` und `1.3.6.1.2.1.31.1.1.1.15`.

Benachrichtigungen

Das ExtraHop-System kann Benachrichtigungen über konfigurierte Warnmeldungen per E-Mail, SNMP-Traps und Syslog-Exporten an Remoteserver senden. Wenn eine E-Mail-Benachrichtigungsgruppe angegeben ist, werden E-Mails an die Gruppen gesendet, die der Alarm zugewiesen sind.

E-Mail-Einstellungen für Benachrichtigungen konfigurieren

Sie müssen einen E-Mail-Server und einen Absender konfigurieren, bevor das ExtraHop-System Warnmeldungen oder geplante Berichte senden kann.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Benachrichtigungen**.
3. Klicken Sie **E-Mail-Server und Absender**.
4. In der SMTP-Server Feld, geben Sie die IP-Adresse oder den Hostnamen für den SMTP-Postausgangsserver ein.

   Der SMTP-Server ist der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse eines Postausgangsservers, auf den vom ExtraHop-System aus zugegriffen werden kann. Wenn der DNS-Server eingerichtet ist, kann der SMTP-Server ein FQDN sein, andernfalls müssen Sie eine IP-Adresse eingeben.
5. In der SMTP-Anschluss Feld, geben Sie die Portnummer für die SMTP-Kommunikation ein.

   Port 25 ist der Standardwert für SMTP, und Port 465 ist der Standardwert für TLS-verschlüsseltes SMTP.
6. Aus dem Verschlüsselung Wählen Sie in der Dropdownliste eine der folgenden Verschlüsselungsmethoden aus:

   Keine

   Die SMTP-Kommunikation ist nicht verschlüsselt.

   TLS

   Die SMTP-Kommunikation wird über das Secure Socket Layer/Transport Layer Security-Protokoll verschlüsselt.

   STARTTLS

   Die SMTP-Kommunikation wird über STARTTLS verschlüsselt.
7. In der Adresse des Absenders der Warnung Feld, geben Sie die E-Mail-Adresse für den Absender der Benachrichtigung ein.

   Hinweis: Die angezeigte Absenderadresse wird möglicherweise vom SMTP-Server geändert. Wenn Sie beispielsweise über einen Google SMTP-Server senden, wird die Absender-E-Mail in den für die Authentifizierung angegebenen Benutzernamen geändert, anstatt in die ursprünglich eingegebene Absenderadresse.
8. Optional: Wählen Sie die SSL-Zertifikate validieren Kontrollkästchen, um die Zertifikatsvalidierung zu aktivieren.

   Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der Stammzertifikatsketten validiert, die vom Trusted Certificates Manager angegeben wurden. Beachten Sie, dass der in dem vom SMTP-Server vorgelegten Zertifikat angegebene Hostname mit dem in Ihrer SMTP-Konfiguration angegebenen Hostnamen übereinstimmen muss. Andernfalls schlägt die Überprüfung fehl. Darüber hinaus müssen Sie auf der Seite Vertrauenswürdige Zertifikate konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.
9. In der Absenderadresse melden In diesem Feld geben Sie die E-Mail-Adresse ein, die für den Versand der Nachricht verantwortlich ist.

   Dieses Feld gilt nur, wenn geplante Berichte von einer ExtraHop-Konsole oder RevealX 360 aus gesendet werden.
10. Wählen Sie die **SMTP-Authentifizierung aktivieren** Ankreuzfeld.
11. In der Nutzername und Passwort Felder, geben Sie die Anmeldeinformationen für das SMTP-Server-Setup ein.
12. Optional: Klicken Sie **Einstellungen testen**, geben Sie Ihre E-Mail-Adresse ein, und klicken Sie dann auf **Senden**.

    Sie sollten eine E-Mail-Nachricht mit dem Betreff erhalten `ExtraHop Test Email`.
13. Klicken Sie **Speichern**.

Nächste Schritte

Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, speichern Sie Ihre Konfigurationsänderungen durch Systemneustart- und Shutdown-Ereignisse, indem Sie die laufende Konfigurationsdatei speichern.

Konfigurieren Sie eine E-Mail-Benachrichtigungsgruppe

Fügen Sie einer Gruppe eine Liste mit E-Mail-Adressen hinzu und wählen Sie dann die Gruppe aus, wenn Sie die E-Mail-Einstellungen für eine Alarm oder einen geplanten Bericht konfigurieren. Sie können zwar einzelne E-Mail-Adressen angeben, E-Mail-Gruppen sind jedoch eine effektive Methode, um Ihre Empfängerliste zu verwalten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Benachrichtigungen**.
3. klicken **E-Mail-Benachrichtigungsgruppen**.
4. klicken **Gruppe hinzufügen**.
5. In der Informationen zur Gruppe Abschnitt, konfigurieren Sie die folgenden Informationen:

   • **Name:** Geben Sie einen Namen für die E-Mail-Gruppe ein.

   • **Benachrichtigungen zum Systemstatus:** Wählen Sie dieses Kontrollkästchen, wenn die E-Mail-Gruppe Systemwarnungen erhalten soll, die unter folgenden Bedingungen generiert werden:

   - Ein virtuelles Laufwerk befindet sich in einem heruntergekommenen Zustand.
   - Eine physische Festplatte befindet sich in einem heruntergefahrenen Zustand oder weist eine steigende Fehleranzahl auf.
   - Eine erforderliche Festplattenpartition für Firmware-, Datenspeicher- oder Paketerfassungsdaten fehlt.
   - Ein Gerät konnte sich nicht wieder mit ExtraHop Cloud Services verbinden.
   - Eine Lizenz ist abgelaufen oder läuft bald ab.
   - Ein Backup für Anpassungen und Ressourcen ist fehlgeschlagen.
6. In der E-Mail-Adressen Textfeld, geben Sie die Empfänger-E-Mail-Adressen ein, die die an diese Gruppe gesendeten E-Mails erhalten sollen. E-Mail-Adressen können eine pro Zeile eingegeben oder durch ein Komma, Semikolon oder Leerzeichen getrennt werden. E-Mail-Adressen werden nur überprüft für [*Name*] @ [*firma*] . [*Domäne*] Formatüberprüfung. Dieses Textfeld muss mindestens eine E-Mail-Adresse enthalten, damit die Gruppe gültig ist.
7. Klicken Sie **Speichern**.

Konfigurieren Sie die Einstellungen, um Benachrichtigungen an einen SNMP-Manager zu senden

Der Zustand des Netzwerk kann über das Simple Network Management Protocol (SNMP) überwacht werden. SNMP sammelt Informationen, indem es Geräte im Netzwerk abfragt. SNMP-fähige Geräte können auch Warnmeldungen an SNMP-Managementstationen senden. SNMP-Communities definieren die Gruppe , zu der Geräte und Verwaltungsstationen, auf denen SNMP ausgeführt wird, gehören, was angibt, wohin Informationen gesendet werden. Der Community-Name identifiziert die Gruppe.

Hinweis: Die meisten Organisationen verfügen über ein etabliertes System zur Erfassung und Anzeige von SNMP-Traps an einem zentralen Ort, der von ihren Betriebsteams überwacht werden kann. Beispielsweise werden SNMP-Traps an einen SNMP-Manager gesendet, und die SNMP-Managementkonsole zeigt sie an.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Benachrichtigungen**.
3. Unter Benachrichtigungen, klicken **SNMP**.

4. Auf dem SNMP-Einstellungen Seite, in der **SNMP-Monitor** Feld, geben Sie den Hostnamen für den SNMP-Trap-Empfänger ein.

   Trennen Sie mehrere Hostnamen durch Kommas.
5. In der **SNMP-Gemeinschaft** Feld, geben Sie den SNMP-Community-Namen ein.
6. In der **SNMP-Anschluss** Geben Sie in dieses Feld die SNMP-Portnummer für Ihr Netzwerk ein, die vom SNMP-Agent verwendet wird, um auf den Quellport im SNMP-Manager zu antworten.

   Der Standard-Antwortport ist `162`.
7. Optional: klicken **Einstellungen testen** um zu überprüfen, ob Ihre SNMP-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollten Sie in der SNMP-Protokolldatei auf dem SNMP-Server einen Eintrag sehen, der diesem Beispiel ähnelt, wobei `192.0.2.0` ist die IP-Adresse Ihres ExtraHop-Systems und `192.0.2.255` ist die IP-Adresse des SNMP-Servers:

   Eine ähnliche Antwort wie in diesem Beispiel wird angezeigt:

   ```
   Connection from UDP: [192.0.2.0]:42164->[ 192.0.2.255]:162
   ```
8. Klicken Sie **Speichern**.

Laden Sie die ExtraHop SNMP MIB herunter
SNMP stellt keine Datenbank mit Informationen bereit, die ein SNMP-überwachtes Netzwerk meldet. SNMP-Informationen werden durch MIBs (Management Information Bases) von Drittanbietern definiert, die die Struktur der gesammelten Daten beschreiben.

Sie können die ExtraHop MIB-Datei aus den Administrationseinstellungen des Systems herunterladen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Gehe zum Netzwerkeinstellungen Abschnitt und klick **Benachrichtigungen**.
3. Unter Benachrichtigungen, klicken **SNMP**.
4. Unter SNMP MIB, klicken Sie auf **ExtraHop SNMP MIB herunterladen**.
   Die Datei wird normalerweise am Standardspeicherort für den Download Ihres Browsers gespeichert.

Extrahieren Sie die ExtraHop-Lieferantenobjekt-OID
Bevor Sie ein Gerät mit SNMP überwachen können, benötigen Sie den `Sysobject-ID`, das eine OID enthält, bei der es sich um die vom Hersteller gemeldete Identität des Gerät handelt.

Die SNMP Vendor Object ID (OID) für das ExtraHop-System lautet iso.3.6.1.4.1.32015. Sie können diesen Wert auch extrahieren mit `snmpwalk`.

1. Melden Sie sich an der Befehlszeilenschnittstelle auf Ihrer Management-Workstation an.
2. Extrahieren Sie die OID, wobei *ip-adresse* ist die IP-Adresse für Ihr ExtraHop-System:
   In diesem Beispiel fragen Sie mit `Sysobject-ID`:

   ```
   snmpwalk -v 2c -c öffentlich < ip-adresse> SNMPv2-MIB: :SysobjectID
   ```

   Eine Antwort ähnlich diesem Beispiel zeigt:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015
   ```

   In diesem Beispiel fragen Sie mit der OID ab:

   ```
   snmpwalk -v 2c -c öffentlich < ip-adresse> 1.3.6.1.2.1.1.2
   ```

   Eine Antwort ähnlich diesem Beispiel zeigt:

   ```
   SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.32015
   ```

Systembenachrichtigungen an einen Remote-Syslog-Server senden

Mit der Syslog-Exportoption können Sie Warnmeldungen von einem ExtraHop-System an jedes Remote-System senden, das Syslog-Eingaben zur Langzeitarchivierung und Korrelation mit anderen Quellen empfängt.

Für jedes ExtraHop-System kann nur ein Remote-Syslog-Server konfiguriert werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Benachrichtigungen**.
3. In der Reiseziel Feld, geben Sie die IP-Adresse des Remote-Syslog-Servers ein.
4. Aus dem **Protokoll** Dropdownliste, wählen **TCP** oder **UDP**.

   Diese Option gibt das Protokoll an, über das die Informationen an Ihren Remote-Syslog-Server gesendet werden.
5. In der Hafen In diesem Feld geben Sie die Portnummer für Ihren Remote-Syslog-Server ein.

   Der Standardwert ist 514.
6. Klicken Sie **Einstellungen testen** um zu überprüfen, ob Ihre Syslog-Einstellungen korrekt sind.

   Wenn die Einstellungen korrekt sind, sollte in der Syslog-Logdatei auf dem Syslog-Server ein Eintrag ähnlich dem folgenden angezeigt werden:

   ```
   Jul 27 21:54:56 extrahop name="ExtraHop Test" event_id=1
   ```
7. Klicken Sie **Speichern**.
8. Optional: Ändern Sie das Format von Syslog-Meldungen.

   Standardmäßig sind Syslog-Meldungen nicht mit RFC 3164 oder RFC 5424 kompatibel. Sie können Syslog-Meldungen jedoch so formatieren, dass sie konform sind, indem Sie die laufende Konfigurationsdatei ändern.
   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie einen Eintrag hinzu unter `syslog_notification`, wo der Schlüssel ist `rfc_compliant_format` und der Wert ist entweder `rfc5424` oder `rfc3164`.

      Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

      ```
      "syslog_notification": {
          "syslog_destination": "192.168.0.0",
          "syslog_ipproto": "udp",
          "syslog_port": 514,
          "rfc_compliant_format": "rfc5424"
      }
      ```
   e) Klicken Sie **Aktualisieren**.
   f) Klicken Sie **Erledigt**.
9. Optional: Ändern Sie die Zeitzone, auf die in den Syslog-Zeitstempeln verwiesen wird.

   Standardmäßig verweisen Syslog-Zeitstempel auf die UTC-Zeit. Sie können Zeitstempel jedoch so ändern, dass sie auf die ExtraHop-Systemzeit verweisen, indem Sie die laufende Konfigurationsdatei ändern.
   a) Klicken Sie **Admin**.
   b) Klicken Sie **Config ausführen (ungespeicherte Änderungen)**.
   c) Klicken Sie **Konfiguration bearbeiten**.
   d) Fügen Sie einen Eintrag hinzu unter `syslog_notification` wo der Schlüssel ist `syslog_use_localtime` und der Wert ist `true`.

Das `syslog_notification` Der Abschnitt sollte dem folgenden Code ähneln:

```
    "syslog_notification": {
        "syslog_destination": "192.168.0.0",
        "syslog_ipproto": "udp",
        "syslog_port": 514,
        "syslog_use_localtime": true
    }
```

e) Klicken Sie **Aktualisieren**.
f) Klicken Sie **Erledigt**.

Nächste Schritte
Nachdem Sie bestätigt haben, dass Ihre neuen Einstellungen erwartungsgemäß funktionieren, speichern Sie Ihre Konfigurationsänderungen durch Systemneustart- und Shutdown-Ereignisse, indem Sie die laufende Konfigurationsdatei speichern.

TLS-Zertifikat

TLS-Zertifikate bieten eine sichere Authentifizierung für das ExtraHop-System.

Sie können ein selbstsigniertes Zertifikat für die Authentifizierung anstelle eines von einer Zertifizierungsstelle signierten Zertifikats angeben. Beachten Sie jedoch, dass ein selbstsigniertes Zertifikat einen Fehler in der Client Browser, der meldet, dass die signierende Zertifizierungsstelle unbekannt ist. Der Browser stellt eine Reihe von Bestätigungsseiten bereit, um dem Zertifikat zu vertrauen, auch wenn das Zertifikat selbst signiert ist. Selbstsignierte Zertifikate können auch die Leistung beeinträchtigen, da sie das Zwischenspeichern in einigen Browsern verhindern. Wir empfehlen Ihnen, eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System aus zu erstellen und stattdessen das signierte Zertifikat hochzuladen.

Wichtig: Beim Ersetzen eines TLS-Zertifikats wird der Webserverdienst neu gestartet. Die getunnelten Verbindungen von ExtraHop-Sensoren zu den ExtraHop-Konsolen gehen verloren, werden dann aber automatisch wiederhergestellt.

Laden Sie ein TLS-Zertifikat hoch

Sie müssen eine PEM-Datei hochladen, die sowohl einen privaten Schlüssel als auch entweder ein selbstsigniertes Zertifikat oder ein Zertifikat einer Zertifizierungsstelle enthält.

Hinweis: Die PEM-Datei darf nicht passwortgeschützt sein.

Hinweis: Du kannst auch automatisiere diese Aufgabe über die REST-API.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** um den Abschnitt zu erweitern.
4. Klicken Sie **Wählen Sie Datei** und navigieren Sie zu dem Zertifikat, das Sie hochladen möchten.
5. Klicken Sie **Offen**.
6. Klicken Sie **Upload**.
7. Speichern Sie die laufende Konfigurationsdatei

Generieren Sie ein selbstsigniertes Zertifikat

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **TLS-Zertifikat**.

3. Klicken Sie **Zertifikate verwalten** um den Abschnitt zu erweitern.
4. Klicken Sie **Erstellen Sie ein selbstsigniertes SSL-Zertifikat basierend auf dem Hostnamen** .
5. Auf dem Zertifikat generieren Seite, klicken **OK** um das selbstsignierte TLS-Zertifikat zu generieren.

   Hinweis: Der Standard-Hostname ist `extrahop`.

6. Speichern Sie die laufende Konfigurationsdatei

Erstellen Sie eine Anfrage zur Zertifikatsignierung von Ihrem ExtraHop-System

Eine Certificate Signing Request (CSR) ist ein verschlüsselter Textblock, der Ihrer Zertifizierungsstelle (CA) zur Verfügung gestellt wird, wenn Sie ein TLS-Zertifikat beantragen. Die CSR wird auf dem ExtraHop-System generiert, auf dem das TLS-Zertifikat installiert wird, und enthält Informationen , die in das Zertifikat aufgenommen werden, wie z. B. den allgemeinen Namen (Domänenname), die Organisation, den Ort und das Land. Die CSR enthält auch den öffentlichen Schlüssel, der im Zertifikat enthalten sein wird. Die CSR wird mit dem privaten Schlüssel aus dem ExtraHop-System erstellt, wodurch ein Schlüsselpaar entsteht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken **TLS-Zertifikat**.
3. Klicken Sie **Zertifikate verwalten** und klicken Sie dann **Eine Zertifikatsignieranforderung (CSR) exportieren**.
4. In der Betreff Alternative Namen Abschnitt, geben Sie den DNS-Namen des ExtraHop-Systems ein.

   Sie können mehrere DNS-Namen und IP-Adressen hinzufügen, die durch ein einziges TLS-Zertifikat geschützt werden sollen.
5. In der Betreff Abschnitt, füllen Sie die folgenden Felder aus.

   Nur die **Allgemeiner Name** Feld ist erforderlich.

Feld	Beschreibung	Beispiele
Allgemeiner Name	Der vollqualifizierte Domänenname (FQDN) des ExtraHop-Systems . Der FQDN muss mit einem der alternativen Betreffnamen übereinstimmen.	*.example.com discover.example.com
E-mail-Adresse	Die E-Mail-Adresse des Hauptansprechpartners für Ihre Organisation.	webmaster@example.com
Organisatorische Einheit	Die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.	IT-Abteilung
Organisation	Der offizielle Name Ihrer Organisation. Dieser Eintrag darf nicht abgekürzt werden und sollte Suffixe wie Inc, Corp oder LLC enthalten.	Beispiel, Inc.
Ort/Stadt	Die Stadt, in der sich Ihre Organisation befindet.	Seattle
Bundesstaat/Provinz	Das Bundesland oder die Provinz, in der sich Ihre Organisation befindet. Dieser Eintrag sollte nicht abgekürzt werden.	Washington

Feld	Beschreibung	Beispiele
Landeskennzahl	Der zweibuchstabige ISO-Code für das Land, in dem sich Ihre Organisation befindet.	UNS

6. Klicken Sie **Exportieren**.
   Die CSR-Datei wird automatisch auf Ihren Computer heruntergeladen.

Nächste Schritte
Senden Sie die CSR-Datei an Ihre Zertifizierungsstelle (CA), um die CSR signieren zu lassen. Wenn Sie das TLS-Zertifikat von der CA erhalten haben, kehren Sie zur TLS-Zertifikat Seite in den Administrationseinstellungen und laden Sie das Zertifikat in das ExtraHop-System hoch.

Hinweis: Wenn Ihre Organisation verlangt, dass der CSR einen neuen öffentlichen Schlüssel enthält, ein selbstsigniertes Zertifikat generieren um neue Schlüsselpaare zu erstellen, bevor die CSR erstellt wird.

Vertrauenswürdige Zertifikate

Mit vertrauenswürdigen Zertifikaten können Sie SMTP-, LDAP-, HTTPS- ODS- und MongoDB-ODS-Ziele sowie Splunk-Recordstore-Verbindungen von Ihrem ExtraHop-System aus validieren.

Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu

Ihr ExtraHop-System vertraut nur Peers, die ein Transport Layer Security (TLS) -Zertifikat vorlegen, das von einem der integrierten Systemzertifikate und allen von Ihnen hochgeladenen Zertifikaten signiert ist. SMTP-, LDAP-, HTTPS-ODS- und MongoDB-ODS-Ziele sowie Splunk-Recordstore-Verbindungen können mithilfe dieser Zertifikate validiert werden.

Bevor Sie beginnen
Sie müssen sich als Benutzer mit Setup- oder Systemberechtigungen anmelden und auf Administratorrechte zugreifen , um vertrauenswürdige Zertifikate hinzuzufügen oder zu entfernen.

Beim Hochladen eines benutzerdefinierten vertrauenswürdigen Zertifikats muss ein gültiger Vertrauenspfad vom hochgeladenen Zertifikat zu einem vertrauenswürdigen, selbstsignierten Stammzertifikat existieren, damit das Zertifikat vollständig vertrauenswürdig ist. Laden Sie entweder die gesamte Zertifikatskette für jedes vertrauenswürdige Zertifikat hoch oder stellen Sie (vorzugsweise) sicher, dass jedes Zertifikat in der Kette in das System für vertrauenswürdige Zertifikate hochgeladen wurde.

Wichtig: Um den integrierten Systemzertifikaten und allen hochgeladenen Zertifikaten zu vertrauen, müssen Sie bei der Konfiguration der Einstellungen für den externen Server auch die TLS- oder STARTTLS-Verschlüsselung und die Zertifikatsvalidierung aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Netzwerkeinstellungen Abschnitt, klicken Sie **Vertrauenswürdige Zertifikate**.
3. Optional: Wenn Sie den im ExtraHop-System enthaltenen integrierten Zertifikaten vertrauen möchten, wählen Sie **Vertrauenssystem-Zertifikate**, klicken **Speichern**, und dann speichern Sie die laufende Konfigurationsdatei.
4. Um Ihr eigenes Zertifikat hinzuzufügen, klicken Sie auf **Zertifikat hinzufügen** und dann in der Zertifikat Feld, fügen Sie den Inhalt der PEM-kodierten Zertifikatskette ein.
5. In der Name Feld, geben Sie einen Namen ein.
6. Klicken Sie **Hinzufügen**.

Auf Einstellungen zugreifen

In der Auf Einstellungen zugreifen In diesem Abschnitt können Sie Benutzerkennwörter ändern, das Support-Konto aktivieren, lokale Benutzer und Benutzergruppen verwalten, die Fernauthentifizierung konfigurieren und den API-Zugriff verwalten.

Globale Richtlinien

Administratoren können globale Richtlinien konfigurieren, die für alle Benutzer gelten, die auf das System zugreifen.

Passwort-Richtlinie

- Wählen Sie zwischen zwei Passwortrichtlinien: der standardmäßigen Passwortrichtlinie mit 5 oder mehr Zeichen oder einer strengeren Passwortrichtlinie mit den folgenden Einschränkungen:
  - 8 oder mehr Zeichen
  - Groß- und Kleinbuchstaben
  - Mindestens eine Zahl
  - Mindestens ein Symbol

  Hinweis: Wenn Sie die strikte Passwortrichtlinie mit 8 oder mehr Zeichen wählen, laufen Passwörter alle 60 Tage ab.

Steuerung zum Bearbeiten von Gerätegruppen

- Steuern Sie, ob Benutzer mit eingeschränkte Schreibrechte kann Gerätegruppen erstellen und bearbeiten. Wenn diese Richtlinie ausgewählt ist, können alle Benutzer mit eingeschränktem Schreibzugriff Gerätegruppen erstellen und andere Benutzer mit eingeschränktem Schreibzugriff als Redakteure zu ihren Gerätegruppen hinzufügen.

Standard-Dashboard

- Geben Sie das Dashboard an, das Benutzer sehen, wenn sie sich am System anmelden. Nur Dashboards, die mit allen Benutzern geteilt werden, können als globaler Standard festgelegt werden. Benutzer können diese Standardeinstellung überschreiben. über das Befehlsmenü eines beliebigen Dashboard.

Passwort für Dateiextraktion

- (Nur NDR-Modul) Geben Sie ein erforderliches Passwort an, das Sie mit zugelassenen Benutzern zum Entpacken teilen können Dateien, die aus einer Paketabfrage extrahiert und heruntergeladen wurden.

Passwörter

Benutzer mit Rechten für die Administrationsseite können das Passwort für lokale Benutzerkonten ändern.

- Wählen Sie einen beliebigen Benutzer aus und ändern Sie sein Passwort
  - Sie können nur Passwörter für lokale Benutzer ändern. Sie können die Passwörter für Benutzer, die über LDAP oder andere Remote-Authentifizierungsserver authentifiziert wurden, nicht ändern.

Weitere Informationen zu Rechten für bestimmte Benutzer und Gruppen der Administrationsseite finden Sie in der Nutzer Abschnitt.

Ändern Sie das Standardkennwort für den Setup-Benutzer

Es wird empfohlen, das Standardkennwort für den Setup-Benutzer auf dem ExtraHop-System zu ändern, nachdem Sie sich zum ersten Mal angemeldet haben. Um Administratoren daran zu erinnern, diese Änderung vorzunehmen, gibt es ein blaues **Passwort ändern** Schaltfläche oben auf der Seite, während der Setup-Benutzer auf die Administrationseinstellungen zugreift. Nachdem das Setup-Benutzerkennwort geändert wurde, wird die Schaltfläche oben auf der Seite nicht mehr angezeigt.

Hinweis: Das Passwort muss mindestens 5 Zeichen lang sein.

1. In der Administrationseinstellungen, klicken Sie auf das blaue **Standardpasswort ändern** knopf. Die Passwortseite wird ohne die Dropdownliste für Konten angezeigt. Das Passwort ändert sich nur für den Setup-Benutzer.
2. In der Altes Passwort Feld, geben Sie das Standardkennwort ein.
3. In der Neues Passwort Feld, geben Sie das neue Passwort ein.
4. In der Bestätigen Sie das Passwort Feld, geben Sie das neue Passwort erneut ein.
5. Klicken Sie **Speichern**.

Zugang zum Support

Support-Konten bieten dem ExtraHop-Supportteam Zugriff, um Kunden bei der Behebung von Problemen mit dem ExtraHop-System zu unterstützen.

Diese Einstellungen sollten nur aktiviert werden, wenn der ExtraHop-Systemadministrator das ExtraHop-Supportteam um praktische Unterstützung bittet.

SSH-Schlüssel generieren

Generieren Sie einen SSH-Schlüssel, damit ExtraHop Support eine Verbindung zu Ihrem ExtraHop-System herstellen kann, wenn Fernzugriff wird konfiguriert durch ExtraHop Cloud-Dienste .

1. In der Auf Einstellungen zugreifen Abschnitt, klicken **Zugriff auf den Support**.
2. klicken **SSH-Schlüssel generieren**.
3. Kopieren Sie den verschlüsselten Schlüssel aus dem Textfeld und senden Sie den Schlüssel per E-Mail an Ihren ExtraHop-Vertreter.
4. Klicken Sie **Erledigt**.

Den SSH-Schlüssel neu generieren oder widerrufen

Um den SSH-Zugriff auf das ExtraHop-System mit einem vorhandenen SSH-Schlüssel zu verhindern, können Sie den aktuellen SSH-Schlüssel widerrufen. Ein neuer SSH-Schlüssel kann bei Bedarf auch neu generiert werden.

1. In der Zugriffs-Einstellungen Abschnitt, klicken **Zugang zum Support**.
2. klicken **SSH-Schlüssel generieren**.
3. Wählen Sie eine der folgenden Optionen:
   - klicken **SSH-Schlüssel neu generieren** und dann klicken **Regenerieren**.

     Kopieren Sie den verschlüsselten Schlüssel aus dem Textfeld und senden Sie den Schlüssel per E-Mail an Ihren ExtraHop-Ansprechpartner. Klicken Sie dann auf **Erledigt**.
   - klicken **SSH-Schlüssel widerrufen** um den SSH-Zugriff auf das System mit dem aktuellen Schlüssel zu verhindern.

Nutzer

Auf der Seite Benutzer können Sie den lokalen Zugriff auf die ExtraHop-Appliance steuern.

Benutzer und Benutzergruppen

Benutzer können auf drei Arten auf das ExtraHop-System zugreifen: über eine Reihe vorkonfigurierter Benutzerkonten, über lokale Benutzerkonten, die auf der Appliance konfiguriert sind, oder über Remote-Benutzerkonten, die auf vorhandenen Authentifizierungsservern wie LDAP, SAML, Radius und TACACS+ konfiguriert sind.

Video: Sehen Sie sich die entsprechenden Schulungen an:

- Benutzerverwaltung
- Benutzergruppen

Lokale Benutzer

In diesem Thema geht es um Standard- und lokale Konten. siehe Fernauthentifizierung um zu lernen, wie man Remote-Konten konfiguriert.

Die folgenden Konten sind standardmäßig auf ExtraHop-Systemen konfiguriert, erscheinen jedoch nicht in der Namensliste auf der Benutzerseite. Diese Konten können nicht gelöscht werden und Sie müssen das Standardkennwort bei der ersten Anmeldung ändern.

Einrichten

Dieses Konto bietet volle System-Lese- und Schreibrechte für die browserbasierte Benutzeroberfläche und die ExtraHop-Befehlszeilenschnittstelle (CLI). Auf physischem Sensoren, das Standardkennwort für dieses Konto ist die Service-Tag-Nummer auf der Vorderseite der Appliance. Auf virtuellem Sensoren, das Standardpasswort ist `default`.

Schale

Die `shell` Das Konto hat standardmäßig Zugriff auf nicht administrative Shell-Befehle in der ExtraHop-CLI. Bei physischen Sensoren ist das Standardkennwort für dieses Konto die Service-Tag-Nummer auf der Vorderseite der Appliance. Bei virtuellen Sensoren lautet das Standardkennwort `default`.

Hinweis: Das standardmäßige ExtraHop-Passwort für eines der Konten, wenn es in Amazon Web Services (AWS) und Google Cloud Platform (GCP) bereitgestellt wird, ist die Instanz-ID der virtuellen Maschine.

Nächste Schritte

- Fügen Sie ein lokales Benutzerkonto hinzu

Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Remoteauthentifizierung können Unternehmen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einem Teil ihrer Benutzer die Möglichkeit geben, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation von Benutzerkennwörtern.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung von ExtraHop-Privilegien auf der Grundlage von Benutzergruppen.
- Administratoren können allen bekannten Benutzern Zugriff gewähren oder den Zugriff einschränken, indem sie LDAP-Filter anwenden.

Nächste Schritte

- Konfigurieren Sie die Fernauthentifizierung über LDAP

- Konfigurieren Sie die Remote-Authentifizierung über SAML
- Konfigurieren Sie die Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Fernauthentifizierung über RADIUS

Entfernte Benutzer
Wenn Ihr ExtraHop-System für die SAML- oder LDAP-Fernauthentifizierung konfiguriert ist, können Sie ein Konto für diese Remote-Benutzer erstellen. Durch die Vorkonfiguration von Konten auf dem ExtraHop-System für Remote-Benutzer können Sie Systemanpassungen mit diesen Benutzern teilen, bevor sie sich anmelden.

Wenn Sie sich bei der Konfiguration der SAML-Authentifizierung für die automatische Bereitstellung von Benutzern entscheiden, wird der Benutzer bei der ersten Anmeldung automatisch zur Liste der lokalen Benutzer hinzugefügt. Sie können jedoch ein SAML-Remotebenutzerkonto auf dem ExtraHop-System erstellen, wenn Sie einen Remote-Benutzer bereitstellen möchten, bevor sich dieser Benutzer am System angemeldet hat. Rechte werden dem Benutzer vom Anbieter zugewiesen. Nachdem der Benutzer erstellt wurde, können Sie ihn zu lokalen Benutzergruppen hinzufügen.

Nächste Schritte

- Konto für einen Remote-Benutzer hinzufügen

Benutzergruppen
Benutzergruppen ermöglichen es Ihnen, den Zugriff auf gemeinsam genutzte Inhalte nach Gruppen statt nach einzelnen Benutzern zu verwalten. Benutzerdefinierte Objekte wie Activity Maps können mit einer Benutzergruppe geteilt werden, und jeder Benutzer, der der Gruppe hinzugefügt wird, hat automatisch Zugriff. Sie können eine lokale Benutzergruppe erstellen, die Remote- und lokale Benutzer umfassen kann. Wenn Ihr ExtraHop-System für die Fernauthentifizierung über LDAP konfiguriert ist, können Sie alternativ Einstellungen für den Import Ihrer LDAP-Benutzergruppen konfigurieren.

- klicken **Benutzergruppe erstellen** um eine lokale Gruppe zu erstellen. Die Benutzergruppe wird in der Liste angezeigt. Aktivieren Sie dann das Kontrollkästchen neben dem Namen der Benutzergruppe und wählen Sie Benutzer aus der **Benutzer filtern...** Drop-down-Liste. klicken **Benutzer zur Gruppe hinzufügen**.
- (nur LDAP) Klicken Sie **Alle Benutzergruppen aktualisieren** oder wählen Sie mehrere LDAP-Benutzergruppen aus und klicken Sie auf **Benutzer in Gruppen aktualisieren**.
- klicken **Benutzergruppe zurücksetzen** um alle geteilten Inhalte aus einer ausgewählten Benutzergruppe zu entfernen. Wenn die Gruppe auf dem Remote-LDAP-Server nicht mehr existiert, wird die Gruppe aus der Benutzergruppenliste entfernt.
- klicken **Benutzergruppe aktivieren** oder **Benutzergruppe deaktivieren** um zu kontrollieren, ob ein Gruppenmitglied auf geteilte Inhalte für die ausgewählte Benutzergruppe zugreifen kann.
- klicken **Benutzergruppe löschen** um die ausgewählte Benutzergruppe aus dem System zu entfernen.
- Sehen Sie sich die folgenden Eigenschaften für aufgelistete Benutzergruppen an:

  Name der Gruppe

  Zeigt den Namen der Gruppe an. Um die Mitglieder der Gruppe anzuzeigen, klicken Sie auf den Gruppennamen.

  Typ

  Zeigt Lokal oder Remote als Art der Benutzergruppe an.

  Mitglieder

  Zeigt die Anzahl der Benutzer in der Gruppe an.

  Geteilter Inhalt

  Zeigt die Anzahl der vom Benutzer erstellten Objekte an, die mit der Gruppe gemeinsam genutzt werden.

  Status

  Zeigt an, ob die Gruppe auf dem System aktiviert oder deaktiviert ist. Wenn der Status ist `Disabled`, wird die Benutzergruppe bei der Durchführung von Mitgliedschaftsprüfungen als

leer betrachtet. Die Benutzergruppe kann jedoch weiterhin angegeben werden, wenn Inhalte geteilt werden.

Mitglieder aktualisiert (nur LDAP)

Zeigt die Zeit an, die seit der Aktualisierung der Gruppenmitgliedschaft vergangen ist. Benutzergruppen werden unter den folgenden Bedingungen aktualisiert:

- Standardmäßig einmal pro Stunde. Die Einstellung für das Aktualisierungsintervall kann auf der **Fernauthentifizierung** > **LDAP-Einstellungen** Seite.
- Ein Administrator aktualisiert eine Gruppe, indem er auf **Alle Benutzergruppen aktualisieren** oder **Benutzer in der Gruppe aktualisieren**, oder programmgesteuert über die REST-API. Sie können eine Gruppe aktualisieren über Benutzergruppe Seite oder aus dem Liste der Mitglieder Seite.
- Ein Remote-Benutzer meldet sich zum ersten Mal beim ExtraHop-System an.
- Ein Benutzer versucht, ein geteiltes Dashboard zu laden, auf das er keinen Zugriff hat.

Benutzerrechte
Administratoren bestimmen die Modulzugriffsebene für Benutzer im ExtraHop-System.

Informationen zu Benutzerberechtigungen für die REST-API finden Sie in der REST-API-Leitfaden.

Informationen zu Remote-Benutzerrechten finden Sie in den Konfigurationsanleitungen für LDAP, RADIUS, SAML, und TACACS+.

Privilegienstufen
Legen Sie die Berechtigungsstufe fest, auf die Ihr Benutzer zugreifen kann, um zu bestimmen, auf welche Bereiche des ExtraHop-Systems er zugreifen kann.

Zugriffsrechte für Module

Diese Rechte bestimmen die Funktionen, auf die Benutzer im ExtraHop-System zugreifen können. Administratoren können die rollenbasierte Zugriffskontrolle (RBAC) aktivieren, indem sie Benutzern Zugriff auf eines oder alle der Module Network Detection and Response (NDR), Network Performance and Monitoring (NPM) und Packet Forensics gewähren. Für den Zugriff auf Modulfunktionen ist eine Modullizenz erforderlich.

Zugriff auf das NDR-Modul

Ermöglicht dem Benutzer den Zugriff auf Sicherheitsfunktionen wie Angriffserkennungen, Untersuchungen und Bedrohungsinformationen.

Zugriff auf das NPM-Modul

Ermöglicht dem Benutzer den Zugriff auf Leistungsfunktionen wie Betriebserkennungen und die Möglichkeit, benutzerdefinierte Dashboards zu erstellen.

Zugriff auf Pakete und Sitzungsschlüssel

Ermöglicht dem Benutzer, Pakete und Sitzungsschlüssel, nur Pakete, nur Paket-Header oder nur Paket-Slices anzuzeigen und herunterzuladen. Ermöglicht dem Benutzer auch das Extrahieren von Dateien, die Paketen zugeordnet sind.

Systemzugriffsrechte

Diese Rechte bestimmen den Funktionsumfang, über den Benutzer in den Modulen verfügen, für die ihnen Zugriff gewährt wurde.

Für RevealX Enterprise können Benutzer mit Systemzugriffs- und Administratorrechten auf alle Funktionen, Pakete und Sitzungsschlüssel für ihre lizenzierten Module zugreifen.

Für RevealX 360 müssen Systemzugriffs- und Administratorrechte sowie der Zugriff auf lizenzierte Module, Pakete und Sitzungsschlüssel separat zugewiesen werden. RevealX 360 bietet auch ein zusätzliches Systemadministrationskonto, das alle Systemberechtigungen gewährt, mit Ausnahme der Möglichkeit, Benutzer und API-Zugriff zu verwalten.

Die folgende Tabelle enthält ExtraHop-Funktionen und die erforderlichen Rechte. Wenn keine Modulanforderung angegeben ist, ist die Funktion sowohl im NDR- als auch im NDM-Modul verfügbar.

	System- und Zugriffsverw	Systemadmi (nur RevealX 360)	Vollständige Schreiben	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkter Schreibschutz
Karten der Aktivitäten							
Karten für gemeinsame Aktivitäten erstellen, anzeigen und laden	Y	Y	Y	Y	Y	Y	N
Aktivitätskarten speichern	Y	Y	Y	Y	Y	N	N
Aktivitätskarten teilen	Y	Y	Y	Y	N	N	N
Warnmeldungen	NDM-Modullizenz und Zugriff erforderlich.						
Warnmeldungen anzeigen	Y	Y	Y	Y	Y	Y	Y
Benachrichtigungen erstellen und ändern	Y	Y	Y	N	N	N	N
Analyse-Prioritäten							
Seite „Analyseprioritäten“ anzeigen	Y	Y	Y	Y	Y	Y	N
Analyseebenen für Gruppen hinzufügen und ändern	Y	Y	Y	N	N	N	N
Geräte zu einer Beobachtungsliste hinzufügen	Y	Y	Y	N	N	N	N
Verwaltung der Transferprioritäten	Y	Y	Y	N	N	N	N
Bündel							
Ein Paket erstellen	Y	Y	Y	N	N	N	N
Laden Sie ein Paket	Y	Y	Y	N	N	N	N

	System- und Zugriffsverw	Systemadmi (nur RevealX 360)	Vollständige Schreiben	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkter Schreibschutz
hoch und wenden Sie es an							
Laden Sie ein Paket herunter	Y	Y	Y	Y	Y	N	N
Liste der Bundles anzeigen	Y	Y	Y	Y	Y	Y	N
Armaturenbretter	Zum Erstellen und Ändern von Dashboards sind eine NPM-Modullizenz und -zugriff erforderlich .						
Dashboards anzeigen und organisieren	Y	Y	Y	Y	Y	Y	Y
Dashboards erstellen und ändern	Y	Y	Y	Y	Y	N	N
Dashboards teilen	Y	Y	Y	Y	N	N	N
Erkennungen	NDR-Modullizenz und Zugriff sind erforderlich , um Sicherheitserkennungen anzuzeigen und zu optimieren und Untersuchungen durchzuführen. Zum Anzeigen und Optimieren von Leistungserkennungen sind eine NPM-Modullizenz und -zugriff erforderlich.						
Erkennungen anzeigen	Y	Y	Y	Y	Y	Y	Y
Erkennungen bestätigen	Y	Y	Y	Y	Y	N	N
Erkennungsstatus und Hinweise ändern	Y	Y	Y	Y	N	N	N
Untersuchungen erstellen und ändern	Y	Y	Y	Y	N	N	N
Tuning-Regeln erstellen und ändern	Y	Y	Y	N	N	N	N
Gerätegruppen	Administratoren können das konfigurieren Globale Richtlinie „Gerätegruppe bearbeiten“ um anzugeben , ob Benutzer mit eingeschränkten Schreibrechten Gerätegruppen erstellen und bearbeiten können.						

	System- und Zugriffsverw	Systemadmi (nur RevealX 360)	Vollständige Schreiben	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkter Schreibschutz
Gerätegruppen erstellen und ändern	Y	Y	Y	Y (Wenn die globale Rechterichtlinie aktiviert ist)	N	N	N
Integrationen	Nur RevealX 360						
Integrationen konfigurieren und ändern	Y	Y	N	N	N	N	N
Metriken							
Metriken anzeigen	Y	Y	Y	Y	Y	Y	N
Regeln für Benachrichtigungen	NDR-Modullizenz und Zugriff sind erforderlich , um Benachrichtigungen für Sicherheitserkennungen, Sicherheitserkennungskataloge und Bedrohungsinformationen zu erstellen und zu ändern. NPM-Modullizenz und Zugriff sind erforderlich, um Benachrichtigungen für Leistungserkennungen und den Leistungserkennungskatalog zu erstellen und zu ändern.						
Regeln für Erkennungsbenachrichtigungen erstellen und ändern	Y	Y	Y	N	N	N	N
Regeln für Erkennungsbenachrichtigungen für SIEM-Integrationen erstellen und ändern (nur RevealX 360)	Y	Y	N	N	N	N	N
Benachrichtigungsregeln für den Erkennungskatalog erstellen und ändern	Y	Y	Y	N	N	N	N
Benachrichtigungsregeln Bedrohungsübersicht erstellen und ändern	Y	Y	Y	N	N	N	N
Regeln für Systembenachrichtigungen erstellen und ändern	Y	Y	N	N	N	N	N
Rekorde	Recordstore erforderlich.						

	System- und Zugriffsverw	Systemadmi (nur RevealX 360)	Vollständige Schreiben	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkter Schreibschutz
Datensatzabfragen anzeigen	Y	Y	Y	Y	Y	Y	N
Aufzeichnungsformate anzeigen	Y	Y	Y	Y	Y	Y	N
Datensatzabfragen erstellen, ändern und speichern	Y	Y	Y	N	N	N	N
Datensatzformate erstellen, ändern und speichern	Y	Y	Y	N	N	N	N
Geplante Berichte	Konsole erforderlich.						
Geplante Berichte erstellen, anzeigen und verwalten	Y	Y	Y	Y	N	N	N
Bedrohungsinformationen	NDR-Modullizenz und Zugriff erforderlich.						
Datei-Hashing-Filter konfigurieren	Y	Y	N	N	N	N	N
Bedrohungssammlungen verwalten	Y	Y	N	N	N	N	N
TAXII-Feeds verwalten	Y	Y	N	N	N	N	N
Bedrohungsinformationen anzeigen	Y	Y	Y	Y	Y	Y	N
Trigger							
Trigger erstellen und ändern	Y	Y	Y	N	N	N	N
Administratorrechte							
Greifen Sie auf die ExtraHop-Administrationseinstellungen zu	Y	Y	N	N	N	N	N

	System- und Zugriffsverw	Systemadmi (nur RevealX 360)	Vollständige Schreiben	Eingeschränk Schreiben	Persönliches Schreiben	Vollständig schreibgesch	Eingeschränkter Schreibschutz
Stellen Sie eine Verbindung zu anderen Geräten her	Y	Y	N	N	N	N	N
Andere Appliances verwalten (Konsole)	Y	Y	N	N	N	N	N
Benutzer und API-Zugriff verwalten	Y	N	N	N	N	N	N

Lokales Benutzerkonto hinzufügen

Indem Sie ein lokales Benutzerkonto hinzufügen, können Sie Benutzern direkten Zugriff auf Ihr ExtraHop-System gewähren und ihre Rechte entsprechend ihrer Rolle in Ihrer Organisation einschränken.

Weitere Informationen zu Standardsystembenutzerkonten finden Sie unter Lokale Benutzer.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Nutzer**.
3. klicken **Benutzer hinzufügen**.
4. In der Personenbezogene Daten Abschnitt, geben Sie in das Feld Anmelde-ID den Benutzernamen ein, mit dem sich Benutzer am Sensor anmelden, der keine Leerzeichen enthalten darf.

   Zum Beispiel `Adalovelace`.
5. Geben Sie im Feld Vollständiger Name einen Anzeigenamen für den Benutzer ein.

   Der Name kann Leerzeichen enthalten. Zum Beispiel `Ada Lovelace`.
6. Geben Sie im Feld Passwort das Passwort für dieses Konto ein.

   Hinweis: Auf Sensoren und Konsolen muss das Passwort die vom globale Passwortrichtlinie. In ExtraHop-Recordstores und Packetstores müssen Passwörter mindestens 5 Zeichen lang sein.
7. Geben Sie im Feld „Passwort bestätigen“ erneut das Passwort aus dem Passwort Feld.
8. In der Authentifizierungstyp Abschnitt, auswählen **Lokal**.
9. In der Benutzertyp Abschnitt, wählen Sie die Art der Rechte für den Benutzer aus.
   - System- und Zugriffsadministrationsrechte ermöglichen den vollen Lese- und Schreibzugriff auf das ExtraHop-System, einschließlich der Administrationseinstellungen.
   - Eingeschränkte Rechte ermöglichen es Ihnen, aus einer Teilmenge von Rechten und Optionen auszuwählen.

     Hinweis: Weitere Informationen finden Sie in der Benutzerrechte Abschnitt.
10. Klicken Sie **Speichern**.

Hinweis: Um die Einstellungen für einen Benutzer zu ändern, klicken Sie auf den Benutzernamen in der Liste, um den Bearbeiten Benutzerseite.

- Um ein Benutzerkonto zu löschen, klicken Sie auf das rote **X** Symbol. Wenn Sie einen Benutzer von einem Remote-Authentifizierungsserver wie LDAP löschen, müssen Sie auch den Eintrag für diesen Benutzer im ExtraHop-System löschen.

Konto für einen Remote-Benutzer hinzufügen

Fügen Sie ein Benutzerkonto für LDAP- oder SAML-Benutzer hinzu, wenn Sie den Remote-Benutzer bereitstellen möchten, bevor sich dieser Benutzer beim ExtraHop-System anmeldet. Nachdem der Benutzer zum System hinzugefügt wurde, können Sie ihn zu lokalen Gruppen hinzufügen oder Elemente direkt mit ihm teilen, bevor er sich über den LDAP- oder SAML-Anbieter anmeldet.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Einstellungen aufrufen Abschnitt, klicken **Nutzer**.
3. Klicken **Benutzer hinzufügen**.
4. In der Personenbezogene Daten Geben Sie in diesem Abschnitt die folgenden Informationen ein:

   • **Anmelde-ID:** Die E-Mail-Adresse, mit der sich der Benutzer bei seinem LDAP- oder SAML-SSO-Identitätsanbieter anmeldet.

   Hinweis: Für Remotebenutzer werden nur E-Mail-Adressen in Kleinbuchstaben unterstützt.

   • **Vollständiger Name:** Der Vor- und Nachname des Benutzers.
5. In der Authentifizierungstyp Abschnitt, wählen **Ferngesteuert**.
6. Klicken Sie **Speichern**.

Sessions

Das ExtraHop-System bietet Steuerelemente zum Anzeigen und Löschen von Benutzerverbindungen zur Weboberfläche. Die Sessions Die Liste ist nach dem Ablaufdatum sortiert, das dem Datum entspricht, an dem die Sitzungen eingerichtet wurden. Wenn eine Sitzung abläuft oder gelöscht wird, muss sich der Benutzer erneut anmelden, um auf die Weboberfläche zuzugreifen.

Fernauthentifizierung

Das ExtraHop-System unterstützt die Fernauthentifizierung für den Benutzerzugriff. Mithilfe der Remoteauthentifizierung können Unternehmen, die über Authentifizierungssysteme wie LDAP (z. B. OpenLDAP oder Active Directory) verfügen, allen oder einem Teil ihrer Benutzer die Möglichkeit geben, sich mit ihren vorhandenen Anmeldedaten am System anzumelden.

Die zentralisierte Authentifizierung bietet die folgenden Vorteile:

- Synchronisation von Benutzerkennwörtern.
- Automatische Erstellung von ExtraHop-Konten für Benutzer ohne Administratoreingriff.
- Verwaltung von ExtraHop-Privilegien auf der Grundlage von Benutzergruppen.
- Administratoren können allen bekannten Benutzern Zugriff gewähren oder den Zugriff einschränken, indem sie LDAP-Filter anwenden.

Nächste Schritte

- Konfigurieren Sie die Fernauthentifizierung über LDAP
- Konfigurieren Sie die Remote-Authentifizierung über SAML
- Konfigurieren Sie die Fernauthentifizierung über TACACS+
- Konfigurieren Sie die Fernauthentifizierung über RADIUS

Konfigurieren Sie die Fernauthentifizierung über LDAP

Das ExtraHop-System unterstützt das Lightweight Directory Access Protocol (LDAP) zur Authentifizierung und Autorisierung. Anstatt Benutzeranmeldedaten lokal zu speichern, können Sie Ihr ExtraHop-System so konfigurieren, dass Benutzer remote mit einem vorhandenen LDAP-Server authentifiziert werden. Beachten Sie, dass die ExtraHop-LDAP-Authentifizierung nur Benutzerkonten abfragt; sie fragt keine anderen Entitäten ab, die sich möglicherweise im LDAP-Verzeichnis befinden.

Bevor Sie beginnen

- Für dieses Verfahren müssen Sie mit der Konfiguration von LDAP vertraut sein.
- Stellen Sie sicher, dass sich jeder Benutzer in einer berechtigungsspezifischen Gruppe auf dem LDAP-Server befindet, bevor Sie mit diesem Verfahren beginnen.
- Wenn Sie verschachtelte LDAP-Gruppen konfigurieren möchten, müssen Sie die Datei Running Configuration ändern. Kontakt ExtraHop-Unterstützung für Hilfe.

Wenn ein Benutzer versucht, sich bei einem ExtraHop-System anzumelden, versucht das ExtraHop-System, den Benutzer auf folgende Weise zu authentifizieren:

- Versucht, den Benutzer lokal zu authentifizieren.
- Versucht, den Benutzer über den LDAP-Server zu authentifizieren, wenn der Benutzer nicht lokal existiert und wenn das ExtraHop-System für die Fernauthentifizierung mit LDAP konfiguriert ist.
- Meldet den Benutzer im ExtraHop-System an, wenn der Benutzer existiert und das Passwort entweder lokal oder über LDAP validiert wurde. Das LDAP-Passwort wird nicht lokal auf dem ExtraHop-System gespeichert. Beachten Sie, dass Sie den Benutzernamen und das Passwort in dem Format eingeben müssen, für das Ihr LDAP-Server konfiguriert ist. Das ExtraHop-System leitet die Informationen nur an den LDAP-Server weiter.
- Wenn der Benutzer nicht existiert oder ein falsches Passwort eingegeben wurde, erscheint eine Fehlermeldung auf der Anmeldeseite.

> **Wichtig:** Wenn Sie die LDAP-Authentifizierung zu einem späteren Zeitpunkt auf eine andere Methode der Fernauthentifizierung umstellen, werden die Benutzer, Benutzergruppen und zugehörigen Anpassungen, die über die Remote-Authentifizierung erstellt wurden, entfernt. Lokale Benutzer sind nicht betroffen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem Methode der Fernauthentifizierung Dropdownliste, wählen **LDAP** und klicken Sie dann **Weiter**.
4. Auf dem LDAP-Einstellungen Seite, füllen Sie die folgenden Serverinformationsfelder aus:
   a) In der Hostname Feld, geben Sie den Hostnamen oder die IP-Adresse des LDAP-Servers ein. Wenn Sie einen Hostnamen konfigurieren, stellen Sie sicher, dass der DNS-Eintrag des ExtraHop-Systems richtig konfiguriert ist.
   b) In der Hafen In diesem Feld geben Sie die Portnummer ein, auf der der LDAP-Server lauscht.
   c) Aus dem **Servertyp** Dropdownliste, wählen **Posix** oder **Aktives Verzeichnis**.
   d) Optional: In der Binden Sie DN Feld, geben Sie den Bindungs-DN ein. Der Bind-DN sind die Benutzeranmeldedaten, mit denen Sie sich beim LDAP-Server authentifizieren können, um die Benutzersuche durchzuführen. Der Bind-DN muss Listenzugriff auf den Basis-DN und alle Organisationseinheiten, Gruppen oder Benutzerkonto haben, die für die LDAP-Authentifizierung erforderlich sind. Wenn dieser Wert nicht gesetzt ist, wird eine anonyme Bindung durchgeführt. Beachten Sie, dass anonyme Bindungen nicht auf allen LDAP-Servern aktiviert sind.
   e) Optional: In der Passwort binden Feld, geben Sie das Bindungskennwort ein. Das Bind-Passwort ist das Passwort, das für die Authentifizierung beim LDAP-Server als den oben angegebenen Bind-DN erforderlich ist. Wenn Sie eine anonyme Bindung konfigurieren, lassen Sie dieses Feld leer. In einigen Fällen ist eine nicht authentifizierte Bindung möglich, bei der Sie einen Bind-DN-Wert, aber kein Bind-Passwort angeben. Fragen Sie Ihren LDAP-Administrator nach den richtigen Einstellungen.

f) Aus dem **Verschlüsselung** Wählen Sie in der Dropdownliste eine der folgenden Verschlüsselungsoptionen aus.

• **Keine:** Diese Option spezifiziert Klartext-TCP-Sockets. In diesem Modus werden alle Passwörter im Klartext über das Netzwerk gesendet.

• **SPRÜNGE:** Diese Option gibt LDAP an, das in TLS eingeschlossen ist.

• **TLS starten:** Diese Option spezifiziert TLS LDAP. (TLS wird ausgehandelt, bevor Passwörter gesendet werden.)

g) Wählen **SSL-Zertifikate validieren** um die Zertifikatsvalidierung zu aktivieren. Wenn Sie diese Option auswählen, wird das Zertifikat auf dem Remote-Endpunkt anhand der Stammzertifikate überprüft, die vom Trusted Certificates Manager angegeben wurden. Auf der Seite Vertrauenswürdige Zertifikate müssen Sie konfigurieren, welchen Zertifikaten Sie vertrauen möchten. Weitere Informationen finden Sie unter Fügen Sie Ihrem ExtraHop-System ein vertrauenswürdiges Zertifikat hinzu.

h) In der Aktualisierungsintervall Feld, geben Sie einen Zeitwert ein oder belassen Sie die Standardeinstellung von 1 Stunde.

Das Aktualisierungsintervall stellt sicher, dass alle Änderungen am Benutzer- oder Gruppenzugriff auf dem LDAP-Server auf dem ExtraHop-System aktualisiert werden.

5. Konfigurieren Sie die folgenden Benutzereinstellungen:

a) In der Basis DN Feld, geben Sie den eindeutigen Basisnamen (DN) ein.

Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzern sucht. Der Basis-DN muss alle Benutzerkonten enthalten, die Zugriff auf das ExtraHop-System haben werden. Die Benutzer können direkte Mitglieder des Basis-DN sein oder innerhalb einer Organisationseinheit innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

b) In der Suchfilter Feld, geben Sie einen Suchfilter ein.

Mithilfe von Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzerkonten durchsuchen.

Wichtig: Das ExtraHop-System fügt automatisch Klammern hinzu, um den Filter zu umschließen, und analysiert diesen Parameter nicht korrekt, wenn Sie Klammern manuell hinzufügen. Fügen Sie in diesem Schritt und in Schritt 5b Ihre Suchfilter hinzu, ähnlich dem folgenden Beispiel:

```
cn=atlas*
|(cn=EH-*)(cn=IT-*)
```

Wenn Ihre Gruppennamen außerdem das Sternchen (*) enthalten, muss das Sternchen als maskiert werden `\2a`. Zum Beispiel, wenn Ihre Gruppe eine CN mit dem Namen hat `test*group`, typ `cn=test\2agroup` im Feld Suchfilter.

c) Aus dem **Umfang der Suche** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus.

Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzerentitäten an.

• **Ganzer Unterbaum:** Diese Option sucht rekursiv unter dem Gruppen-DN nach passenden Benutzern.

• **Einstufig:** Diese Option sucht nur nach Benutzern, die im Basis-DN existieren, nicht nach Unterbäumen.

6. Optional: Um Benutzergruppen zu importieren, wählen Sie das **Benutzergruppen vom LDAP-Server importieren** setzen Sie ein Häkchen und konfigurieren Sie die folgenden Einstellungen.

Hinweis: Durch den Import von LDAP-Benutzergruppen können Sie Dashboards mit diesen Gruppen teilen. Die importierten Gruppen werden auf der Seite Benutzergruppe in den Administrationseinstellungen angezeigt.

a) In der Basis DN Feld, geben Sie den Basis-DN ein.

Der Basis-DN ist der Punkt, von dem aus ein Server nach Benutzergruppen sucht. Der Basis-DN muss alle Benutzergruppen enthalten, die Zugriff auf das ExtraHop-System haben werden. Die Benutzergruppen können direkte Mitglieder des Basis-DN sein oder innerhalb einer Organisationseinheit innerhalb des Basis-DN verschachtelt sein, wenn **Gesamter Teilbaum** Option ist ausgewählt für Umfang der Suche unten angegeben.

b) In der Suchfilter Feldtyp einen Suchfilter.

Mithilfe von Suchfiltern können Sie Suchkriterien definieren, wenn Sie das LDAP-Verzeichnis nach Benutzergruppen durchsuchen.

Wichtig: Bei Gruppensuchfiltern filtert das ExtraHop-System implizit nach objectclass=group, weshalb objectclass=group diesem Filter nicht hinzugefügt werden sollte.

c) Aus dem **Umfang der Suche** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus.

Der Suchbereich gibt den Umfang der Verzeichnissuche bei der Suche nach Benutzergruppenentitäten an.

- **Ganzer Unterbaum:** Diese Option sucht rekursiv unter dem Basis-DN nach passenden Benutzergruppen.
- **Einstufig:** Diese Option sucht nach Benutzergruppen, die im Basis-DN existieren, nicht nach Unterbäumen.

7. klicken **Einstellungen testen**.

Wenn der Test erfolgreich ist, wird unten auf der Seite eine Statusmeldung angezeigt. Wenn der Test fehlschlägt, klicken Sie auf **Zeige Details** um eine Liste der Fehler zu sehen. Sie müssen alle Fehler beheben, bevor Sie fortfahren.

8. Klicken Sie **Speichern und fortfahren**.

Nächste Schritte
Benutzerrechte für die Fernauthentifizierung konfigurieren

Benutzerrechte für die Fernauthentifizierung konfigurieren
Sie können einzelnen Benutzern in Ihrem ExtraHop-System Benutzerrechte zuweisen oder Rechte über Ihren LDAP-Server konfigurieren und verwalten.

Wenn Sie Benutzerberechtigungen über LDAP zuweisen, müssen Sie mindestens eines der verfügbaren Benutzerberechtigungsfelder ausfüllen. Für diese Felder sind Gruppen (keine Organisationseinheiten) erforderlich , die auf Ihrem LDAP-Server vordefiniert sind. Ein Benutzerkonto mit Zugriff muss ein direktes Mitglied einer bestimmten Gruppe sein. Benutzerkonten, die nicht Mitglied einer oben angegebenen Gruppe sind, haben keinen Zugriff. Gruppen, die nicht anwesend sind, werden im ExtraHop-System nicht authentifiziert.

Das ExtraHop-System unterstützt sowohl Active Directory- als auch POSIX-Gruppenmitgliedschaften. Für Active Directory `memberOf` wird unterstützt. Für POSIX `memberuid`, `posixGroups`, `groupofNames`, und `groupofuniqueNames` werden unterstützt.

1. Wählen Sie eine der folgenden Optionen aus dem Optionen für die Zuweisung von Rechten Dropdownliste:

- **Berechtigungsstufe vom Remoteserver abrufen**

  Diese Option weist Rechte über Ihren Remote-Authentifizierungsserver zu. Sie müssen mindestens eines der folgenden Distinguished Name (DN) -Felder ausfüllen.

  - **System- und Zugriffsverwaltung DN:** Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, einschließlich der Administrationseinstellungen.
  - **Vollständiger Schreib-DN:** Erstellen und ändern Sie Objekte auf dem ExtraHop-System, ohne die Administrationseinstellungen.
  - **Eingeschränkte Schreib-DN:** Erstellen, ändern und teilen Sie Dashboards.

• **Persönliches Schreiben DN:** Erstellen Sie persönliche Dashboards und ändern Sie Dashboards, die mit dem angemeldeten Benutzer geteilt werden.

• **Vollständiger schreibgeschützter DN:** Objekte im ExtraHop-System anzeigen.

• **Eingeschränkter schreibgeschützter DN:** Sehen Sie sich Dashboards an, die mit dem angemeldeten Benutzer geteilt wurden.

• **Packet Slices Access DN:** Zeigen Sie die ersten 64 Byte an Paketen an, die über die ExtraHop Trace-Appliance erfasst wurden, und laden Sie sie herunter.

• **Paketzugriffs-DN:** Über die ExtraHop Trace-Appliance erfasste Pakete anzeigen und herunterladen.

• **Paket- und Sitzungsschlüssel Access DN:** Pakete und alle zugehörigen TLS-Sitzungsschlüssel, die über die ExtraHop Trace-Appliance erfasst wurden, anzeigen und herunterladen.

• **NDR-Modulzugriff DN:** Sicherheitserkennungen, die im ExtraHop-System erscheinen, anzeigen, bestätigen und ausblenden.

• **NPM-Modulzugriffs-DN:** Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und ausblenden.

- **Remote-Benutzer haben vollen Schreibzugriff**

  Diese Option gewährt Remote-Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
- **Remote-Benutzer haben vollen Lesezugriff**

  Diese Option gewährt Remote-Benutzern schreibgeschützten Zugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.

2. Optional: Konfigurieren Sie den Zugriff auf Paket und Sitzungsschlüssel. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und TLS-Sitzungsschlüsseln zu ermöglichen.
   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
3. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff.
   - **Kein Zugriff**
   - **Voller Zugriff**
4. Klicken Sie **Speichern und fertig**.
5. Klicken Sie **Erledigt**.

Konfigurieren Sie die Fernauthentifizierung über SAML

Sie können die sichere SSO-Authentifizierung (Single Sign-On) für das ExtraHop-System über einen oder mehrere SAML-Identitätsanbieter (Security Assertion Markup Language) konfigurieren.

Video: Sehen Sie sich die entsprechende Schulung an: SSO-Authentifizierung

Wenn sich ein Benutzer bei einem ExtraHop-System anmeldet, das als Service Provider (SP) für die SAML-SSO-Authentifizierung konfiguriert ist, fordert das ExtraHop-System die Autorisierung vom entsprechenden Identity Provider (IdP) an. Der Identitätsanbieter authentifiziert die Anmeldedaten des Benutzers und gibt dann die Autorisierung für den Benutzer an das ExtraHop-System zurück. Der Benutzer kann dann auf das ExtraHop-System zugreifen.

Die Konfigurationsleitfäden für bestimmte Identitätsanbieter sind unten verlinkt. Wenn Ihr Anbieter nicht aufgeführt ist, wenden Sie die vom ExtraHop-System erforderlichen Einstellungen auf Ihren Identitätsanbieter an.

Identitätsanbieter müssen die folgenden Kriterien erfüllen:

- SAML 2.0
- Unterstützt SP-initiierte Anmeldeabläufe. IDP-initiierte Anmeldeabläufe werden nicht unterstützt.
- Unterstützt signierte SAML-Antworten
- Unterstützt HTTP-Redirect-Binding

Die Beispielkonfiguration in diesem Verfahren ermöglicht den Zugriff auf das ExtraHop-System über Gruppenattribute.

Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

SAML-Remoteauthentifizierung aktivieren

Bevor Sie beginnen

Warnung: Wenn Ihr System bereits mit einer Fernauthentifizierungsmethode konfiguriert ist, werden durch das Ändern dieser Einstellungen alle Benutzer und zugehörigen Anpassungen entfernt, die mit dieser Methode erstellt wurden, und Remotebenutzer können nicht auf das System zugreifen. Lokale Benutzer sind nicht betroffen.

Sie können die Fernauthentifizierung mit SAML auf diesem ExtraHop-System aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem **Methode der Fernauthentifizierung** Dropdownliste, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. klicken **SP-Metadaten anzeigen** um die Assertion Consumer Service (ACS) -URL und die Entitäts-ID des ExtraHop-Systems anzuzeigen.

   Diese Zeichenfolgen werden von Ihrem Identitätsanbieter benötigt, um die SSO-Authentifizierung zu konfigurieren. Sie können auch nach unten scrollen, um die Metadaten als XML-Datei herunterzuladen , die Sie in Ihre Identitätsanbieter-Konfiguration importieren können.

   Hinweis: Die ACS-URL enthält den in den Netzwerkeinstellungen konfigurierten Hostnamen. Wenn die ACS-URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`, müssen Sie die URL bearbeiten, wenn Sie die ACS-URL zu Ihrem Identitätsanbieter hinzufügen, und den vollqualifizierten Domänenname (FQDN) des ExtraHop-Systems angeben.
6. klicken **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen Namen ein, um Ihren spezifischen Identitätsanbieter zu identifizieren.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems nach dem Text Anmelden mit Text.
8. In der Entitäts-ID Feld, fügen Sie die von Ihrem Identitätsanbieter bereitgestellte Entitäts-ID ein.
9. In der SSO-URL Fügen Sie in dieses Feld die von Ihrem Identitätsanbieter bereitgestellte Single Sign-On-URL ein.
10. In der Öffentliches Zertifikat Fügen Sie in dieses Feld das X.509-Zertifikat ein, das von Ihrem Identitätsanbieter bereitgestellt wurde.
11. Wählen Sie die **Automatisches Provisioning von Benutzern** Kontrollkästchen, um anzugeben , dass ExtraHop-Benutzerkonten automatisch erstellt werden, wenn sich der Benutzer über den Identitätsanbieter anmeldet.

Um manuell zu steuern, welche Benutzer sich anmelden können, deaktivieren Sie dieses Kontrollkästchen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Jeder manuell erstellte Remote-Benutzername sollte mit dem auf dem Identitätsanbieter konfigurierten Benutzernamen übereinstimmen.

12. Wählen Sie die **Diesen Identitätsanbieter aktivieren** Kontrollkästchen, um Benutzern die Anmeldung am ExtraHop-System zu ermöglichen.

    Dies ist standardmäßig aktiviert. Um zu verhindern, dass sich Benutzer über diesen Identitätsanbieter anmelden, deaktivieren Sie das Kontrollkästchen.

13. In der Attribute von Benutzerrechten Abschnitt, Konfiguration von Benutzerberechtigungsattributen.

    Dies muss abgeschlossen sein, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Bei Werten wird nicht zwischen Groß- und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Die Namen und Werte der Benutzerberechtigungsattribute müssen mit den Namen und Werten übereinstimmen, die Ihr Identitätsanbieter in SAML-Antworten einbezieht, die konfiguriert werden, wenn Sie die ExtraHop-Anwendung zu einem Anbieter hinzufügen. In Microsoft Entra ID konfigurieren Sie beispielsweise Anspruchsnamen und Anspruchsbedingungswerte, die mit den Namen und Werten der Benutzerberechtigungsattribute im ExtraHop-System übereinstimmen müssen.

    Hinweis: Wenn ein Benutzer mehreren Attributwerten entspricht, wird dem Benutzer das Zugriffsrecht mit den meisten Berechtigungen gewährt. Wenn ein Benutzer beispielsweise den Werten Eingeschränktes Schreiben und Vollständiges Schreiben entspricht, erhält der Benutzer volle Schreibberechtigungen. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

    Ausführlichere Beispiele finden Sie in den folgenden Themen:

    - SAML-Single-Sign-On mit JumpCloud konfigurieren
    - SAML-Single-Sign-On mit Google konfigurieren
    - SAML-Single-Sign-On mit Okta konfigurieren
    - SAML-Single-Sign-On mit Microsoft Entra ID konfigurieren

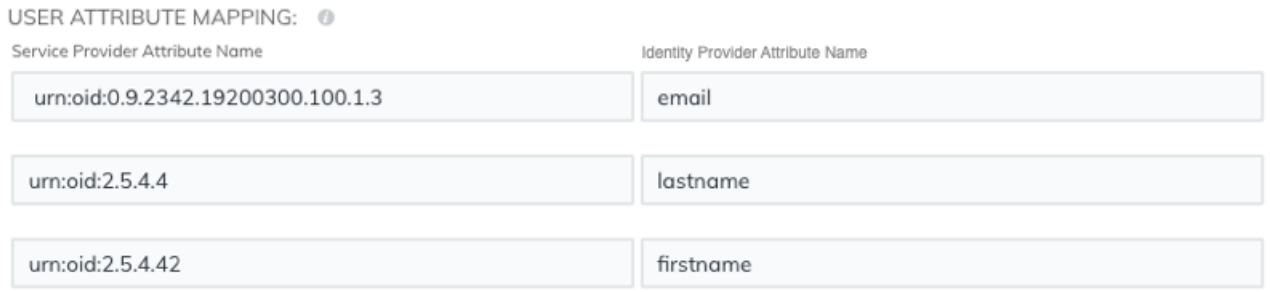
14. In der Zugriff auf das NDR-Modul Abschnitt, Konfiguration von Attributen, um Benutzern den Zugriff auf NDR-Funktionen zu ermöglichen.
15. In der Zugriff auf das NPM-Modul Abschnitt, Konfigurieren Sie Attribute, um Benutzern den Zugriff auf NPM-Funktionen zu ermöglichen.
16. In der Zugriff auf Pakete und Sitzungsschlüssel Abschnitt, konfigurieren Sie Attribute, um Benutzern den Zugriff auf Pakete und Sitzungsschlüssel zu ermöglichen.

    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen angeschlossenen ExtraHop-Paketstore haben.

17. Klicken Sie **Speichern**.

Zuordnung von Benutzerattributen
Sie müssen den folgenden Satz von Benutzerattributen im Abschnitt zur Zuordnung von Anwendungsattributen auf Ihrem Identitätsanbieter konfigurieren. Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System. Die richtigen Eigenschaftsnamen beim Zuordnen von Attributen finden Sie in der Dokumentation Ihres Identitätsanbieters.

ExtraHop-Attributname	Freundlicher Name	Kategorie	Attributname des Identitätsanbieters
`urn:oid:0.9.2342.19200300.100.1.3`	Mail	Standardattribut	Primäre E-Mail-Adresse
`urn:oid:2.5.4.4`	sn	Standardattribut	Nachname
`urn:oid:2.5.4.42`	Vorgegebener Name	Standardattribut	Vorname



Attributaussagen gruppieren
Das ExtraHop-System unterstützt Anweisungen zu Gruppenattributen, um Benutzerberechtigungen einfach allen Mitgliedern einer bestimmten Gruppe zuzuordnen. Wenn Sie die ExtraHop-Anwendung auf Ihrem Identitätsanbieter konfigurieren, geben Sie einen Gruppenattributnamen an. Dieser Name wird dann in das Name des Attributs Feld, wenn Sie den Identity Provider auf dem ExtraHop-System konfigurieren.

Wenn Ihr Identitätsanbieter keine Gruppenattributanweisungen unterstützt, konfigurieren Sie Benutzerattribute mit den entsprechenden Rechten für Modulzugriff, Systemzugriff und Paketforensik.

Die nächsten Schritte

Nachdem Sie die Remote-Authentifizierung über SAML konfiguriert haben, überprüfen Sie diese Aufgaben.

- SAML-Single-Sign-On mit JumpCloud konfigurieren
- SAML-Single-Sign-On mit Google konfigurieren
- SAML-Single-Sign-On mit Okta konfigurieren

SAML-Single-Sign-On mit Okta konfigurieren

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Benutzer über den Okta Identity Management Service beim System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verabreichung von Okta vertraut sein. Diese Verfahren basieren auf der Okta Classic-Benutzeroberfläche. Wenn Sie Okta über die Developer Console konfigurieren, ist das Verfahren möglicherweise etwas anders.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Okta Classic-Benutzeroberfläche kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen .

SAML auf dem ExtraHop-System aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem **Methode der Fernauthentifizierung** Dropdownliste, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. Klicken Sie **SP-Metadaten anzeigen**.

Sie müssen die ACS-URL und die Entitäts-ID kopieren, um sie im nächsten Verfahren in die Okta-Konfiguration einzufügen.

SAML-Einstellungen in Okta konfigurieren
Bei diesem Verfahren müssen Sie Informationen zwischen den ExtraHop-Administrationseinstellungen und der Okta Classic-Benutzeroberfläche kopieren und einfügen. Daher ist es hilfreich, wenn alle Benutzeroberflächen nebeneinander geöffnet sind.

1. Loggen Sie sich bei Okta ein.
2. Ändern Sie in der oberen rechten Ecke der Seite die Ansicht von **Entwicklerkonsole** zu **Klassische Benutzeroberfläche**.

3. Klicken Sie im oberen Menü auf **Anwendungen**.
4. Klicken Sie **Anwendung hinzufügen**.
5. Klicken Sie **Neue App erstellen**.
6. Aus dem Plattform Dropdownliste, wählen **Netz**.
7. Für die Anmeldemethode, wählen **SAML 2.0** .
8. Klicken Sie **Erstellen**.
9. In der Allgemeine Einstellungen Abschnitt, in der App Namensfeld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.
10. Optional: Konfiguriere die Logo der App und Sichtbarkeit der App Felder, die für Ihre Umgebung erforderlich sind.
11. Klicken Sie **Weiter**.
12. In der SAML-Einstellungen Fügen Sie in den Abschnitten die URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System in das Feld Single Sign On URL in Okta ein.

    Hinweis: Möglicherweise müssen Sie die ACS-URL manuell bearbeiten, wenn die URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`. Wir empfehlen Ihnen, den vollqualifizierten Domänenname für das ExtraHop-System in der URL anzugeben.
13. Fügen Sie die SP Entity ID aus dem ExtraHop-System in das Zielgruppen-URI (SP-Entitäts-ID) Feld in Okta.
14. Aus dem **Namens-ID-Format** Dropdownliste, wählen **Hartnäckig**.
15. Aus dem **Nutzername der Anwendung** Wählen Sie in der Dropdownliste ein Benutzernamenformat aus.
16. In der Angaben zu Attributen Abschnitt, fügen Sie die folgenden Attribute hinzu.

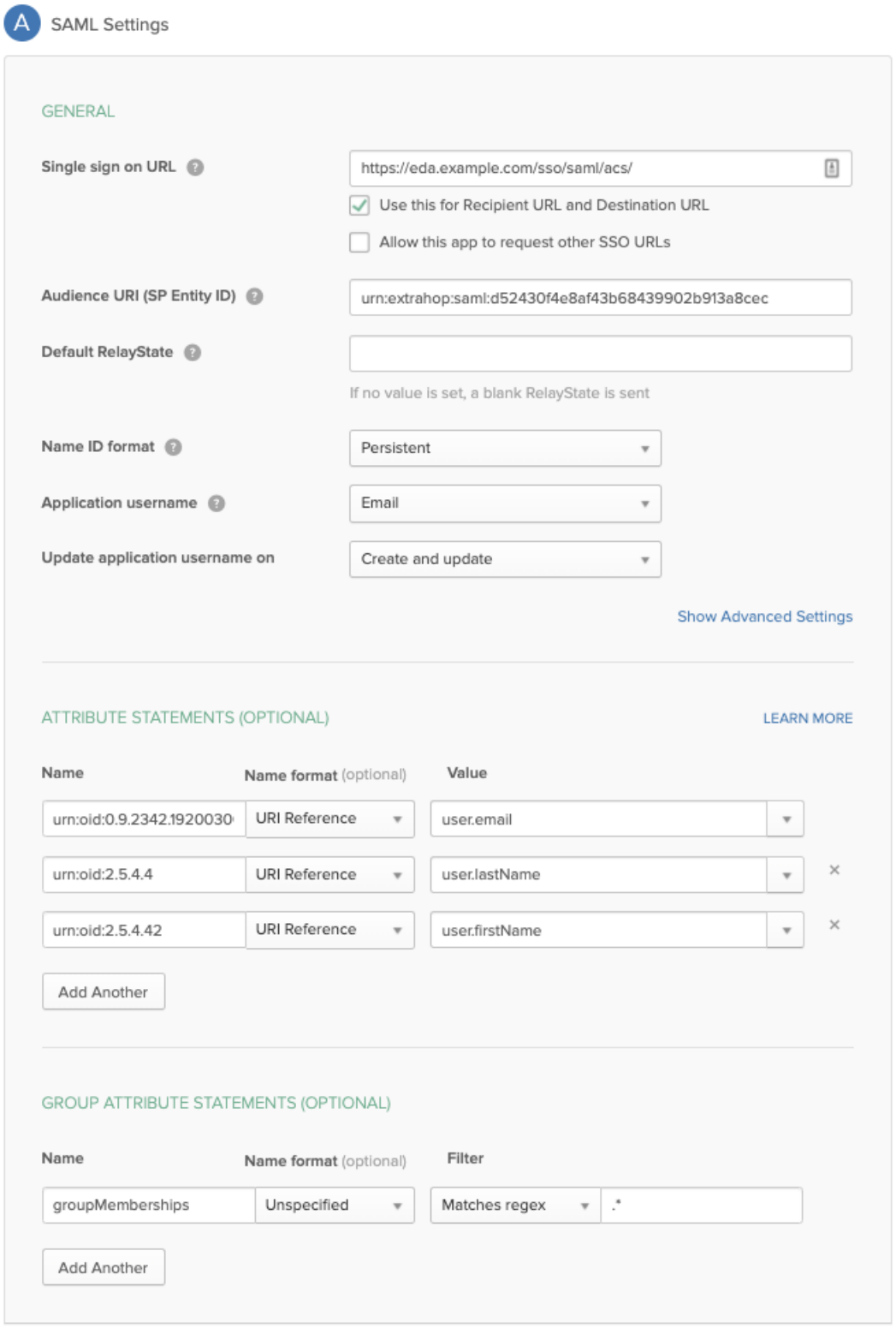
    Diese Attribute identifizieren den Benutzer im gesamten ExtraHop-System.

Name	Format des Namens	Wert
`urn:oid:0.9.2342.19200300.100.1.3`	URI-Referenz	Benutzer.E-Mail
`urn:oid:2.5.4.4`	URI-Referenz	Benutzer.Nachname
`urn:oid:2.5.4.42`	URI-Referenz	Benutzer.Vorname

17. In der Anweisung zu Gruppenattributen Abschnitt, in der Name Feld, geben Sie eine Zeichenfolge ein und konfigurieren Sie einen Filter.

    Sie geben den Namen des Gruppenattributs an, wenn Sie Benutzerberechtigungsattribute im ExtraHop-System konfigurieren.

Die folgende Abbildung zeigt eine Beispielkonfiguration.



18. Klicken Sie **Weiter** und klicken Sie dann **Fertig**.
    Sie kehren zurück zum Einstellungen für die Anmeldung Seite.
19. In der Einstellungen Abschnitt, klicken Sie **Anweisungen zur Einrichtung anzeigen**.

Ein neues Browserfenster wird geöffnet und zeigt Informationen an, die für die Konfiguration des ExtraHop-Systems erforderlich sind.

Weisen Sie das ExtraHop-System Okta-Gruppen zu

Wir gehen davon aus, dass Sie bereits Benutzer und Gruppen in Okta konfiguriert haben. Falls nicht, schlagen Sie in der Okta-Dokumentation nach, um neue Benutzer und Gruppen hinzuzufügen.

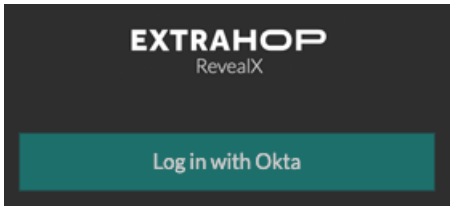
1. Wählen Sie im Menü Verzeichnis **Gruppen**.
2. Klicken Sie auf den Gruppennamen.
3. klicken **Apps verwalten**.
4. Suchen Sie den Namen der Anwendung, die Sie für das ExtraHop-System konfiguriert haben, und klicken Sie auf **Zuweisen**.
5. klicken **Erledigt**.

Fügen Sie Informationen zum Identitätsanbieter im ExtraHop-System hinzu

1. Kehren Sie zu den Administrationseinstellungen auf dem ExtraHop-System zurück.

   Schließen Sie das Service Provider-Metadatenfenster, falls es noch geöffnet ist, und klicken Sie dann auf **Identitätsanbieter hinzufügen**.
2. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.

   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.



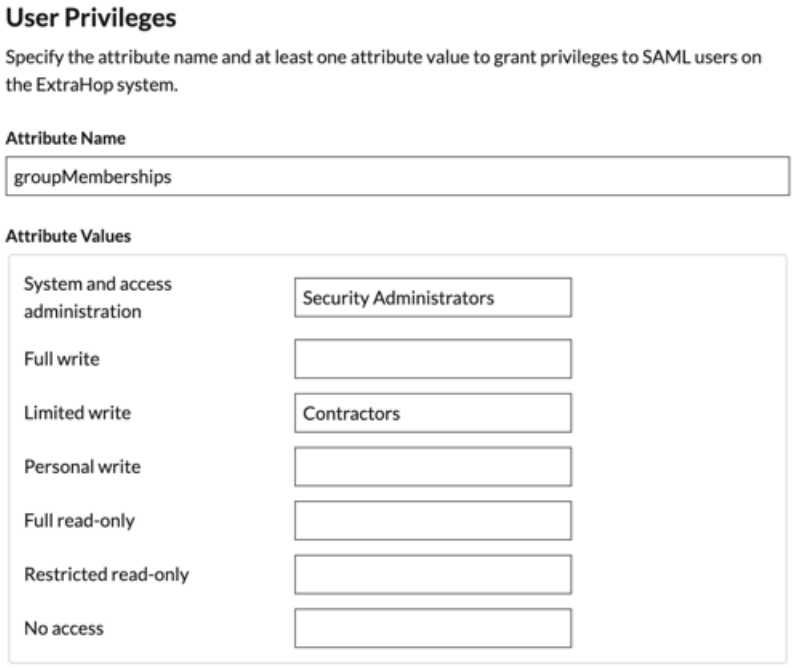
3. Kopieren Sie aus Okta das URL für einmaliges Anmelden des Identitätsanbieters und fügen Sie es in das SSO-URL-Feld auf dem ExtraHop-System ein.
4. Kopieren Sie aus Okta das URL des Ausstellers des Identitätsanbieters und füge es in das Entitäts-ID Feld auf dem ExtraHop-System.
5. Kopieren Sie das X.509-Zertifikat von Okta und fügen Sie es in das Öffentliches Zertifikat Feld auf dem ExtraHop-System.
6. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
   - Wählen Sie Benutzer automatisch bereitstellen, um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet.
   - Deaktivieren Sie das Kontrollkästchen Benutzer automatisch bereitstellen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Okta bestimmt.
7. Das **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden.

   Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
8. Konfigurieren Sie Benutzerberechtigungsattribute.

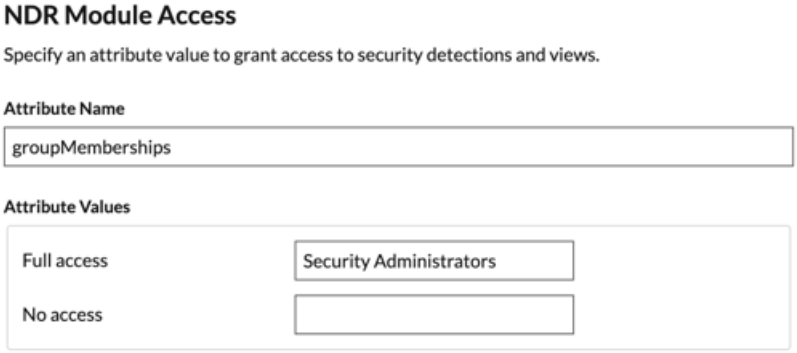
   Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei Werten wird nicht zwischen Groß - und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen.

Wichtig: Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

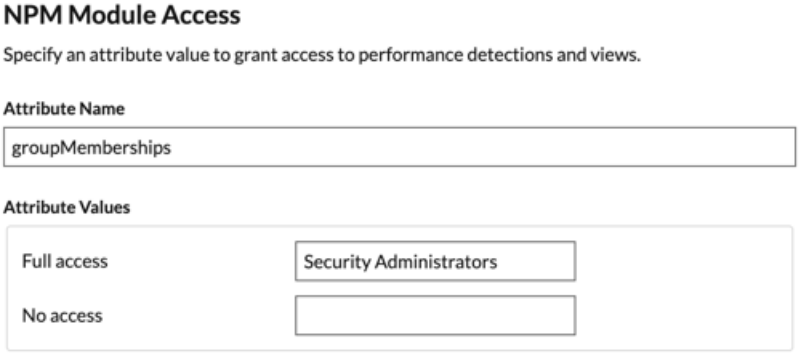
In den folgenden Beispielen ist Name des Attributs Feld ist das Gruppenattribut, das bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde, und Attributwerte sind die Namen Ihrer Benutzergruppen. Wenn ein Benutzer Mitglied von mehr als einer Gruppe ist, wird ihm das Zugriffsrecht mit den meisten Berechtigungen gewährt.



9. Konfigurieren Sie den NDR-Modulzugriff.



10. Konfigurieren Sie den NPM-Modulzugriff.



11. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.

Dieser Schritt ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore und das Packet Forensics Modul haben.

12. Klicken Sie **Speichern**.
13. Speichern Sie die laufende Konfigurationsdatei.

Loggen Sie sich in das ExtraHop-System ein

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Loggen Sie sich ein mit** *<provider name>*.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.

SAML-Single-Sign-On mit Google konfigurieren

Sie können Ihr ExtraHop-System so konfigurieren, dass sich Nutzer über den Google-Identitätsverwaltungsdienst beim System anmelden können.

Bevor Sie beginnen

- Sie sollten mit der Verwaltung von Google Admin vertraut sein.
- Sie sollten mit der Verwaltung von ExtraHop-Systemen vertraut sein.

Bei diesen Verfahren müssen Sie Informationen zwischen dem ExtraHop-System und der Google Admin-Konsole kopieren und einfügen. Daher ist es hilfreich, jedes System nebeneinander zu öffnen.

SAML auf dem ExtraHop-System aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem **Methode der Fernauthentifizierung** Dropdownliste, wählen **SAML**.
4. Klicken Sie **Weiter**.
5. Klicken Sie **SP-Metadaten anzeigen**.
6. Kopieren Sie das ACS-URL und Entitäts-ID in eine Textdatei.

   Sie werden diese Informationen in einem späteren Verfahren in die Google-Konfiguration einfügen.

Benutzerdefinierte Benutzerattribute hinzufügen

1. Loggen Sie sich in die Google Admin-Konsole ein.
2. Klicken Sie **Nutzer**.

3. Klicken Sie auf das Symbol Benutzerdefinierte Attribute verwalten  .
4. Klicken Sie **Benutzerdefiniertes Attribut hinzufügen**.
5. In der Kategorie Feld, Typ `ExtraHop`.
6. Optional: In der Beschreibung Feld, geben Sie eine Beschreibung ein.
7. In der Benutzerdefinierte Felder Abschnitt, geben Sie die folgenden Informationen ein:
   a) In der Name Feld, Typ `Level schreiben`.
   b) Aus dem **Art der Information** Dropdownliste, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Dropdownliste, wählen **Sichtbar für Domain**.
   d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.
8. Aktivieren Sie den Zugriff auf das NDR-Modul:
   a) In der Name Feld, Typ `ndr-Niveau`.
   b) Aus dem **Art der Information** Dropdownliste, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Dropdownliste, wählen **Sichtbar für Domain**.
   d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.
9. Aktivieren Sie den NPM-Modulzugriff:
   a) In der Name Feld, Typ `npm-Ebene`.
   b) Aus dem **Art der Information** Dropdownliste, wählen **Text**.
   c) Aus dem **Sichtbarkeit** Dropdownliste, wählen **Sichtbar für Domain**.
   d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.
10. Optional: Wenn Sie Paketspeicher verbunden haben, aktivieren Sie den Paketzugriff, indem Sie ein benutzerdefiniertes Feld konfigurieren:
    a) In der Name Feld, Typ `Paketebene`.
    b) Aus dem **Art der Information** Dropdownliste, wählen **Text**.
    c) Aus dem **Sichtbarkeit** Dropdownliste, wählen **Sichtbar für Domain**.
    d) Aus dem **Anzahl der Werte** Dropdownliste, wählen **Einzelner Wert**.
11. Klicken Sie **Hinzufügen**.

Fügen Sie Identitätsanbieterinformationen von Google zum ExtraHop-System hinzu

1. Klicken Sie in der Google Admin-Konsole auf das Hauptmenüsymbol  und wähle **Apps** > **SAML-Apps**.
2. Klicken Sie auf SSO für eine SAML-Anwendung aktivieren Symbol  .
3. klicken **RICHTE MEINE EIGENE BENUTZERDEFINIERTE APP EIN**.
4. Auf dem Google IdP-Informationen Bildschirm, klicken Sie auf **Herunterladen** Schaltfläche zum Herunterladen des Zertifikats (`GoogleIDPCertificate.pem`).
5. Kehren Sie zu den Administrationseinstellungen auf dem ExtraHop-System zurück.
6. klicken **Identitätsanbieter hinzufügen**.
7. In der Name des Anbieters Feld, geben Sie einen eindeutigen Namen ein.
   Dieser Name erscheint auf der Anmeldeseite des ExtraHop-Systems.
8. Aus dem Google IdP-Informationen Bildschirm, kopiere die SSO-URL und füge sie in das SSO-URL Feld auf der ExtraHop-Appliance.
9. Aus dem Google IdP-Informationen Bildschirm, kopieren Sie die Entitäts-ID und fügen Sie sie in das Feld Entitäts-ID auf dem ExtraHop-System ein.
10. Öffne das `GoogleIDPCertificate` Kopieren Sie den Inhalt in einem Texteditor und fügen Sie ihn in den Öffentliches Zertifikat Feld auf dem ExtraHop-System.
11. Wählen Sie aus einer der folgenden Optionen aus, wie Sie Benutzer bereitstellen möchten.
    - Wählen **Automatische Bereitstellung von Benutzern** um ein neues Remote-SAML-Benutzerkonto auf dem ExtraHop-System zu erstellen, wenn sich der Benutzer zum ersten Mal anmeldet .

- Löschen Sie das **Automatische Bereitstellung von Benutzern** Markieren Sie das Kontrollkästchen und konfigurieren Sie neue Remote-Benutzer manuell über die ExtraHop-Administrationseinstellungen oder die REST-API. Zugriffs- und Berechtigungsstufen werden durch die Benutzerkonfiguration in Google bestimmt.

12. Das **Diesen Identitätsanbieter aktivieren** Die Option ist standardmäßig ausgewählt und ermöglicht es Benutzern, sich beim ExtraHop-System anzumelden. Um zu verhindern, dass sich Benutzer anmelden, deaktivieren Sie das Kontrollkästchen.
13. Konfigurieren Sie Benutzerberechtigungsattribute.

    Sie müssen die folgenden Benutzerattribute konfigurieren, bevor sich Benutzer über einen Identitätsanbieter beim ExtraHop-System anmelden können. Werte sind benutzerdefinierbar; sie müssen jedoch mit den Attributnamen übereinstimmen, die in der SAML-Antwort Ihres Identitätsanbieters enthalten sind. Bei Werten wird nicht zwischen Groß - und Kleinschreibung unterschieden und sie können Leerzeichen enthalten. Weitere Hinweise zu Berechtigungsstufen finden Sie unter Benutzer und Benutzergruppen..

    Wichtig: Sie müssen den Attributnamen angeben und mindestens einen anderen Attributwert konfigurieren als **Kein Zugriff** um Benutzern die Anmeldung zu ermöglichen.

    Im Beispiel unten ist der Name des Attributs Feld ist das Anwendungsattribut und Attributwert ist der Name des Benutzerfeldes, der bei der Erstellung der ExtraHop-Anwendung auf dem Identity Provider konfiguriert wurde.

Name des Feldes	Beispiel für einen Attributwert
Name des Attributs	`urn:extrahop:saml:2.0: Ebene schreiben`
System- und Zugriffsverwaltung	`illimitiert`
Volle Schreibrechte	`voll_schreiben`
Eingeschränkte Schreibrechte	`begrenztes_schreiben`
Persönliche Schreibrechte	`persönliches_schreiben`
Volle Nur-Lese-Rechte	`voll_schreibgeschützt`
Eingeschränkte Nur-Lese-Rechte	`restricted_readonly`
Kein Zugriff	`keine`

14. Konfigurieren Sie den NDR-Modulzugriff.

Feld	Beispiel für einen Attributwert
Name des Attributs	`urn:extrahop:saml:2.0: ndrlevel`
Voller Zugriff	`voll`
Kein Zugriff	`keine`

15. Konfigurieren Sie den NPM-Modulzugriff.

Feld	Beispiel für einen Attributwert
Name des Attributs	`urn:extrahop:saml:2.0: npmlevel`
Voller Zugriff	`voll`
Kein Zugriff	`keine`

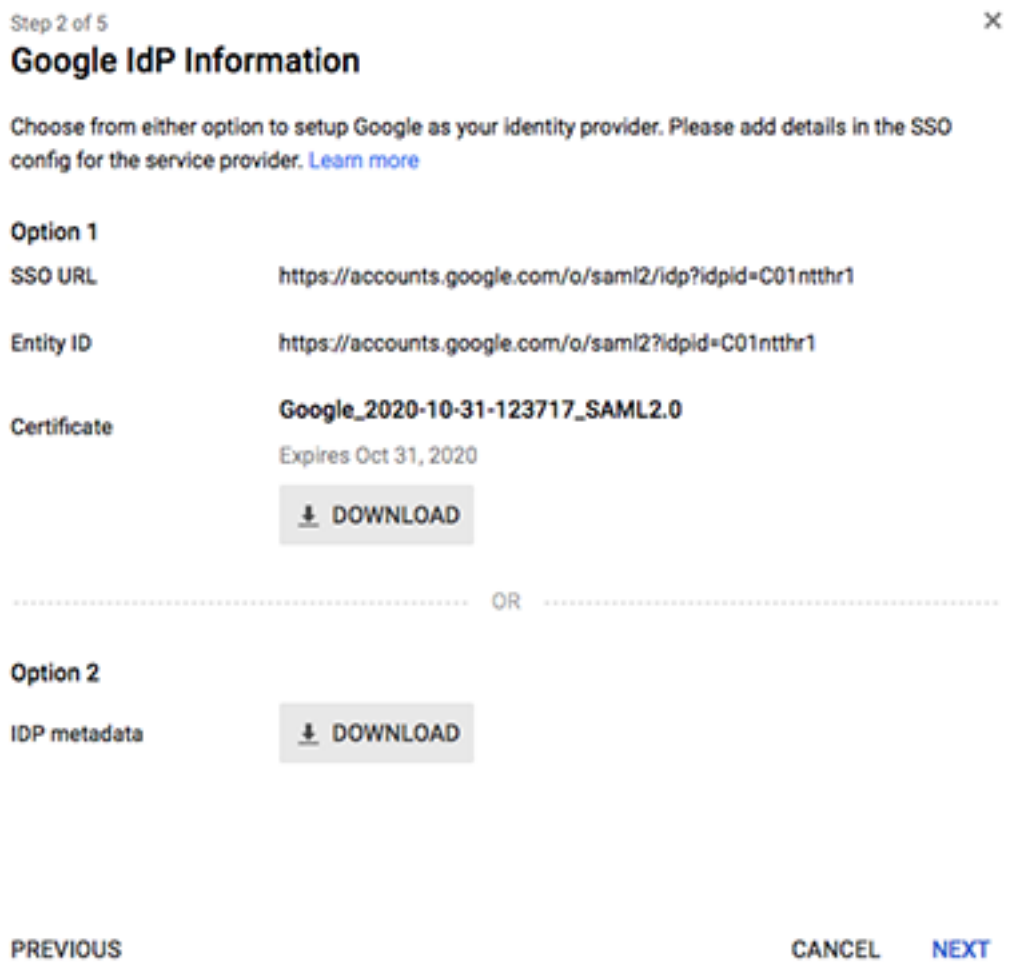
16. Optional: Konfigurieren Sie den Zugriff auf Pakete und Sitzungsschlüssel.
    Die Konfiguration von Paketen und Sitzungsschlüsselattributen ist optional und nur erforderlich , wenn Sie einen verbundenen Packetstore haben.

Name des Feldes	Beispiel für einen Attributwert
Name des Attributs	`urn:extrahop:saml:2.0: Paketebene`
Pakete und Sitzungsschlüssel	`voll_mit_Schlüsseln`
Nur Pakete	`voll`
Pakete nur in Segmenten	`Scheiben`
Kein Zugriff	`keine`

17. Klicken Sie **Speichern**.
18. Speichern Sie die laufende Konfiguration.

Fügen Sie Informationen zum ExtraHop-Dienstanbieter zu Google hinzu

1. Kehren Sie zur Google Admin-Konsole zurück und klicken Sie auf **Weiter** auf dem Google Idp-Informationen Seite, um mit Schritt 3 von 5 fortzufahren.



2. In der Name der Anwendung Feld, geben Sie einen eindeutigen Namen ein, um das ExtraHop-System zu identifizieren.

Jedes ExtraHop-System, für das Sie eine SAML-Anwendung erstellen, benötigt einen eindeutigen Namen.

3. Optional: Geben Sie eine Beschreibung für diese Anwendung ein oder laden Sie ein benutzerdefiniertes Logo hoch.
4. Klicken Sie **Weiter**.
5. Kopieren Sie das URL des Assertion Consumer Service (ACS) aus dem ExtraHop-System und füge es ein in das ACS-URL Feld in Google Admin.

   Hinweis: Möglicherweise müssen Sie die ACS-URL manuell bearbeiten, wenn die URL einen nicht erreichbaren Hostnamen enthält, z. B. den Standardsystemhostnamen `extrahop`. Wir empfehlen Ihnen, den vollqualifizierten Domänenname für das ExtraHop-System in der URL anzugeben.
6. Kopieren Sie das SP-Entitäts-ID aus dem ExtraHop-System und füge es ein in das Entitäts-ID Feld in Google Admin.
7. Wählen Sie die **Signierte Antwort** Ankreuzfeld.
8. In der Name ID Abschnitt, belassen Sie die Standardeinstellung **Grundlegende Informationen** und **Primäre E-Mail** Einstellungen unverändert.
9. Aus dem **Namens-ID-Format** Dropdownliste, wählen **HARTNÄCKIG**.
10. Klicken Sie **Weiter**.
11. Auf dem Zuordnung von Attributen Bildschirm, klicken **NEUES MAPPING HINZUFÜGEN**.
12. Fügen Sie die folgenden Attribute genau wie gezeigt hinzu.

    Die ersten vier Attribute sind erforderlich. Das `packetslevel` Das Attribut ist optional und nur erforderlich, wenn Sie einen verbundenen Packetstore haben. Wenn Sie einen Packetstore haben und den nicht konfigurieren `packetslevel` Attribut, Benutzer können Paketerfassungen im ExtraHop-System nicht anzeigen oder herunterladen.

Anwendungsattribut	Kategorie	Benutzerfeld
`urn:oid:0.9.2342.19200300.100.1.3`	Grundlegende Informationen	Primäre E-Mail
`urn:oid:2.5.4.4`	Grundlegende Informationen	Nachname
`urn:oid:2.5.4.42`	Grundlegende Informationen	Vorname
`urn:extrahop:saml:2.0: Ebene schreiben`	ExtraHop	Level schreiben
`urn:extrahop:saml:2.0: ndrlevel`	ExtraHop	ndr-Niveau
`urn:extrahop:saml:2.0: npmlevel`	ExtraHop	npm-Ebene
`urn:extrahop:saml:2.0: Paketebene`	ExtraHop	Paketebene

13. Klicken Sie **Fertig** und klicken Sie dann **OK**.
14. Klicken Sie **Dienst bearbeiten**.
15. Wählen **An für alle**.
16. Klicken Sie **Speichern**.

Benutzerrechte zuweisen

1. Klicken Sie **Nutzer** um zur Tabelle aller Benutzer in Ihren Organisationseinheiten zurückzukehren.
2. Klicken Sie auf den Namen des Benutzers, dem Sie die Anmeldung am ExtraHop-System ermöglichen möchten.

3. In der Informationen zum Nutzer Abschnitt, klicken **Angaben zum Nutzer**.
4. In der ExtraHop Abschnitt, klicken **Level schreiben** und geben Sie eine der folgenden Berechtigungsstufen ein.

   - `illimitiert`
   - `voll_schreiben`
   - `begrenztes_schreiben`
   - `persönliches_schreiben`
   - `voll_schreibgeschützt`
   - `restricted_readonly`
   - `keine`

   Hinweise zu Benutzerrechten finden Sie unter Benutzer und Benutzergruppen.
5. Optional: Wenn du das hinzugefügt hast `packetslevel` Attribut oben, klicken **Paketebene** und geben Sie eines der folgenden Rechte ein.

   - `voll`
   - `voll_mit_schreiben`
   - `keine`

6. Optional: Wenn du das hinzugefügt hast `detectionslevel` Attribut oben, klicken **Erkennungsstufe** und geben Sie eines der folgenden Rechte ein.

   - `voll`
   - `keine`
7. Klicken Sie **Speichern**.

Loggen Sie sich in das ExtraHop-System ein

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. klicken **Loggen Sie sich ein mit** *<provider name>*.
3. Melden Sie sich mit Ihrer E-Mail-Adresse und Ihrem Passwort bei Ihrem Anbieter an. Sie werden automatisch zur ExtraHop-Übersichtsseite weitergeleitet.

Konfigurieren Sie die Fernauthentifizierung über RADIUS

Das ExtraHop-System unterstützt den Remote Authentifizierung Dial In User Service (RADIUS) nur für Fernauthentifizierung und lokale Autorisierung. Für die Fernauthentifizierung unterstützt das ExtraHop-System unverschlüsselte RADIUS- und Klartext-Formate.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.
3. Aus dem Methode der Fernauthentifizierung Dropdownliste, wählen **RADIUS** und klicken Sie dann **Fortfahren**.
4. Auf dem RADIUS-Server hinzufügen Seite, geben Sie die folgenden Informationen ein:

   Gastgeber

   Der Hostname oder die IP-Adresse des RADIUS-Servers. Stellen Sie sicher, dass das DNS des ExtraHop-Systems richtig konfiguriert ist, wenn Sie einen Hostnamen angeben.

   Geheim

   Das gemeinsame Geheimnis zwischen dem ExtraHop-System und dem RADIUS-Server. Wenden Sie sich an Ihren RADIUS-Administrator, um das gemeinsame Geheimnis zu erhalten.

   Auszeit

   Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom RADIUS-Server wartet, bevor es erneut versucht, eine Verbindung herzustellen .
5. klicken **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. Klicken Sie **Speichern und fertig**.
8. Aus dem Optionen für die Zuweisung von Rechten Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   - **Remote-Benutzer haben vollen Schreibzugriff**

     Diese Option gewährt Remote-Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
   - **Remote-Benutzer haben vollen Lesezugriff**

     Diese Option gewährt Remote-Benutzern schreibgeschützten Zugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
9. Optional: Konfigurieren Sie den Zugriff auf Paket und Sitzungsschlüssel. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und TLS-Sitzungsschlüsseln zu ermöglichen.

   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
10. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff.

    - **Kein Zugriff**
    - **Voller Zugriff**
11. Klicken Sie **Speichern und fertig**.
12. Klicken Sie **Erledigt**.

Konfigurieren Sie die Fernauthentifizierung über TACACS+

Das ExtraHop-System unterstützt das Terminal Access Controller Access-Control System Plus (TACACS+) für die Fernauthentifizierung und Autorisierung.

Stellen Sie sicher, dass jeder Benutzer, der per Fernzugriff autorisiert werden soll, über die ExtraHop-Dienst, der auf dem TACACS+-Server konfiguriert ist bevor Sie mit diesem Verfahren beginnen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **Fernauthentifizierung**.

3. Aus dem Methode der Fernauthentifizierung Dropdownliste, wählen **TACACS+**, und klicken Sie dann auf **Weiter**.
4. Auf dem TACACS+ Server hinzufügen Seite, geben Sie die folgenden Informationen ein:

   • Gastgeber **:** Der Hostname oder die IP-Adresse des TACACS+-Servers. Stellen Sie sicher, dass das DNS des ExtraHop-Systems richtig konfiguriert ist, wenn Sie einen Hostnamen eingeben.

   • Geheim **:** Das gemeinsame Geheimnis zwischen dem ExtraHop-System und dem TACACS+-Server . Wenden Sie sich an Ihren TACACS+-Administrator, um das gemeinsame Geheimnis zu erhalten.

   Hinweis: Das Geheimnis darf das Nummernzeichen (#) nicht enthalten.

   • Auszeit **:** Die Zeit in Sekunden, die das ExtraHop-System auf eine Antwort vom TACACS+-Server wartet, bevor es erneut versucht, eine Verbindung herzustellen.
5. Klicken Sie **Server hinzufügen**.
6. Optional: Fügen Sie nach Bedarf weitere Server hinzu.
7. Klicken Sie **Speichern und fertig**.
8. Aus dem Optionen für die Zuweisung von Berechtigungen Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:

   - **Berechtigungsstufe vom Remoteserver abrufen**

     Diese Option ermöglicht es Remotebenutzern, Berechtigungsstufen vom Remoteserver zu erhalten. Sie müssen auch Berechtigungen auf dem TACACS+-Server konfigurieren.

   - **Remote-Benutzer haben vollen Schreibzugriff**

     Diese Option gewährt Remote-Benutzern vollen Schreibzugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
   - **Remote-Benutzer haben vollen Lesezugriff**

     Diese Option gewährt Remote-Benutzern schreibgeschützten Zugriff auf das ExtraHop-System. Darüber hinaus können Sie zusätzlichen Zugriff für Paketdownloads, TLS-Sitzungsschlüssel, NDR-Modulzugriff und NPM-Modulzugriff gewähren.
9. Optional: Konfigurieren Sie den Zugriff auf Paket und Sitzungsschlüssel. Wählen Sie eine der folgenden Optionen, um Remote-Benutzern das Herunterladen von Paketerfassungen und TLS-Sitzungsschlüsseln zu ermöglichen.

   - **Kein Zugriff**
   - **Nur Paketsegmente**
   - **Nur Pakete**
   - **Pakete und Sitzungsschlüssel**
10. Optional: Konfigurieren Sie den NDR- und NPM-Modulzugriff.

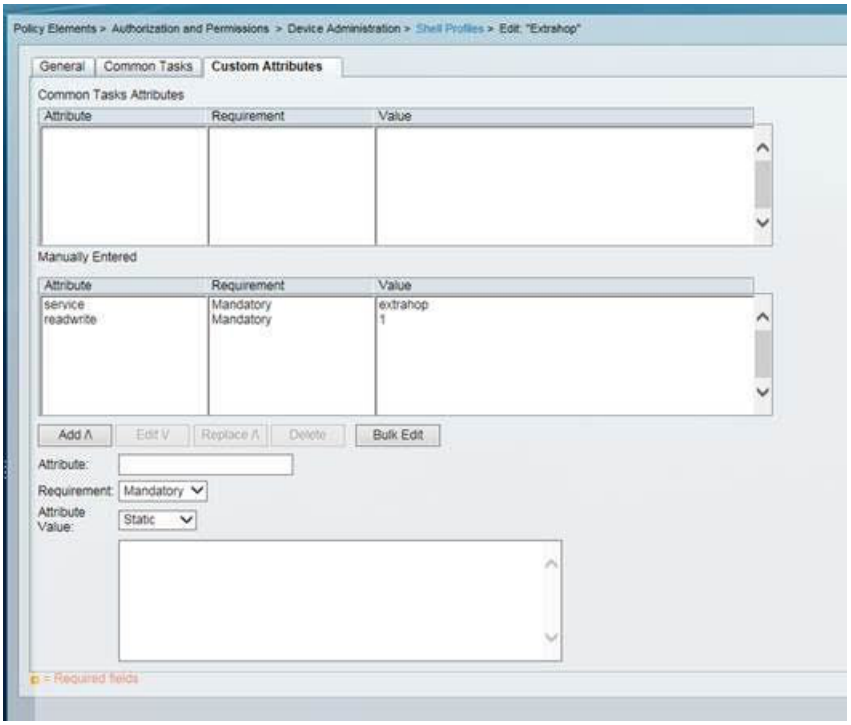
    - **Kein Zugriff**
    - **Voller Zugriff**
11. Klicken Sie **Speichern und fertig**.
12. Klicken Sie **Erledigt**.

Konfigurieren Sie den TACACS+-Server
Zusätzlich zur Konfiguration der Fernauthentifizierung auf Ihrem ExtraHop-System müssen Sie Ihren TACACS+-Server mit zwei Attributen konfigurieren, eines für den ExtraHop-Dienst und eines für die Berechtigungsstufe. Wenn Sie einen ExtraHop-Paketstore haben, können Sie optional ein drittes Attribut für die PCAP und Sitzungsschlüsselprotokollierung hinzufügen.

1. Melden Sie sich bei Ihrem TACACS+-Server an und navigieren Sie zum Shell-Profil für Ihre ExtraHop-Konfiguration.
2. Fügen Sie für das erste Attribut hinzu `Bedienung`.

3. Für den ersten Wert addieren `ExtraHop`.
4. Fügen Sie für das zweite Attribut die Berechtigungsstufe hinzu, z. B. `lesen/schreiben`.
5. Für den zweiten Wert addieren `1`.

Die folgende Abbildung zeigt zum Beispiel `extrahop` Attribut und eine Privilegienstufe von `readwrite`.



Hier ist eine Tabelle mit verfügbaren Berechtigungsattributen, Werten und Beschreibungen:

Attribut	Wert	Beschreibung
`setup`	`1`	Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System und verwalten Sie den Benutzerzugriff
`readwrite`	`1`	Erstellen und ändern Sie alle Objekte und Einstellungen auf dem ExtraHop-System, ohne die Administrationseinstellungen
`limited`	`1`	Dashboards erstellen, ändern und teilen
`readonly`	`1`	Objekte im ExtraHop-System anzeigen
`personal`	`1`	Erstellen Sie persönliche Dashboards für sich selbst und ändern Sie alle Dashboards, die mit ihnen geteilt wurden
`limited_metrics`	`1`	Geteilte Dashboards anzeigen
`ndrfull`	`1`	Sicherheitserkennungen anzeigen, bestätigen und ausblenden

Attribut	Wert	Beschreibung
`npmfull`	`1`	Leistungserkennungen anzeigen, bestätigen und ausblenden
`packetsfull`	`1`	Pakete anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind.
`packetslicesonly`	`1`	Paketsegmente in einem verbundenen Packetstore anzeigen und herunterladen.
`packetsfullwithkeys`	`1`	Pakete und zugehörige Sitzungsschlüssel anzeigen und herunterladen, die in einem verbundenen Packetstore gespeichert sind.

6. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Sicherheitserkennungen anzeigen, bestätigen und ausblenden können

Attribut	Wert
`ndrvoll`	`1`

7. Optional: Fügen Sie das folgende Attribut hinzu, damit Benutzer Leistungserkennungen, die im ExtraHop-System angezeigt werden, anzeigen, bestätigen und ausblenden können.

Attribut	Wert
`npm voll`	`1`

8. Optional: Wenn Sie einen ExtraHop-Paketstore haben, fügen Sie ein Attribut hinzu, damit Benutzer Paketerfassungen oder Paketerfassungen mit zugehörigen Sitzungsschlüsseln herunterladen können.

Attribut	Wert	Beschreibung
`Pakete nur Scheiben`	`1`	Benutzer mit jeder Berechtigungsstufe können die ersten 64 Byte an Paketen anzeigen und herunterladen.
`Pakete voll`	`1`	Benutzer mit jeder Berechtigungsstufe können Pakete, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen.
`Pakete voll mit Schlüsseln`	`1`	Benutzer mit jeder Berechtigungsstufe können Pakete und zugehörige Sitzungsschlüssel, die in einem verbundenen Packetstore gespeichert sind, anzeigen und herunterladen.

API-Zugriff

Auf der Seite API-Zugriff können Sie den Zugriff auf die API-Schlüssel generieren, anzeigen und verwalten, die für die Ausführung von Vorgängen über die ExtraHop REST API erforderlich sind.

API-Schlüsselzugriff verwalten

Benutzer mit System- und Zugriffsadministrationsrechten können konfigurieren, ob Benutzer API-Schlüssel für das ExtraHop-System generieren können. Sie können nur lokalen Benutzern erlauben, Schlüssel zu generieren, oder Sie können die API-Schlüsselgenerierung auch vollständig deaktivieren.

Benutzer müssen einen API-Schlüssel generieren, bevor sie Operationen über die ExtraHop REST API ausführen können. Schlüssel können nur von dem Benutzer, der den Schlüssel generiert hat, oder von Systemadministratoren mit unbegrenzten Rechten eingesehen werden. Nachdem ein Benutzer einen API-Schlüssel generiert hat, muss er den Schlüssel an seine Anforderungsheader anhängen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **API-Zugriff**.
3. In der API-Zugriff verwalten Abschnitt, wählen Sie eine der folgenden Optionen aus:
   - **Allen Benutzern erlauben, einen API-Schlüssel zu generieren**: Lokale und entfernte Benutzer können API-Schlüssel generieren.
   - **Nur lokale Benutzer können einen API-Schlüssel generieren**: Remote-Benutzer können keine API-Schlüssel generieren.
   - **Kein Benutzer kann einen API-Schlüssel generieren**: Es können keine API-Schlüssel von jedem Benutzer generiert werden.
4. klicken **Einstellungen speichern**.

Cross-Origin Resource Sharing (CORS) konfigurieren

Quellübergreifende gemeinsame Nutzung von Ressourcen (CORS) ermöglicht Ihnen den Zugriff auf die ExtraHop REST-API über Domänengrenzen und von bestimmten Webseiten aus, ohne dass die Anfrage über einen Proxyserver übertragen werden muss.

Sie können eine oder mehrere zulässige Ursprünge konfigurieren oder den Zugriff auf die ExtraHop REST-API von jedem beliebigen Ursprung aus zulassen. Nur Benutzer mit System- und Zugriffsadministrationsrechten können CORS-Einstellungen anzeigen und bearbeiten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Auf Einstellungen zugreifen Abschnitt, klicken **API-Zugriff**.
3. In der CORS-Einstellungen Abschnitt, geben Sie eine der folgenden Zugriffskonfigurationen an.
   - Um eine bestimmte URL hinzuzufügen, geben Sie eine Quell-URL in das Textfeld ein und klicken Sie dann auf das Pluszeichen (+) oder drücken Sie die EINGABETASTE.

     Die URL muss ein Schema enthalten, z. B. `HTTP` oder `HTTPS`, und der genaue Domänenname. Sie können keinen Pfad anhängen, Sie können jedoch eine Portnummer angeben.
   - Um den Zugriff von einer beliebigen URL aus zu ermöglichen, wählen Sie die **Erlaube API-Anfragen von jedem Ursprung** Ankreuzfeld.

     Hinweis: Das Zulassen des REST-API-Zugriffs von einem beliebigen Ursprung aus ist weniger sicher als das Bereitstellen einer Liste expliziter Ursprünge.
4. Klicken Sie **Einstellungen speichern** und klicken Sie dann **Erledigt**.

Generieren Sie einen API-Schlüssel

Sie müssen einen API-Schlüssel generieren, bevor Sie Operationen über die ExtraHop REST-API ausführen können. Schlüssel können nur von dem Benutzer eingesehen werden, der den Schlüssel generiert hat, oder von Benutzern mit System - und Zugriffsadministrationsrechten. Nachdem Sie einen API-Schlüssel generiert haben, fügen Sie den Schlüssel zu Ihren Anforderungsheadern oder dem ExtraHop REST API Explorer hinzu.

Bevor Sie beginnen
Stellen Sie sicher, dass das ExtraHop-System konfiguriert, um die Generierung von API-Schlüsseln zu ermöglichen.

1. In der Auf Einstellungen zugreifen Abschnitt, klicken Sie **API-Zugriff**.
2. In der Generieren Sie einen API-Schlüssel Abschnitt, geben Sie eine Beschreibung für den neuen Schlüssel ein, und klicken Sie dann auf **Generieren**.
3. Scrollen Sie nach unten zum API-Schlüssel Abschnitt und kopieren Sie den API-Schlüssel , der Ihrer Beschreibung entspricht.

Sie können den Schlüssel in den REST API Explorer einfügen oder den Schlüssel an einen Anforderungsheader anhängen.

Privilegienstufen

Die Benutzerberechtigungsstufen bestimmen, welche ExtraHop-System- und Verwaltungsaufgaben der Benutzer über die ExtraHop-REST-API ausführen kann.

Sie können die Berechtigungsstufen für Benutzer über das `granted_roles` und `effective_roles` Eigenschaften. Das `granted_roles` Diese Eigenschaft zeigt Ihnen, welche Rechtestufen dem Benutzer explizit gewährt werden. Das `effective_roles` Diese Eigenschaft zeigt Ihnen alle Berechtigungsstufen für einen Benutzer an, einschließlich derer, die Sie außerhalb der erteilten Rolle erhalten haben, z. B. über eine Benutzergruppe.

Das `granted_roles` und `effective_roles` Eigenschaften werden durch die folgenden Operationen zurückgegeben:

- GET /users
- GET /users/ {username}

Das `granted_roles` und `effective_roles` Eigenschaften unterstützen die folgenden Berechtigungsstufen. Beachten Sie, dass die Art der Aufgaben für jedes ExtraHop-System je nach Verfügbarkeit variiert Ressourcen sind im REST API Explorer aufgeführt und hängen von den Modulen ab, die für die System- und Benutzermodulzugriffsrechte aktiviert sind.

Privilegienstufe	Zulässige Aktionen
„system“: „voll“	• Aktiviert oder deaktiviert die API-Schlüsselgenerierung für das ExtraHop-System. • Generieren Sie einen API-Schlüssel. • Sehen Sie sich die letzten vier Ziffern und die Beschreibung für jeden API-Schlüssel auf dem System an. • Löschen Sie API-Schlüssel für jeden Benutzer. • CORS anzeigen und bearbeiten. • Führen Sie alle Verwaltungsaufgaben aus, die über die REST-API verfügbar sind. • Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind.
„write“: „voll“	• Generieren Sie Ihren eigenen API-Schlüssel. • Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn.

Privilegienstufe	Zulässige Aktionen
	• Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. • Führen Sie alle ExtraHop-Systemaufgaben aus, die über die REST-API verfügbar sind.
„write“: „begrenzt“	• Generieren Sie einen API-Schlüssel. • Zeigen Sie ihren eigenen API-Schlüssel an oder löschen Sie ihn. • Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. • Führen Sie alle GET-Operationen über die REST-API aus. • Führen Sie Metrik- und Datensatzabfragen durch.
„write“: „persönlich“	• Generieren Sie einen API-Schlüssel. • Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn. • Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. • Führen Sie alle GET-Operationen über die REST-API aus. • Führen Sie Metrik- und Datensatzabfragen durch.
„Metriken“: „voll“	• Generieren Sie einen API-Schlüssel. • Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn. • Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen. • Führen Sie Metrik- und Datensatzabfragen durch.
„metrics“: „eingeschränkt“	• Generieren Sie einen API-Schlüssel. • Zeigen Sie Ihren eigenen API-Schlüssel an oder löschen Sie ihn. • Ändern Sie Ihr eigenes Passwort, aber Sie können keine anderen Verwaltungsaufgaben über die REST-API ausführen.
„ndr“: „voll“	• Sicherheitserkennungen anzeigen • Untersuchungen anzeigen und erstellen Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„ndr“: „keiner“	• Kein Zugriff auf NDR-Modulinhalte Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“

Privilegienstufe	Zulässige Aktionen
	• „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„npm“: „voll“	• Leistungserkennungen anzeigen • Dashboards anzeigen und erstellen • Benachrichtigungen anzeigen und erstellen Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„npm“: „keine“	• Kein Zugriff auf NPM-Modulinhalte Dies ist ein Modulzugriffsrecht, das einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„Pakete“: „voll“	• Pakete anzeigen und herunterladen über das `GET /packets/search` und `POST /packets/search` Operationen. Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„Pakete“: „voll_mit_Schlüsseln“	• Pakete und Sitzungsschlüssel anzeigen und herunterladen über das `GET /packets/search` und `POST /packets/search` Operationen. Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“

Privilegienstufe	Zulässige Aktionen
	• „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“
„Pakete“: „slices_only“	• Sehen Sie sich die ersten 64 Byte an Paketen an und laden Sie sie herunter über die `GET /packets/search` und `POST /packets/search` Operationen. Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „Metriken“: „voll“ • „metrics“: „eingeschränkt“

Konfiguration des Systems

In der Konfiguration des Systems In diesem Abschnitt können Sie die folgenden Einstellungen ändern.

Erfassen

Konfigurieren Sie die Netzwerkaufzeichnungseinstellungen. (Nur Sensoren)

Datenspeicher

Konfigurieren Sie einen erweiterten Datenspeicher oder setzen Sie den lokalen Datenspeicher zurück. (Nur Sensoren)

Benennung von Geräten

Konfigurieren Sie die Rangfolge, wenn mehrere Namen für ein Gerät gefunden werden.

Inaktive Quellen

Entfernen Sie Geräte und Anwendungen, die zwischen 1 und 90 Tagen inaktiv waren, aus den Suchergebnissen.

Erkennungsverfolgung

Wählen Sie aus, ob die Erkennungsuntersuchungen mit dem ExtraHop-System oder von einem externen Ticketsystem aus verfolgt werden sollen.

Endpunktsuche

Konfigurieren Sie Links zu einem externen IP-Adress-Suchtool für Endpunkte im ExtraHop-System .

Geomap-Datenquelle

Ändern Sie die Informationen in kartierten Geolokationen.

Datenströme öffnen

Senden Sie Protokolldaten an ein Drittanbietersystem, z. B. ein Syslog-System, eine MongoDB-Datenbank oder einen HTTP-Server. (Nur Sensoren)

Tendenzen

Setze alle Trends und trendbasierten Benachrichtigungen zurück. (Nur Sensoren).

Sichern und Wiederherstellen

System-Backups erstellen, anzeigen oder wiederherstellen.

Erfassen

Die Capture-Seite bietet Steuerelemente, mit denen Sie einstellen können, wie das ExtraHop-System Ihren Netzwerkverkehr zur Analyse erfasst.

Protokollmodule ausschließen

Standardmäßig sind alle unterstützten Module auf dem ExtraHop-System in der Erfassung enthalten, sofern Sie sie nicht manuell ausschließen.

1. Klicken Sie **Konfiguration des Systems** > **Erfassen**.
2. Klicken Sie **Ausgeschlossene Protokollmodule**.
3. Hinzufügen **Auszuschließendes Modul**.
4. Auf dem Wählen Sie das auszuschließende Protokollmodul aus Seite, von der **Name des Moduls** Wählen Sie in der Dropdownliste das Modul aus, das Sie von der Erfassung ausschließen möchten .
5. Klicken Sie **Hinzufügen**.
6. Auf dem Ausgeschlossene Protokollmodule Seite, klicken **Capture neu starten**.
7. Nachdem die Aufnahme neu gestartet wurde, klicken Sie auf **OK**.

Um das Modul wieder aufzunehmen, klicken Sie auf das rote X, um es aus der Liste der aktuell ausgeschlossenen Module zu löschen.

MAC-Adressen ausschließen

Fügen Sie Filter hinzu, um bestimmte MAC-Adressen oder den Geräteverkehr eines Anbieters von der Netzwerkerfassung auszuschließen

1. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
2. Klicken Sie **MAC-Adressfilter**.
3. Klicken Sie **Filter hinzufügen**.
4. In der MAC-Adresse Feld, geben Sie die MAC-Adresse ein, die ausgeschlossen werden soll.
5. In der Maske Feld, geben Sie die Maske ein, um anzugeben, wie viele Bits der Filter von links nach rechts mit der MAC-Adresse vergleicht.
6. Klicken Sie **Hinzufügen**.

   Im folgenden Beispiel wird die vollständige MAC-Adresse von der Erfassung ausgeschlossen:

   • **MAC-Adresse:** `60:98:2 D:B1:EC:42`

   • **Maske:** `FF:FF:FF:FF:FF:FF`

   In diesem Beispiel werden nur die ersten 24 Bits zum Ausschluss ausgewertet:

   • **MAC-Adresse:** `60:98:2 D:B1:EC:42`

   • **Maske:** `FF:FF:FF: 00:00:00`

Um eine MAC-Adresse erneut hinzuzufügen, klicken Sie auf **Löschen** um die Adresse aus der Liste zu entfernen.

Eine IP-Adresse oder einen Bereich ausschließen

Fügen Sie Filter hinzu, um bestimmte IP-Adressen und IP-Bereiche von der Netzwerkerfassung auf dem ExtraHop-System auszuschließen.

1. klicken **Konfiguration des Systems** > **Erfassen**.
2. klicken **IP-Adressfilter**.
3. klicken **Filter hinzufügen**.
4. Auf dem IP-Adressfilter Seite, geben Sie entweder eine einzelne IP-Adresse ein, die Sie ausschließen möchten, oder eine IP-Adressmaske im CIDR-Format für einen Bereich von IP-Adressen, den Sie ausschließen möchten.
5. Klicken Sie **Hinzufügen**.

Um eine IP-Adresse oder einen Bereich erneut einzuschließen, klicken Sie auf **Löschen** neben dem Filter für jede Adresse.

Einen Port ausschließen

Fügen Sie Filter hinzu, um den Datenverkehr von bestimmten Ports von der Netzwerkerfassung auf dem ExtraHop-System auszuschließen.

1. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
2. Klicken Sie **Port-Filter**.
3. Klicken Sie **Filter hinzufügen**.
4. Auf dem Portfilter hinzufügen Seite, geben Sie den Port ein, den Sie ausschließen möchten.
   - Um einen Quellport anzugeben, den Sie ausschließen möchten, geben Sie die Portnummer in das Quellport Feld.
   - Um einen Zielport anzugeben, den Sie ausschließen möchten, geben Sie die Portnummer in das Zielhafen Feld.

5. Aus dem **IP-Protokoll** Wählen Sie in der Dropdownliste das Protokoll aus, das Sie auf dem angegebenen Port ausschließen möchten.
6. Klicken Sie **Hinzufügen**.

Um einen Port erneut einzuschließen, klicken Sie auf **Löschen** neben dem Hafen.

Filterung und Datendeduplikation

In der folgenden Tabelle finden Sie die Auswirkungen von Filterung und Datendeduplikation auf Metriken, PCAP und Geräteerkennung. Die Deduplizierung ist auf dem System standardmäßig aktiviert.

Paket gelöscht von	MAC-Adressfilter	IP-Adressfilter	Anschlussfilter	L2-Deduplizierung	L3-Deduplizierung
Netzwerk-VLAN L2-Metriken	Nicht gesammelt	Nicht gesammelt	Nicht fragmentiert*: Nicht gesammelt Fragmentiert: Gesammelt	Nicht gesammelt	Gesammelt
Netzwerk-VLAN L3-Metriken	Nicht gesammelt	Nicht gesammelt	Nicht fragmentiert: Nicht gesammelt Fragmentiert: Gesammelt	Nicht gesammelt	Gesammelt
L2/L3-Metriken für Geräte	Nicht gesammelt	Nicht gesammelt	Nicht fragmentiert: Nicht gesammelt Fragmentiert, auf oberster Ebene: Gesammelt Fragmentiert, Detail: Nicht gesammelt	Nicht gesammelt	Gesammelt
Globale PCAP-Pakete	Gefangen	Gefangen	Gefangen	Gefangen	Gefangen
Precision PCAP-Pakete	Nicht erfasst	Nicht erfasst	Nicht erfasst	Nicht erfasst	Gefangen
L2-Geräteerkennung	Keine Entdeckung	Entdeckung	Entdeckung	--	--
L3-Geräteerkennung	Keine Entdeckung	Keine Entdeckung	Nicht fragmentiert: Keine Entdeckung Fragmentiert: Discovery	--	--

*Wenn bei Portfiltern IP-Fragmente im Datenfeed vorhanden sind, wird bei der erneuten Zusammenstellung des Fragments keine Portnummer bestimmt. Das ExtraHop-System sammelt möglicherweise Messwerte, erfasst Pakete oder erkennt ein Gerät, auch wenn die Port-Filterregel dies andernfalls ausschließt.

L2-Duplikate sind identische Ethernet-Frames. Die doppelten Frames sind normalerweise nicht auf der Leitung vorhanden, sondern sind ein Artefakt der Datenfeed-Konfiguration. L3-Duplikate sind Frames, die sich nur im L2-Header und IP-TTL unterscheiden. Diese Frames entstehen normalerweise durch Tippen auf beiden Seiten eines Routers. Da diese Frames im überwachten Netzwerk vorhanden sind, werden sie an den oben genannten Orten auf L2 und L3 gezählt. Die L3-Deduplizierung ist beispielsweise auf L4 und höher ausgerichtet, um zu vermeiden, dass die L3-Duplikate als TCP-Neuübertragungen gezählt werden.

Klassifizierung des Protokolls

Die Protokollklassifizierung basiert auf bestimmten Nutzlasten, um benutzerdefinierte Protokolle über bestimmte Ports zu identifizieren. Bei diesen Protokollen handelt es sich um Layer-7-Protokolle (Anwendungsebene), die über dem Layer-4-Protokoll (TCP oder UDP) liegen. Diese Anwendungen haben ihr eigenes benutzerdefiniertes Protokoll und verwenden auch das TCP-Protokoll.

Das Klassifizierung des Protokolls Seite bietet eine Schnittstelle zur Ausführung der folgenden Funktionen:

- Listet Anwendungen und Ports für die folgenden Netzwerkentitäten auf:
  - Allgemein bekannte Anwendungen, die nicht standardmäßigen Ports zugeordnet sind.
  - Weniger bekannte und benutzerdefinierte Netzwerkanwendungen.
  - Unbenannte Anwendungen mit TCP- und UDP-Verkehr (z. B. TCP 1234).
- Fügen Sie eine benutzerdefinierte Protokoll-Anwendungs-Zuordnung hinzu, die die folgenden Informationen enthält:

  Name

  Der vom Benutzer angegebene Protokollname.

  Protokoll

  Das gewählte Layer-4-Protokoll (TCP oder UDP).

  Quelle

  (Optional) Der angegebene Quellport. Port 0 gibt einen beliebigen Quellport an.

  Reiseziel

  Der Zielport oder der Bereich von Anschlüssen.

  Lose Initiation

  Wählen Sie dieses Kontrollkästchen, wenn der Klassifikator versuchen soll, die Verbindung zu kategorisieren, ohne dass die Verbindung geöffnet ist. ExtraHop empfiehlt, für langlebige Abläufe eine lockere Initiierung zu wählen.

  Standardmäßig verwendet das ExtraHop-System eine lose initiierte Protokollklassifizierung und versucht daher, zu klassifizieren Flüsse auch nachdem die Verbindung initiiert wurde. Sie können die lose Initiierung für Ports deaktivieren, die nicht immer den Protokollverkehr übertragen (z. B. den Platzhalterport 0).
- Löschen Sie Protokolle mit dem ausgewählten Anwendungsnamen und der Portzuordnung aus der Liste.

  Der Name und der Port der Anwendung werden weder im ExtraHop-System noch in Berichten angezeigt, die auf zukünftigen Datenerfassungen basieren. Das Gerät erscheint in Berichten mit historischen Daten, wenn das Gerät innerhalb des gemeldeten Zeitraums aktiv und auffindbar war.
- Starten Sie die Netzwerkaufnahme neu.
  - Sie müssen die Netzwerkaufzeichnung neu starten, bevor Änderungen an der Protokollklassifizierung wirksam werden.
  - Zuvor gesammelte Erfassungsdaten werden beibehalten.

Das ExtraHop-System erkennt die meisten Protokolle an ihren Standardports mit einigen Ausnahmen. In der Performance Edition werden die folgenden Protokolle an jedem Port erkannt:

- AJP
- DTLS
- FIX
- HTTP
- HTTP2
- IIOP
- Java-RMI
- LDAP
- RPC
- SSH
- TLS

Auf RevealX 360 werden die folgenden Protokolle an jedem Port erkannt:

- Ethminer
- Blockvorlage abrufen
- RDP
- RFB
- Schicht
- LDAP
- Java-RMI
- IIOP

Wenn ein Protokoll über einen nicht standardmäßigen Port kommuniziert, ist es in einigen Fällen erforderlich, den nicht standardmäßigen Port auf der Seite „Protokollklassifizierung“ hinzuzufügen. In diesen Fällen ist es wichtig, den nicht standardmäßigen Port richtig zu benennen. In der folgenden Tabelle sind die Standardports für jedes der Protokolle zusammen mit dem Protokollnamen aufgeführt, der beim Hinzufügen der benutzerdefinierten Portnummern auf der Seite „Protokollklassifizierung“ angegeben werden muss.

In den meisten Fällen ist der von Ihnen eingegebene Name mit dem Namen des Protokoll identisch. Die häufigsten Ausnahmen von dieser Regel sind Oracle (wo der Protokollname TNS ist) und Microsoft SQL (wo der Protokollname TDS ist).

Wenn Sie einen Protokollnamen hinzufügen, der mehrere Zielports hat, fügen Sie den gesamten Portbereich hinzu, getrennt durch einen Bindestrich (-). Wenn Ihr Protokoll beispielsweise das Hinzufügen der Ports 1434, 1467 und 1489 für den Datenbankverkehr erfordert, geben Sie `1434-1489` in der Zielhafen Feld. Fügen Sie alternativ jeden der drei Ports in drei separaten Protokollklassifizierungen mit demselben Namen hinzu.

Kanonischer Name	Name des Protokolls	Verkehr	Standard-Quellport	Standard-Zielport
ActiveMQ	ActiveMQ	TCP	0	61616
AJP	AJP	TCP	0	8009
DB2	DB2	TCP	0	50000, 60000
DHCP	DHCP	TCP	68	67
Durchmesser	AAA	TCP	0	3868
DICOM	DICOM	TCP	0	3868
DNS	DNS	TCP, UDP	0	53

Kanonischer Name	Name des Protokolls	Verkehr	Standard-Quellport	Standard-Zielport
FIX	FIX	TCP	0	0
FTP	FTP	TCP	0	21
FTP-DATEN	FTP-DATEN	TCP	0	20
HL7	HL7	TCP, UDP	0	2575
HTTPS	HTTPS	TCP	0	443
IBM MQ	IBMMQ	TCP, UDP	0	1414
ICA	ICA	TCP	0	1494, 2598
IKE	IKE	UDP	0	500
IMAP	IMAP	TCP	0	143
IMAPS	IMAPS	TCP	0	993
Informix	Informix	TCP	0	1526, 1585
IPSEC	IPSEC	TCP, UDP	0	1293
IPX	IPX	TCP, UDP	0	213
IRC	IRC	TCP	0	6660-6669
ISAKMP	ISAKMP	UDP	0	500
iSCSI	iSCSI	TCP	0	3260
Kerberos	Kerberos	TCP, UDP	0	88
LDAP	LDAP	TCP	0	389, 390, 3268
LLDP	LLDP	Link-Ebene	N/A	N/A
L2TP	L2TP	UDP	0	1701
Memcache	Memcache	TCP	0	11210, 11211
Modbus	Modbus	TCP	0	502
MongoDB	MongoDB	TCP	0	27017
MS SQL Server	TDS	TCP	0	1433
MSMQ	MSMQ	TCP	0	1801
MSRPC	MSRPC	TCP	0	135
MySQL	MySQL	TCP	0	3306
NetFlow	NetFlow	UDP	0	2055
NFS	NFS	TCP	0	2049
NFS	NFS	UDP	0	2049
NTP	NTP	UDP	0	123
OpenVPN	OpenVPN	UDP	0	1194
Orakel	TNS	TCP	0	1521
PCoIP	PCoIP	UDP	0	4172

Kanonischer Name	Name des Protokolls	Verkehr	Standard-Quellport	Standard-Zielport
POP3	POP3	TCP	0	143
POP 3	POP 3	TCP	0	995
PostgreSQL	PostgreSQL	TCP	0	5432
RADIUS	AAA	TCP	0	1812, 1813
RADIUS	AAA	UDP	0	1645, 1646, 1812, 1813
RDP	RDP	TCP	0	3389
Redis	Redis	TCP	0	6397
RFB	RFB	TCP	0	5900
SCCP	SCCP	TCP	0	2000
SIP	SIP	TCP	0	5060, 5061
SMB	SMB	TCP	0	139, 445
SMPP	SMPP	TCP	0	2775
SMTP	SMTP	TCP	0	25
SNMP	SNMP	UDP	0	162
SSH	SSH	TCP	0	0
Sybase	Sybase	TCP	0	10200
Sybase IQ	Sybase IQ	TCP	0	2638
Syslog	Syslog	UDP	0	514
Telnet	Telnet	TCP	0	23
TLS	TLS	TCP	0	443
VNC	VNC	TCP	0	5900
WebSocket	WebSocket	TCP	0	80, 443
Optimierung der Windows Update-Bereitstellung	Optimierung der Windows Update-Bereitstellung	TCP	0	7860

Der in der Spalte Protokollname der Tabelle angegebene Name wird auf der Seite „ Protokollklassifizierung“ angezeigt, um ein allgemeines Protokoll zu klassifizieren, das über nicht standardmäßige Ports kommuniziert.

Zu den Protokollen im ExtraHop-System, die in dieser Tabelle nicht aufgeführt sind, gehören die folgenden:

HTTP

Das ExtraHop-System klassifiziert HTTP auf allen Ports.

HTTP-AMF

Dieses Protokoll läuft auf HTTP und wird automatisch klassifiziert.

Zu den Protokollen in dieser Tabelle, die nicht im ExtraHop-System erscheinen, gehören die folgenden:

FTP-DATEN

Das ExtraHop-System verarbeitet keine FTP-DATEN auf nicht standardmäßigen Ports.

LLDP

Da es sich um ein Protokoll auf Linkebene handelt, gilt die portbasierte Klassifizierung nicht.

Fügen Sie eine benutzerdefinierte Protokollklassifizierung hinzu

Das folgende Verfahren beschreibt, wie Sie benutzerdefinierte hinzufügen Protokoll Klassifizierungsetiketten mit dem TDS-Protokoll (MS SQL Server) als Beispiel.

Standardmäßig sucht das ExtraHop-System auf dem TCP-Port 1433 nach TDS-Verkehr. Gehen Sie wie folgt vor, um MS SQL Server TDS-Parsing auf einem anderen Port hinzuzufügen.

1. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
2. Klicken Sie **Klassifizierung des Protokolls**.
3. Klicken Sie **Protokoll hinzufügen**.
4. Auf dem Klassifizierung des Protokolls Seite, geben Sie die folgenden Informationen ein:

   Name

   Wählen Sie aus dem Drop-down-Menü **Benutzerdefiniertes Etikett hinzufügen...**.

   Name

   Geben Sie TDS für den Namen des benutzerdefinierten Protokoll ein.

   Protokoll

   Wählen Sie aus der Dropdownliste ein L4-Protokoll aus, das dem benutzerdefinierten Protokoll zugeordnet werden soll (in diesem Beispiel TCP).

   Quelle

   Der Quellport für das benutzerdefinierte Protokoll. (Der Standardwert 0 gibt einen beliebigen Quellport an.)

   Reiseziel

   Der Zielport für das benutzerdefinierte Protokoll. Um einen Bereich von Anschlüssen anzugeben, setzen Sie einen Bindestrich zwischen den ersten und letzten Port im Bereich. Zum Beispiel `3400-4400`.

   Lose Initiation

   Wählen Sie dieses Kontrollkästchen, wenn der Klassifikator versuchen soll, die Verbindung zu kategorisieren, ohne dass die Verbindung geöffnet ist. ExtraHop empfiehlt, für langlebige Abläufe eine lockere Initiierung zu wählen.

   Standardmäßig verwendet das ExtraHop-System eine lose initiierte Protokollklassifizierung und versucht daher, zu klassifizieren Flüsse auch nachdem die Verbindung initiiert wurde. Sie können die lose Initiierung für Ports deaktivieren, die nicht immer den Protokollverkehr übertragen (z. B. den Platzhalterport 0).
5. Klicken Sie **Hinzufügen**.
6. Bestätigen Sie die Einstellungsänderung und klicken Sie dann auf **Capture neu starten** damit die Änderung wirksam wird.

   Dadurch wird die Datenerfassung kurzzeitig unterbrochen. Nach dem Neustart der Aufnahme wird eine Bestätigungsmeldung angezeigt.
7. Klicken Sie **Erledigt**.
8. Klicken Sie **Änderungen anzeigen und speichern** oben auf dem Bildschirm.

   Diese Änderung wurde auf die laufende Konfigurationsdatei angewendet. Wenn Sie die Änderung in der laufenden Konfigurationsdatei speichern, wird sie beim Neustart des ExtraHop-Systems erneut angewendet.
9. Klicken Sie **Speichern** um die Änderung in die Standardkonfiguration zu schreiben.

   Nachdem die Konfiguration gespeichert wurde, erscheint eine Bestätigungsmeldung.

10. Klicken Sie **Erledigt**.

Datenbank Statistiken werden jetzt für alle Geräte angezeigt, auf denen TDS auf dem hinzugefügten Port läuft (in diesem Beispiel 65000). Diese Einstellung wird auf die gesamte Aufnahme angewendet, sodass Sie sie nicht pro Gerät hinzufügen müssen.

Geräteerkennung konfigurieren

Das ExtraHop-System kann Geräte anhand ihrer MAC-Adresse (L2 Discovery) oder anhand ihrer IP-Adressen (L3 Discovery) erkennen und verfolgen. L2 Discovery bietet den Vorteil, dass Messwerte für ein Gerät auch dann verfolgt werden können, wenn die IP-Adresse durch eine DHCP-Anfrage geändert oder neu zugewiesen wird. Das System kann VPN-Clients auch automatisch erkennen.

Bevor Sie beginnen
Erfahre wie Geräteerkennung und L2-Entdeckung funktioniert im ExtraHop-System. Das Ändern dieser Einstellungen wirkt sich darauf aus, wie Metriken mit Geräten verknüpft werden.

Hinweis: Paketbroker können ARP-Anfragen filtern. Das ExtraHop-System stützt sich auf ARP-Anfragen, um L3-IP-Adressen mit L2-MAC-Adressen zu verknüpfen.

Entdecken Sie lokale Geräte
Wenn Sie L3 Discovery aktivieren, werden lokale Geräte anhand ihrer IP-Adresse verfolgt. Das System erstellt einen übergeordneten L2-Eintrag für die MAC-Adresse und einen untergeordneten L3-Eintrag für die IP-Adresse. Wenn sich die IP-Adresse für ein Gerät im Laufe der Zeit ändert, wird möglicherweise ein einziger Eintrag für ein L2-Elternteil mit einer MAC-Adresse mit mehreren untergeordneten L3-Einträgen mit unterschiedlichen IP-Adressen angezeigt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **Gerätesuche**.
4. In der Lokale Gerätesuche Abschnitt, wählen Sie aus den folgenden Optionen:
   - Wählen Sie die **Lokale Geräteerkennung aktivieren** Kontrollkästchen , um L3 Discovery zu aktivieren.
   - Löschen Sie das **Lokale Geräteerkennung aktivieren** Kontrollkästchen , um L2 Discovery zu aktivieren.
5. Klicken Sie **Speichern**.

Ermitteln Sie Remote-Geräte anhand der IP-Adresse
Sie können das ExtraHop-System so konfigurieren, dass Geräte in Remote-Subnetzen automatisch erkannt werden, indem Sie eine Reihe von IP-Adressen hinzufügen.

Hinweis: Wenn Ihr ExtraHop-System für L2 Discovery konfiguriert ist und Ihre Remote-Geräte IP-Adressen über einen DHCP-Relay-Agenten anfordern, können Sie Geräte anhand ihrer MAC-Adresse verfolgen, und Sie müssen Remote L3 Discovery nicht konfigurieren. Erfahre mehr über Geräteerkennung.

Wichtige Überlegungen zu Remote L3 Discovery:

- L2-Informationen wie die MAC-Adresse des Geräts und der L2-Verkehr sind nicht verfügbar, wenn sich das Gerät in einem anderen Netzwerk befindet als dem, das vom ExtraHop-System überwacht wird. Diese Informationen werden nicht von Routern weitergeleitet und sind daher für das ExtraHop-System nicht sichtbar.
- Seien Sie vorsichtig, wenn Sie die CIDR-Notation angeben. Ein /24-Subnetzpräfix kann dazu führen , dass 255 neue Geräte vom ExtraHop-System entdeckt werden. Ein breites /16-Subnetzpräfix kann dazu führen, dass 65.535 neue Geräte entdeckt werden, was Ihr Gerätelimit überschreiten könnte.
- Wenn eine IP-Adresse aus den Remote L3 Gerät Discovery-Einstellungen entfernt wird, bleibt die IP-Adresse im ExtraHop-System als Remote-L3-Gerät bestehen, solange aktive Datenflüsse für diese IP-

Adresse existieren oder bis die Erfassung neu gestartet wird. Nach einem Neustart wird das Gerät als inaktives Remote-L3-Gerät aufgeführt.

Wenn dieselbe IP-Adresse später über den lokalen Datenfeed hinzugefügt wird, kann dieses entfernte L3-Gerät zu einem lokalen L3-Gerät wechseln, jedoch nur, wenn der Erfassungsvorgang neu gestartet und die Einstellung Local Device Discovery aktiviert ist.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Geräteerkennung**.
4. In der Geräteerkennung aus der Ferne Abschnitt, in der IP-Adressbereiche Feld, geben Sie die IP-Adresse ein.

   Sie können eine IP-Adresse oder eine CIDR-Notation angeben, z. B. `192.168.0.0/24` für ein IPv4-Netzwerk oder `2001:db8::/32` für ein IPv6-Netzwerk.

   Wichtig: Jede aktiv kommunizierende Remote-IP-Adresse, die dem CIDR-Block entspricht, wird im ExtraHop-System als einzelnes Gerät erkannt. Die Angabe breiter Subnetzpräfixe wie /16 kann dazu führen, dass Tausende von Geräten erkannt werden, wodurch Ihr Gerätelimit möglicherweise überschritten wird.
5. Klicken Sie auf das grüne Plussymbol (**+**), um die IP-Adresse hinzuzufügen. Sie können eine weitere IP-Adresse oder einen weiteren IP-Adressbereich hinzufügen, indem Sie die Schritte 4 bis 5 wiederholen.

   Wichtig: Der Erfassungsvorgang muss beim Entfernen von IP-Adressbereichen neu gestartet werden, bevor die Änderungen wirksam werden. Wir empfehlen, alle Einträge zu löschen, bevor Sie den Erfassungsvorgang neu starten. Der Erfassungsvorgang muss beim Hinzufügen von IP-Adressbereichen nicht neu gestartet werden.

Entdecken Sie VPN-Clients
Ermöglichen Sie die Erkennung interner IP-Adressen, die VPN-Clientgeräten zugeordnet sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **Gerätesuche**.
4. In der VPN-Client-Erkennung Abschnitt, wählen Sie aus den folgenden Optionen:
   - Wählen Sie die **VPN-Client-Erkennung aktivieren** Kontrollkästchen , um die VPN-Client-Erkennung zu aktivieren.
   - Löschen Sie das **VPN-Client-Erkennung aktivieren** Kontrollkästchen, um die VPN-Client-Erkennung zu deaktivieren.
5. Klicken Sie **Speichern**.

TLS-Entschlüsselung

Das ExtraHop-System unterstützt die Echtzeit-Entschlüsselung von TLS-Verkehr zur Analyse. Bevor das System Ihren Datenverkehr entschlüsseln kann, müssen Sie die Weiterleitung von Sitzungsschlüsseln konfigurieren oder ein TLS-Serverzertifikat und einen privaten Schlüssel hochladen. Das Serverzertifikat und die privaten Schlüssel werden über eine HTTPS-Verbindung von einem Webbrowser auf das ExtraHop-System hochgeladen.

Hinweis: Ihr Serververkehr muss mit einem von verschlüsselt werden diese unterstützten Cipher Suites.

Hilfe auf dieser Seite

- Entschlüsseln Sie den TLS-Verkehr mit Sitzungsschlüsselweiterleitung ohne private Schlüssel.
  - Deaktivieren Sie das Kontrollkästchen für **Private Schlüssel erforderlich**.

- Installieren Sie die Sitzungsschlüsselweiterleitungssoftware auf Ihrem Linux oder Windows Server.
- Einen globalen Port zur Protokollzuordnung hinzufügen für jedes Protokoll, das Sie entschlüsseln möchten.

- Entschlüsseln Sie den TLS-Verkehr, indem Sie ein Zertifikat und einen privaten Schlüssel hochladen.
  - Laden Sie ein PEM-Zertifikat und einen privaten RSA-Schlüssel hoch oder Laden Sie eine PKCS #12 /PFX-Datei hoch
  - Verschlüsselte Protokolle hinzufügen

Hinweis: Für die TLS-Entschlüsselung ist eine Lizenz erforderlich. Wenn Sie jedoch eine Lizenz für MS SQL haben, können Sie auch ein TLS-Zertifikat hochladen, um den MS SQL-Verkehr aus diesen Einstellungen zu entschlüsseln.

Laden Sie ein PEM-Zertifikat und einen privaten RSA-Schlüssel hoch

Hinweis: Sie können einen kennwortgeschützten Schlüssel exportieren, um ihn Ihrem ExtraHop-System hinzuzufügen, indem Sie den folgenden Befehl in einem Programm wie OpenSSL ausführen:

```
openssl rsa -in yourcert.pem -out new.key
```

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, wählen Sie das Kontrollkästchen für **Private Schlüssel erforderlich**.
5. Klicken Sie **Speichern**.
6. In der Private Schlüssel Abschnitt, klicken **Schlüssel hinzufügen**.
7. In der Name Feld, geben Sie einen beschreibenden Namen zur Identifizierung dieses Zertifikats und Schlüssels ein.
8. Löschen Sie das **Aktiviert** Checkbox, wenn Sie dieses TLS-Zertifikat deaktivieren möchten.
9. In der Zertifikat Feld, fügen Sie das Public-Key-Zertifikat ein.
10. In der Privater Schlüssel Feld, fügen Sie den privaten RSA-Schlüssel ein.
11. Klicken Sie **Hinzufügen**.

Nächste Schritte
Fügen Sie die verschlüsselten Protokolle hinzu Sie möchten mit diesem Zertifikat entschlüsseln.

Laden Sie eine PKCS #12 /PFX-Datei hoch

PKCS #12 /PFX-Dateien werden in einem sicheren Container auf dem ExtraHop-System archiviert und enthalten sowohl öffentliche als auch private Schlüsselpaare, auf die nur mit einem Passwort zugegriffen werden kann.

Hinweis: Um private Schlüssel aus einem Java KeyStore in eine PKCS #12 -Datei zu exportieren, führen Sie den folgenden Befehl auf Ihrem Server aus, wobei `javakeystore.jks` ist der Pfad Ihres Java-KeyStores:

```
keytool -importkeystore -srckeystore javakeystore.jks -
destkeystore
pkcs.p12 -srcstoretype jks -deststoretype pkcs12
```

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.

4. In der Entschlüsselung des privaten Schlüssels Abschnitt, wählen Sie das Kontrollkästchen für **Private Schlüssel erforderlich**.
5. Klicken Sie **Speichern**.
6. In der Private Schlüssel Abschnitt, klicken Sie **Schlüssel hinzufügen**.
7. In der PKCS #12 /PFX-Datei mit Passwort hinzufügen Abschnitt, geben Sie im Feld Beschreibung einen beschreibenden Namen zur Identifizierung dieses Zertifikats und Schlüssels ein.
8. Löschen Sie das **Aktiviert** Checkbox, wenn Sie dieses TLS-Zertifikat deaktivieren möchten.
9. Für PKCS #12 /PFX-Datei, klicken Sie **Stöbern**.
10. Navigieren Sie zu der Datei, wählen Sie sie aus und klicken Sie dann auf **Offen**.
11. In der Passwort Feld, geben Sie das Passwort für die PKCS #12 /PFX-Datei ein.
12. Klicken Sie **Hinzufügen**.
13. Klicken Sie **OK**.

Nächste Schritte
Fügen Sie die verschlüsselten Protokolle hinzu Sie möchten mit diesem Zertifikat entschlüsseln.

Verschlüsselte Protokolle hinzufügen
Sie müssen jedes Protokoll, das Sie entschlüsseln möchten, für jedes hochgeladene Zertifikat hinzufügen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Zuordnung von Protokoll zu Port nach Schlüssel Abschnitt, klicken Sie **Protokoll hinzufügen**.
5. Aus dem **Protokoll** Wählen Sie in der Dropdownliste das Protokoll aus, das Sie entschlüsseln möchten.
6. Aus dem **Schlüssel** Wählen Sie in der Dropdownliste einen hochgeladenen privaten Schlüssel aus.
7. In der Hafen Feld, geben Sie den Quellport für das Protokoll ein.

   Der Standardwert ist 443, was den HTTP-Verkehr angibt. Geben Sie 0 an, um den gesamten Protokollverkehr zu entschlüsseln.
8. Klicken Sie **Hinzufügen**.

Einen globalen Port zur Protokollzuordnung hinzufügen
Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, löschen Sie das Private Schlüssel erforderlich Ankreuzfeld.
5. In der Zuordnung von globalem Protokoll zu Port Abschnitt, klicken **Globales Protokoll hinzufügen**.
6. Aus dem **Protokoll** Wählen Sie in der Dropdownliste das Protokoll für den Verkehr aus, den Sie entschlüsseln möchten.
7. In der Hafen Feld, geben Sie die Nummer des Ports ein.

   Typ `0` um alle Ports hinzuzufügen.
8. Klicken Sie **Hinzufügen**.

Installieren Sie den ExtraHOP Session Key Forwarder auf einem Windows-Server

Perfect Forward Secrecy (PFS) ist eine Eigenschaft sicherer Kommunikationsprotokolle, die den kurzfristigen, vollständig privaten Austausch von Sitzungsschlüsseln zwischen Clients und Servern

ermöglichen. ExtraHop bietet eine Software zur Weiterleitung von Sitzungsschlüsseln an, die Sitzungsschlüssel zur TLS-Entschlüsselung an das ExtraHop-System senden kann. Kommunikation zwischen dem Key Spediteur und dem Sensor ist mit TLS 1.2 oder TLS 1.3 verschlüsselt, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Hinweis: Weitere Informationen darüber, wie sich der Traffic-Feed oder Änderungen an der Konfiguration auf Sensoren auswirken könnten, finden Sie in den Metriken für Desynchronisierung und Erfassung der Drop-Rate in der Systemstatus-Dashboard.

Sie müssen das ExtraHop-System für die Weiterleitung von Sitzungsschlüsseln konfigurieren und dann die Forwarder-Software auf dem Windows und Linux Server mit dem TLS-Verkehr, den Sie entschlüsseln möchten.

Bevor du anfängst

- Lesen Sie über TLS-Entschlüsselung und überprüfen Sie die Liste von unterstützte Cipher Suites.
- Stellen Sie sicher, dass das ExtraHop-System für TLS Decryption und TLS Shared Secrets lizenziert ist.
- Stellen Sie sicher, dass Ihre Serverumgebung von der ExtraHop Session Key Forwarder-Software unterstützt wird:
  - Microsoft Secure Channel (Schannel) -Sicherheitspaket
  - Java TLS (Java-Versionen 8 bis 17). Führen Sie kein Upgrade auf diese Version des Session Key Forwarders durch, wenn Sie derzeit Java 6- oder Java 7-Umgebungen überwachen. Version 7.9 des Session Key Forwarders unterstützt Java 6 und Java 7 und ist mit der neuesten ExtraHop-Firmware kompatibel.
  - Dynamisch verknüpfte OpenSSL-Bibliotheken (1.0.x und 1.1.x). OpenSSL wird nur auf Linux-Systemen mit den Kernelversionen 4.4 und höher sowie RHEL 7.6 und höher unterstützt.
- Stellen Sie sicher, dass der Server, auf dem Sie den Session Key Forwarder installieren, dem TLS-Zertifikat des ExtraHop vertraut Sensor.
- Stellen Sie sicher, dass Ihre Firewallregeln zulassen, dass vom überwachten Server Verbindungen zum TCP-Port 4873 auf dem Sensor initiiert werden.

  Wichtig: Das ExtraHop-System kann den TLS-verschlüsselten TDS-Verkehr nicht durch Weiterleitung von Sitzungsschlüsseln entschlüsseln. Stattdessen können Sie ein RSA hochladen privater Schlüssel.

- Installieren Sie den Session Key Forwarder auf einem oder mehreren Windows 2016- oder Windows 2019-Servern, auf denen TLS-basierte Dienste mit dem nativen Windows TLS-Framework ausgeführt werden. OpenSSL unter Windows wird derzeit nicht unterstützt.

  Wichtig: Nach der Installation der Sitzungsschlüsselweiterleitungssoftware funktionieren Anwendungen, die TLS-fähige Funktionen enthalten, wie EDR-Agenten und Windows Store-Anwendungen, möglicherweise nicht richtig.

  Überprüfen Sie die Kompatibilität des Session Key Forwarders in Ihrer Windows-Testumgebung, bevor Sie ihn in Ihrer Produktionsumgebung bereitstellen.

Entschlüsselung des Windows-Anwendungsverkehrs

Der folgende Microsoft-Anwendungsdatenverkehr kann mit der Sitzungsschlüsselweiterleitung entschlüsselt werden.

- Microsoft IIS
- Microsoft PowerShell
- Microsoft SQL Server

Installieren Sie die Software mit dem Installationsassistenten

1. Loggen Sie sich auf dem Windows-Server ein.
2. Herunterladen die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Doppelklicken Sie auf `ExtraHopSessionKeyForwarder.exe` ablegen und klicken **Weiter**.

4. Wenn das System Sie auffordert, das Installationsprogramm für die Ausführung mit Administratorrechten zu autorisieren, klicken Sie auf **OK**.
5. Wählen Sie das Kästchen aus, um die Bedingungen der Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Weiter**.
6. Geben Sie den Hostnamen oder die IP-Adresse des Sensor wohin Sie Sitzungsschlüssel weiterleiten möchten.

   Hinweis Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie kommagetrennte Hostnamen eingeben. Zum Beispiel:

   ```
   packet-sensor.example.com,ids-sensor.example.com
   ```

7. Optional: Wählen Sie den **Erweiterte Optionen** Checkbox. Akzeptieren Sie den standardmäßigen TCP-Listenportwert 598 (empfohlen), oder geben Sie einen benutzerdefinierten Portwert ein.
8. Klicken **Installieren**.
9. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertig stellen**.

Installationsoption über die Befehlszeile
Die folgenden Schritte zeigen Ihnen, wie Sie die Sitzungsschlüsselweiterleitung über eine Windows-Eingabeaufforderung oder Windows PowerShell installieren.

1. Loggen Sie sich auf dem Windows-Server ein.
2. Herunterladen die neueste Version der Sitzungsschlüsselweiterleitungssoftware.
3. Führen Sie den folgenden Befehl aus:

   ```
   ExtraHopSessionKeyForwarderSetup.exe -q EDA_HOSTNAME="<hostname or IP
    address of sensor>"
   ```

   Hinweis Das `-q` Die Option installiert den Forwarder im nicht interaktiven Modus, der nicht zur Bestätigung auffordert. Sie können das weglassen `-q` Option, um den Forwarder im interaktiven Modus zu installieren.

   Hinweis Sie können mehrere Sensoren in einer kommagetrennten Liste angeben. Der folgende Befehl spezifiziert beispielsweise zwei Sensoren:

   ```
   ExtraHopSessionKeyForwarderSetup.exe EDA_HOSTNAME="packet-
   sensor.example.com,ids-sensor.example.com"
   ```

   Weitere Hinweise zu den Installationsoptionen finden Sie unter Installationsparameter.

Aktivieren Sie den TLS-Sitzungsschlüsselempfängerdienst
Sie müssen den Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktivieren, bevor das System Sitzungsschlüssel vom Sitzungsschlüssel-Forwarder empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Wählen Sie die **Empfänger für SSL-Sitzungsschlüssel** Ankreuzfeld.
4. Klicken Sie **Speichern**.

Einen globalen Port zur Protokollzuordnung hinzufügen
Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.

3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, löschen Sie das Private Schlüssel erforderlich Ankreuzfeld.
5. In der Zuordnung von globalem Protokoll zu Port Abschnitt, klicken **Globales Protokoll hinzufügen**.
6. Aus dem **Protokoll** Wählen Sie in der Dropdownliste das Protokoll für den Verkehr aus, den Sie entschlüsseln möchten.
7. In der Hafen Feld, geben Sie die Nummer des Ports ein.

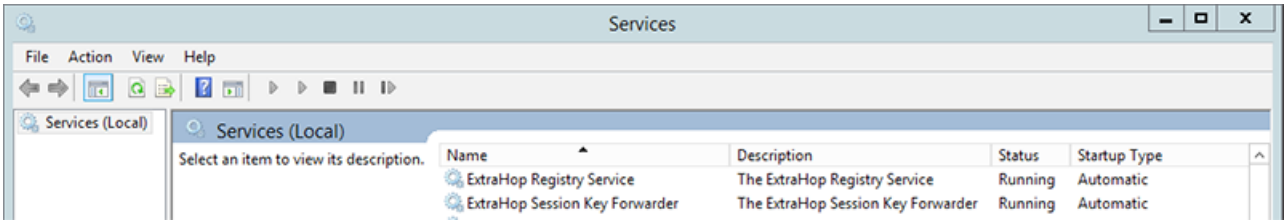
   Typ `0` um alle Ports hinzuzufügen.
8. Klicken Sie **Hinzufügen**.

Schlüsselweiterleitungen verbundener Sitzungen anzeigen
Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den TLS-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Geteilte SSL-Geheimnisse**.

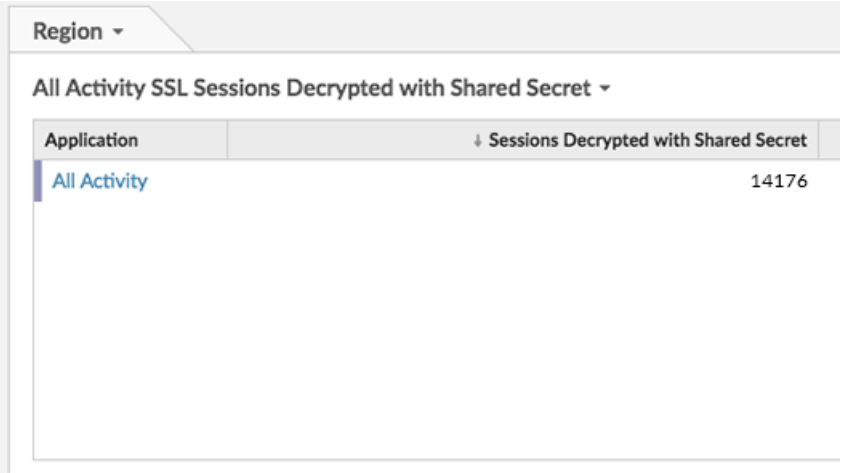
Weiterleitung des Sitzungsschlüssels validieren
Gehen Sie wie folgt vor, um sicherzustellen, dass die Installation erfolgreich war und der Session Key Forwarder die Schlüssel an das ExtraHop-System weiterleitet.

1. Melden Sie sich beim Windows-Server an.
2. Öffnen Sie das MMC-Snap-In Services. Stellen Sie sicher, dass beide Dienste, „ExtraHop Session Key Forwarder“ und „ExtraHop Registry Service“, den Status „Wird ausgeführt“ anzeigen.



3. Wenn einer der Dienste nicht ausgeführt wird, beheben Sie das Problem, indem Sie die folgenden Schritte ausführen.
   a) Öffnen Sie das MMC-Snap-In der Ereignisanzeige und navigieren Sie zu Windows-Protokolle > Anwendung.
   b) Suchen Sie die neuesten Einträge für die ExtraHopAgent-Quelle. Häufige Fehlerursachen und die zugehörigen Fehlermeldungen sind in der Beheben Sie häufig auftretende Fehlermeldungen Abschnitt unten.
4. Wenn das Snap-In „Dienste“ und die Ereignisanzeige keine Probleme anzeigen, wenden Sie eine Arbeitslast auf die überwachten Dienste an und überprüfen Sie im ExtraHop-System, ob die geheime Entschlüsselung funktioniert.

Wenn das ExtraHop-System Sitzungsschlüssel empfängt und sie auf entschlüsselte Sitzungen anwendet, wird der Shared Secret-Metrikzähler (unter Anwendungen > Alle Aktivitäten > SSL-Sitzungen entschlüsselt) erhöht. Erstellen Sie ein Dashboard-Diagramm mit dieser Metrik, um zu sehen, ob der Sensor erfolgreich Sitzungsschlüssel von den überwachten Servern empfängt.



Überprüfen Sie die Konfiguration über die Kommandozeile

In Fällen, in denen Sie möglicherweise Probleme mit der Konfiguration haben, enthält die Binärdatei für die Sitzungsschlüsselweiterleitung einen Testmodus, auf den Sie über die Kommandozeile zugreifen können, um Ihre Konfiguration zu testen.

1. Loggen Sie sich auf Ihrem Windows-Server ein.
2. Öffnen Sie die Windows PowerShell-Anwendung.
3. Führen Sie einen Verifizierungstest durch, indem Sie den folgenden Befehl ausführen:

   ```
   & 'C:\Program Files\ExtraHop\extrahop-agent.exe' -t -server <eda
    hostname>
   ```

   Wo `<eda hostname>` ist der vollqualifizierte Domainname des Sensor, an den Sie Secrets weiterleiten.

   Die folgende Ausgabe sollte erscheinen:

   ```
   <timestamp> Performing connectivity test
   <timestamp> No connectivity issues detected
   ```

   Wenn ein Konfigurationsproblem auftritt, werden in der Ausgabe Tipps zur Fehlerbehebung angezeigt, die Ihnen bei der Behebung des Problems helfen. Folgen Sie den Vorschlägen, um das Problem zu lösen, und führen Sie den Test dann erneut aus.
4. Sie können optional die Überschreibung des Zertifikatspfads und des Servernamens testen, indem Sie dem obigen Befehl die folgenden Optionen hinzufügen.

   - Geben Sie diese Option an, um das Zertifikat zu testen, ohne es dem Zertifikatsspeicher hinzuzufügen.

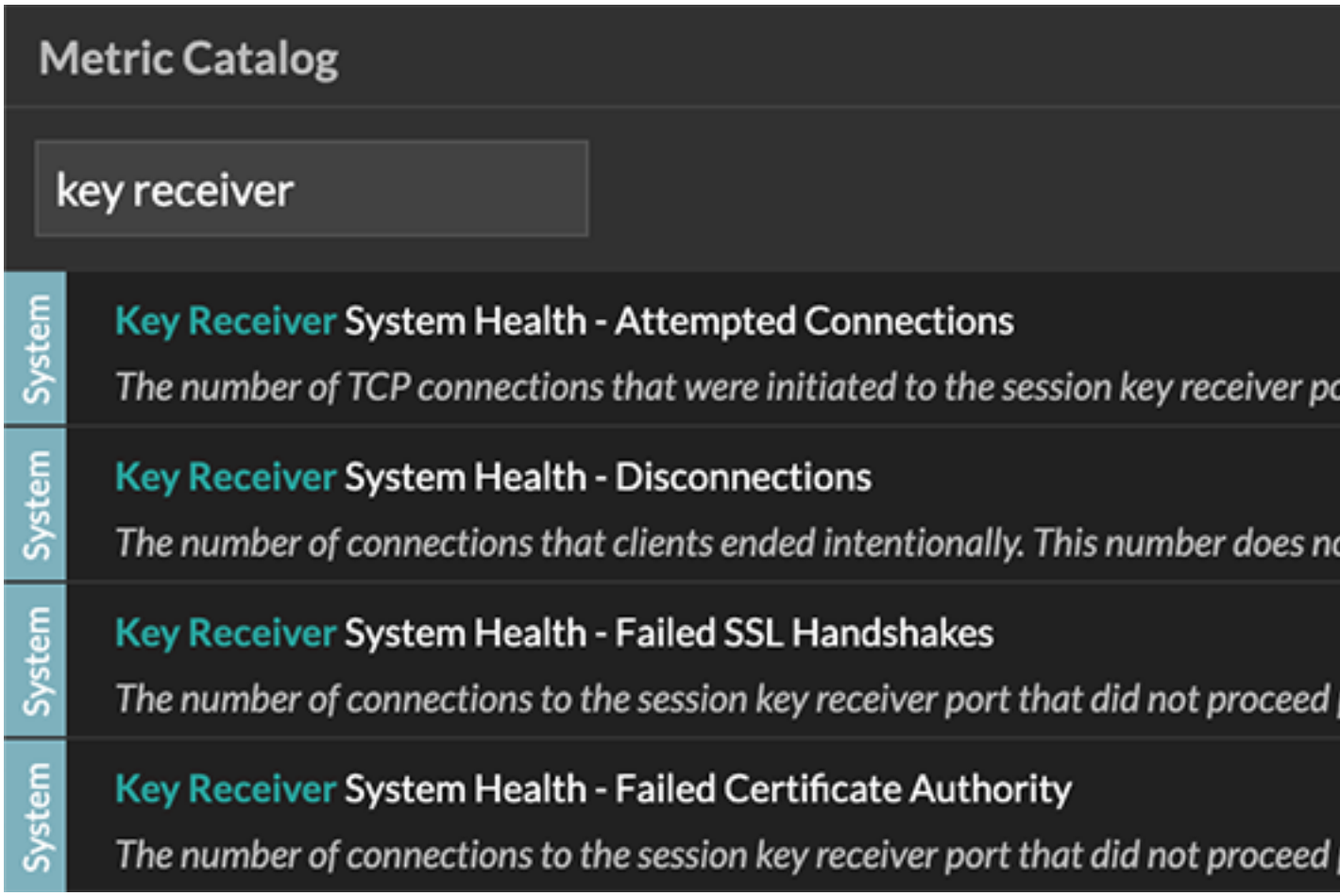
     ```
     -cert <file path to certificate>
     ```

   - Geben Sie diese Option an, um die Verbindung zu testen, falls eine Diskrepanz zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem allgemeinen Namen (CN), der im TLS-Zertifikat des ExtraHop-Systems enthalten ist, besteht.

     ```
     -server-name-override <common name>
     ```

Wichtige Kennzahlen zum Zustand des Empfängersystems
Das ExtraHop-System bietet wichtige Empfängermetriken, die Sie zu einem Dashboard-Diagramm hinzufügen können, um den Zustand und die Funktionalität der wichtigsten Empfänger zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen ⚙ und dann klicken **Metrischer Katalog**. Typ `Schlüsselempfänger` im Filterfeld, um alle verfügbaren wichtigen Empfängermetriken anzuzeigen.



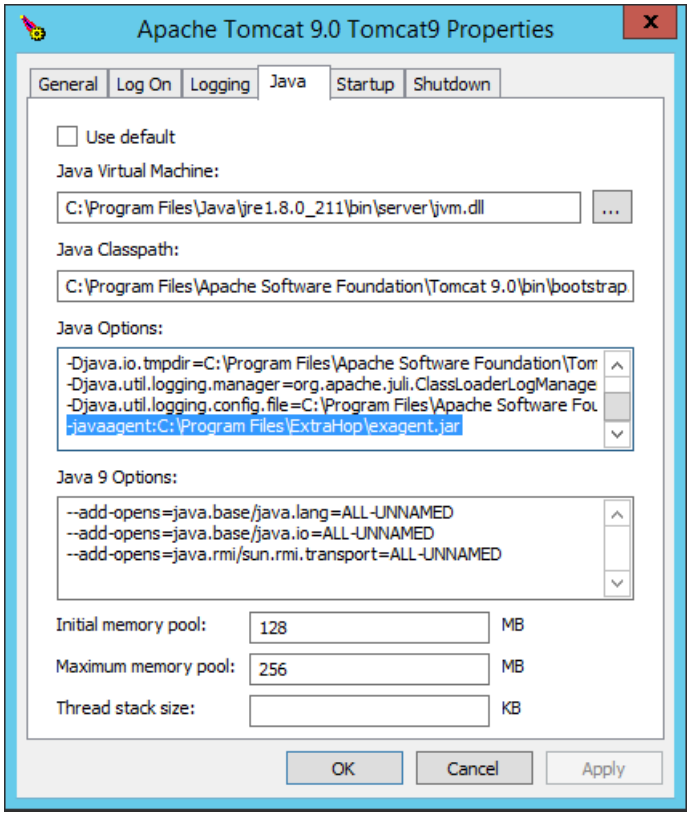
Hinweis: Informationen zum Erstellen eines neuen Dashboard-Diagramms finden Sie unter Ein Diagramm mit dem Metric Explorer bearbeiten.

Integrieren Sie den Forwarder in die Java-basierte TLS-Anwendung

Der ExtraHop Session Key Forwarder integriert sich in Java-Anwendungen über den `-javaagent` Option. Lesen Sie die spezifischen Anweisungen Ihrer Anwendung zum Ändern der Java-Laufzeitumgebung, um Folgendes einzubeziehen `-javaagent` Option.

Beispielsweise unterstützt Apache Tomcat die Anpassung von Java-Optionen in den Eigenschaften des Tomcat Service Managers. Im folgenden Beispiel fügen Sie `-javaagent` Die Option für den Abschnitt Java-Optionen bewirkt, dass die Java-Laufzeitumgebung die Geheimnisse der TLS-Sitzung mit dem Key-Forwarder-Prozess teilt, der die Geheimnisse dann an das ExtraHop-System weiterleitet, damit die Geheimnisse entschlüsselt werden können.

```
-javaagent:C:\Program Files\ExtraHop\exagent.jar
```



Hinweis: Wenn auf Ihrem Server Java 17 oder höher ausgeführt wird, müssen Sie dem sun.security.ssl-Modul auch den Zugriff auf alle unbenannten Module mit dem `--add-opens` Option, wie im folgenden Beispiel gezeigt:

```
--add-opens java.base/sun.security.ssl=ALL-UNNAMED
```

Anlage

Beheben Sie häufig auftretende Fehlermeldungen

Fehlermeldungen werden in Protokolldateien an den folgenden Speicherorten gespeichert, wobei TMP der Wert Ihrer TMP-Umgebungsvariablen ist:

- `TMP\ExtraHopSessionKeyForwarderSetup.log`
- `TMP\ExtraHopSessionKeyForwarderMsi.log`

Die folgende Tabelle enthält häufig auftretende Fehlermeldungen, die Sie beheben können. Wenn Sie einen anderen Fehler sehen oder die vorgeschlagene Lösung Ihr Problem nicht löst, wenden Sie sich an den ExtraHop Support.

Nachricht	Ursache	Lösung
`connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected`	Der überwachte Server kann keinen Datenverkehr an den weiterleiten Sensor.	Stellen Sie sicher, dass die Firewallregeln das Initiieren von Verbindungen durch den überwachten Server zum TCP-Port 4873 auf dem Sensor.

Nachricht	Ursache	Lösung
`host has failed to respond`		
`connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it`	Der überwachte Server kann den Verkehr an den weiterleiten Sensor, aber der Empfangsvorgang hört nicht zu.	Stellen Sie sicher, dass Sensor ist sowohl für die Funktionen TLS Decryption als auch TLS Shared Secrets lizenziert.
`connect: x509: certificate signed by unknown authority`	Der überwachte Server ist nicht in der Lage, die zu verketten Sensor Zertifikat für eine vertrauenswürdige Zertifizierungsstelle (CA).	Stellen Sie sicher, dass der Windows-Zertifikatspeicher für das Computerkonto über vertrauenswürdige Stammzertifizierungsstellen verfügt, die eine Vertrauenskette für das Sensor.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	Eine IP-Adresse wurde als angegeben `EDA_HOSTNAME` Parameter bei der Installation des Forwarders, aber das vom Sensor vorgelegte TLS-Zertifikat enthält keine IP-Adresse als Subject Alternate Name (SAN).	Wählen Sie aus den folgenden drei Lösungen. • Wenn es einen Hostnamen gibt, mit dem der Server eine Verbindung herstellen kann Sensor mit, und dieser Hostname entspricht dem Betreffnamen in der Sensor Zertifikat, deinstalliere und installiere den Forwarder neu, wobei du diesen Hostnamen als Wert von angibst `EDA_HOSTNAME`. • Wenn der Server eine Verbindung zum herstellen muss Sensor nach IP-Adresse, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, wobei Sie den Betreffnamen aus dem Sensorzertifikat als Wert von angeben `SERVERNAMEOVERRIDE`. • Neuauflage der Sensor Zertifikat, das einen IP Subject Alternative Name (SAN) für die angegebene IP-Adresse enthält.

Deinstalliere die Software
Wenn Sie nicht mehr möchten, dass die ExtraHop-Sitzungsschlüsselweiterleitungssoftware installiert wird, oder wenn sich einer der ursprünglichen Installationsparameter geändert hat (Sensor-Hostname oder Zertifikat) und Sie die Software mit neuen Parametern neu installieren müssen, gehen Sie wie folgt vor:

Wichtig: Sie müssen den Server neu starten, damit die Konfigurationsänderungen wirksam werden.

1. Loggen Sie sich auf dem Windows-Server ein.
2. Optional: Wenn Sie den Sitzungsschlüssel-Forwarder in Apache Tomcat integriert haben, entfernen Sie den `-javaagent:C:\Program Files\ExtraHop\exagent.jar` Eintrag von Tomcat, um zu verhindern, dass der Webservice gestoppt wird.
3. Wählen Sie eine der folgenden Optionen, um die Software zu entfernen:
   - Öffnen Sie das Control Panel und klicken Sie auf **Deinstalliere ein Programm**. Wählen **ExtraHop-Sitzungsschlüsselweiterleitung** aus der Liste und klicken Sie dann auf **Deinstallation**.
   - Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie die folgenden Befehle aus, um die Software und die zugehörigen Registrierungseinträge zu entfernen:
     1. ```
        $app=Get-WMIObject -class win32_product | where-object {$_.name -eq
         "ExtraHop Session Key Forwarder"}
        ```
     2. ```
        $app.Uninstall()
        ```
4. Klicken **Ja** zur Bestätigung.
5. Nachdem die Software entfernt wurde, klicken Sie auf **Ja** um das System neu zu starten

Installationsparameter

Sie können die folgenden MSI-Parameter angeben:

MSI-Installationsparameter	`EDA_HOSTNAME`
Eintrag in die Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\EDAHost`
Beschreibung	Das Sensor Hostname oder IP-Adresse, an die TLS-Sitzungsschlüssel gesendet werden. Dieser Parameter ist erforderlich.

MSI-Installationsparameter	`EDA_CERTIFICATEPATH`
Eintrag in die Registrierung	N/A
Beschreibung	Der überwachte Server muss dem Aussteller des vertrauen Sensor TLS-Zertifikat über den Zertifikatsspeicher des Servers. In einigen Umgebungen ist der Sensor arbeitet mit dem selbstsignierten Zertifikat , das die ExtraHop-Firmware bei der Installation generiert. In diesem Fall muss das Zertifikat zum Zertifikatsspeicher hinzugefügt werden. Das `EDA_CERTIFICATEPATH` Mit diesem Parameter kann ein dateibasiertes PEM-kodiertes Zertifikat bei der Installation in den Windows-Zertifikatsspeicher importiert werden. Wenn der Parameter bei der Installation nicht angegeben wird und ein selbstsigniertes oder anderes CA-Zertifikat manuell im Zertifikatsspeicher abgelegt werden muss, muss der Administrator das Zertifikat auf dem überwachten System unter Zertifikate (Computerkonto) > Vertrauenswürdige Stammzertifizierungsstellen importieren.

	Dieser Parameter ist optional, wenn der überwachte Server zuvor so konfiguriert wurde, dass er dem TLS-Zertifikat des Sensor über den Windows-Zertifikatsspeicher.

MSI-Installationsparameter	`SERVERNAMEOVERRIDE`
Eintrag in die Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\ServerNameOverride`
Beschreibung	Wenn es eine Diskrepanz zwischen dem Sensor Hostname, den der Forwarder kennt (EDA_HOSTNAME) und der allgemeine Name (CN), der im TLS-Zertifikat des Sensor, dann muss der Forwarder mit dem richtigen CN konfiguriert werden. Dieser Parameter ist optional. Wir empfehlen, dass Sie das selbstsignierte TLS-Zertifikat auf der Grundlage des Hostnamens aus dem TLS-Zertifikat Abschnitt der Administrationseinstellungen, anstatt diesen Parameter anzugeben.

MSI-Installationsparameter	`TCPLISTENPORT`
Eintrag in die Registrierung	`HKEY_LOCAL_MACHINE\SOFTWARE\ExtraHop\TCPListenPort`
Beschreibung	Der Key Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den in der `TCPListenPort` Eintrag. Wir empfehlen, für diesen Port die Standardeinstellung 598 beizubehalten. Dieser Parameter ist optional.

Unterstützte TLS-Verschlüsselungssammlungen
Das ExtraHop-System kann TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher-Suites verschlüsselt wurde. Alle unterstützten Cipher-Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites für RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln — mit oder ohne Sitzungsschlüsselweiterleitung.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste von Cipher-Suites, die das ExtraHop-System kann entschlüsseln zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP**: das ExtraHop-System kann diese Verschlüsselungssammlungen mit Sitzungsschlüsselweiterleitung entschlüsseln und Zuordnung von globalem Protokoll zu Port
- **PFS + Zertifikat**: Das ExtraHop-System kann diese Cipher-Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und Zertifikat und privater Schlüssel
- **RSA + Zertifikat**: das ExtraHop-System kann diese Cipher-Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, solange Sie die Datei hochgeladen haben Zertifikat und privater Schlüssel

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 0A	TLS_RSA_MIT_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_MIT_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0x35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0x6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat
0x9C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9D	TLS_RSA_MIT_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0x9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_MIT_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_MIT_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0xCCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat

Exportieren Sie die MSI-Datei aus der ausführbare Datei
Sie können die MSI-Datei aus der ausführbare Datei exportieren, um einen benutzerdefinierten Installationsablauf zu unterstützen.

Öffnen Sie eine PowerShell-Eingabeaufforderung und führen Sie den folgenden Befehl aus:

```
ExtraHopSessionKeyForwarderSetup.exe -e
```

Hinweis Sie können anhängen `<directory>` zum `-e` Parameter zum Speichern des `.msi` Datei in ein anderes Verzeichnis als das aktuelle Arbeitsverzeichnis. Mit dem folgenden Befehl wird die Datei beispielsweise im `install_dir` Verzeichnis:

```
ExtraHopSessionKeyForwarderSetup.exe -e install_dir
```

Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server

Perfect Forward Secrecy (PFS) ist eine Eigenschaft sicherer Kommunikationsprotokolle, die den kurzfristigen, vollständig privaten Austausch von Sitzungsschlüsseln zwischen Clients und Servern ermöglichen. ExtraHop bietet eine Software zur Weiterleitung von Sitzungsschlüsseln an, die Sitzungsschlüssel zur TLS-Entschlüsselung an das ExtraHop-System senden kann. Kommunikation zwischen dem Key Spediteur und dem Sensor ist mit TLS 1.2 oder TLS 1.3 verschlüsselt, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Hinweis Weitere Informationen darüber, wie sich der Traffic-Feed oder Änderungen an der Konfiguration auf Sensoren auswirken könnten, finden Sie in den Metriken für Desynchronisierung und Erfassung der Drop-Rate in der Systemstatus-Dashboard.

Sie müssen das ExtraHop-System für die Weiterleitung von Sitzungsschlüsseln konfigurieren und dann die Forwarder-Software auf dem Windows und Linux Server mit dem TLS-Verkehr, den Sie entschlüsseln möchten.

Bevor du anfängst

- Lesen Sie über TLS-Entschlüsselung und überprüfen Sie die Liste von unterstützte Cipher Suites.
- Stellen Sie sicher, dass das ExtraHop-System für TLS Decryption und TLS Shared Secrets lizenziert ist.
- Stellen Sie sicher, dass Ihre Serverumgebung von der ExtraHop Session Key Forwarder-Software unterstützt wird:
  - Microsoft Secure Channel (Schannel) -Sicherheitspaket
  - Java TLS (Java-Versionen 8 bis 17). Führen Sie kein Upgrade auf diese Version des Session Key Forwarders durch, wenn Sie derzeit Java 6- oder Java 7-Umgebungen überwachen. Version 7.9 des Session Key Forwarders unterstützt Java 6 und Java 7 und ist mit der neuesten ExtraHop-Firmware kompatibel.
  - Dynamisch verknüpfte OpenSSL-Bibliotheken (1.0.x und 1.1.x). OpenSSL wird nur auf Linux-Systemen mit den Kernelversionen 4.4 und höher sowie RHEL 7.6 und höher unterstützt.

- Stellen Sie sicher, dass der Server, auf dem Sie den Session Key Forwarder installieren, dem TLS-Zertifikat des ExtraHop vertraut Sensor.
- Stellen Sie sicher, dass Ihre Firewallregeln zulassen, dass vom überwachten Server Verbindungen zum TCP-Port 4873 auf dem Sensor initiiert werden.

  Wichtig: Das ExtraHop-System kann den TLS-verschlüsselten TDS-Verkehr nicht durch Weiterleitung von Sitzungsschlüsseln entschlüsseln. Stattdessen können Sie ein RSA hochladen privater Schlüssel.

- Installieren Sie den Session Key Forwarder auf RHEL-, CentOS-, Fedora- oder Debian-Ubuntu-Linux-Distributionen. Die Sitzungsschlüsselweiterleitung funktioniert auf anderen Distributionen möglicherweise nicht richtig.
- Der Session Key Forwarder wurde nicht ausführlich mit SELinux getestet und ist möglicherweise nicht kompatibel, wenn er auf einigen Linux-Distributionen aktiviert ist.

Aktivieren Sie den TLS-Sitzungsschlüsselempfängerdienst
Sie müssen den Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktivieren, bevor das System Sitzungsschlüssel vom Sitzungsschlüssel-Forwarder empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Wählen Sie die **Empfänger für SSL-Sitzungsschlüssel** Ankreuzfeld.
4. Klicken Sie **Speichern**.

Einen globalen Port zur Protokollzuordnung hinzufügen
Fügen Sie jedes Protokoll für den Datenverkehr hinzu, den Sie mit Ihren Sitzungsschlüsselweiterleitungen entschlüsseln möchten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **SSL-Entschlüsselung**.
4. In der Entschlüsselung des privaten Schlüssels Abschnitt, löschen Sie das Private Schlüssel erforderlich Ankreuzfeld.
5. In der Zuordnung von globalem Protokoll zu Port Abschnitt, klicken **Globales Protokoll hinzufügen**.
6. Aus dem **Protokoll** Wählen Sie in der Dropdownliste das Protokoll für den Verkehr aus, den Sie entschlüsseln möchten.
7. In der Hafen Feld, geben Sie die Nummer des Ports ein.

   Typ `0` um alle Ports hinzuzufügen.
8. Klicken Sie **Hinzufügen**.

Installieren Sie die Software
RPM-basierte Distributionen

Hinweis: Sie können den Forwarder ohne Benutzerinteraktion installieren, indem Sie Folgendes angeben Umgebungsvariablen im Installationsbefehl.

1. Melden Sie sich bei Ihrem RPM-basierten Linux-Server an.
2. Herunterladen die neueste Version der ExtraHop Session Key Forwarder-Software.
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus:

```
sudo rpm --install <path to installer file>
```

4. Öffnen Sie das Initialisierungsskript in einem Texteditor (z. B. vi oder vim).

```
sudo vi /opt/extrahop/etc/extrahop-key-forwarder.conf
```

5. Entfernen Sie das Hash-Symbol (#) vor dem Feld EDA_HOSTNAME und geben Sie den vollqualifizierten Domänenname Ihres Sensor ein, ähnlich dem folgenden Beispiel.

```
EDA_HOSTNAME=discover.example.com
```

Hinweis: Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie kommagetrennte Hostnamen eingeben. Zum Beispiel:

```
EDA_HOSTNAME=packet-sensor.example.com,ids-sensor.example.com
```

6. Optional: Der Key Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den in der `LOCAL_LISTENER_PORT` Feld. Wir empfehlen, für diesen Port die Standardeinstellung 598 beizubehalten. Wenn Sie die Portnummer ändern, müssen Sie die `-javaagent` Argument, um den neuen Port zu berücksichtigen.
7. Optional: Wenn Sie es vorziehen, dass Syslog in eine andere Einrichtung schreibt als `local3` Für Key-Forwarder-Lognachrichten können Sie das bearbeiten `SYSLOG` Feld.
Der Inhalt der `extrahop-key-forwarder.conf` Die Datei sollte dem folgenden Beispiel ähneln:

```
#EDA_HOSTED_PLATFORM=aws
EDA_HOSTNAME=sensor.example.com
LOCAL_LISTENER_PORT=598
SYSLOG=local3
ADDITIONAL_ARGS=''
```

8. Speichern Sie die Datei und beenden Sie den Texteditor.
9. Wenn Ihr Server Container mit der containerd-Laufzeit verwaltet, müssen Sie hinzufügen die folgenden Parameter für `/opt/extrahop/etc/extrahop-key-forwarder.conf` Aufbau datei:

   - `-containerd-enable`
   - `-containerd-socket`
   - `-containerd-state`
   - `-containerd-state-rootfs-subdir`

   Weitere Informationen zu diesen Parametern und anderen optionalen Parametern finden Sie sehen Optionen für die Weiterleitung von Sitzungsschlüsseln.
10. Starte den `extrahop-key-forwarder` Bedienung:

```
sudo service extrahop-key-forwarder start
```

Debian-Ubuntu-Distributionen

Hinweis: Sie können den Forwarder ohne Benutzerinteraktion installieren, indem Sie Folgendes angeben Umgebungsvariablen im Installationsbefehl.

1. Loggen Sie sich auf Ihrem Debian- oder Ubuntu-Linux-Server ein.
2. Herunterladen die neueste Version der ExtraHop Session Key Forwarder-Software.
3. Öffnen Sie eine Terminal-Anwendung und führen Sie den folgenden Befehl aus.

```
sudo dpkg --install <path to installer file>
```

4. Wählen **richten** und drücken Sie dann die EINGABETASTE.
5. Geben Sie den vollqualifizierten Domänenname oder die IP-Adresse des ExtraHop-Systems ein, an das die Sitzungsschlüssel weitergeleitet werden, und drücken Sie dann die EINGABETASTE.

Hinweis: Sie können Sitzungsschlüssel an mehr als einen Sensor weiterleiten, indem Sie kommagetrennte Hostnamen eingeben. Zum Beispiel:

```
packet-sensor.example.com,ids-sensor.example.com
```

6. Wenn Ihr Server Container mit der containerd-Laufzeit verwaltet, müssen Sie hinzufügen die folgenden Parameter für `/opt/extrahop/etc/extrahop-key-forwarder.conf` Aufbau datei:

   - `-containerd-enable`
   - `-containerd-socket`
   - `-containerd-state`
   - `-containerd-state-rootfs-subdir`

   Weitere Informationen zu diesen Parametern und anderen optionalen Parametern finden Sie sehen Optionen für die Weiterleitung von Sitzungsschlüsseln.

7. Stellen Sie sicher, dass die `extrahop-key-forwarder` Dienst gestartet:

   ```
   sudo service extrahop-key-forwarder status
   ```

   Die folgende Ausgabe sollte erscheinen:

   ```
   extrahop-key-forwarder.service - LSB: ExtraHop Session Key Forwarder
   Loaded: loaded (/etc/rc.d/init.d/extrahop-key-forwarder; bad; vendor
    preset: disabled)
   Active: active (running) since Tue 2018-04-10 10:55:47 PDT; 5s ago
   ```

   Wenn der Dienst nicht aktiv ist, führen Sie den folgenden Befehl aus:

   ```
   sudo service extrahop-key-forwarder start
   ```

Integrieren Sie den Forwarder in die Java-basierte TLS-Anwendung

Der ExtraHop Session Key Forwarder integriert sich in Java-Anwendungen über den `-javaagent` Option. Lesen Sie die spezifischen Anweisungen Ihrer Anwendung zum Ändern der Java-Laufzeitumgebung, um Folgendes einzubeziehen `-javaagent` Option.

Beispielsweise unterstützen viele Tomcat-Umgebungen die Anpassung von Java-Optionen in der `/etc/default/tomcat7` Datei. Im folgenden Beispiel fügen Sie `-javaagent` Die Option in der Zeile JAVA_OPTS bewirkt, dass die Java-Laufzeitumgebung die Geheimnisse der TLS-Sitzung mit dem Key-Forwarder-Prozess teilt, der die Geheimnisse dann an das ExtraHop-System weiterleitet, damit die Geheimnisse entschlüsselt werden können.

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar
```

Wenn auf Ihrem Server Java 17 oder höher ausgeführt wird, müssen Sie dem Modul sun.security.ssl auch den Zugriff auf alle unbenannten Module mit der Option --add-opens ermöglichen, wie im folgenden Beispiel gezeigt:

```
JAVA_OPTS="... -javaagent:/opt/extrahop/lib/exagent.jar --add-opens
 java.base/sun.security.ssl=ALL-UNNAMED
```

Überprüfen Sie Ihre Installation und beheben Sie Fehler
Wenn Ihr Linux-Server Netzwerkzugriff auf das ExtraHop-System hat und die Server-TLS-Konfiguration dem Zertifikat des ExtraHop-Systems vertraut, das Sie bei der Installation des Sitzungsschlüsselweiterleiters angegeben haben, ist die Konfiguration abgeschlossen.

In Fällen, in denen Sie möglicherweise Probleme mit der Konfiguration haben, enthält die Binärdatei für die Sitzungsschlüsselweiterleitung einen Testmodus, auf den Sie über die Befehlszeile zugreifen können, um Ihre Konfiguration zu testen .

1. Loggen Sie sich auf Ihrem Linux-Server ein.
2. Um Ihre Installation zu überprüfen, führen Sie einen ersten Test durch, indem Sie den folgenden Befehl ausführen:

   ```
   /opt/extrahop/sbin/extrahop-agent -t=true -server <eda hostname>
   ```

   Die folgende Ausgabe sollte erscheinen:

   ```
   <timestamp> Performing connectivity test
   <timestamp> No connectivity issues detected
   ```

   Wenn ein Konfigurationsproblem auftritt, werden in der Ausgabe Tipps zur Fehlerbehebung angezeigt, die Ihnen bei der Behebung des Problems helfen. Folgen Sie den Vorschlägen, um das Problem zu lösen, und führen Sie den Test dann erneut aus.
3. Sie können optional die Überschreibung des Zertifikatspfads und des Servernamens testen, indem Sie dem obigen Befehl die folgenden Optionen hinzufügen.

   - Geben Sie diese Option an, um das Zertifikat zu testen, ohne es dem Zertifikatsspeicher hinzuzufügen.

     ```
     -cert <file path to certificate>
     ```
   - Geben Sie diese Option an, um die Verbindung zu testen, falls eine Diskrepanz zwischen dem Hostnamen des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem allgemeinen Namen (CN), der im TLS-Zertifikat des ExtraHop-Systems enthalten ist, besteht.

     ```
     -server-name-override <common name>
     ```

(Optional) Konfigurieren Sie eine Servernamenüberschreibung
Wenn der Hostname des ExtraHop-Systems, den der Forwarder kennt (SERVER), und dem Common Name (CN), der im TLS-Zertifikat des ExtraHop-Systems angegeben ist, nicht übereinstimmt, muss der Forwarder mit dem richtigen CN konfiguriert werden.

Wir empfehlen, dass Sie das selbstsignierte TLS-Zertifikat auf der Grundlage des Hostnamens aus dem SSL-Zertifikat Abschnitt der Administrationseinstellungen, anstatt diesen Parameter anzugeben.

1. Loggen Sie sich auf Ihrem Linux-Server ein.
2. Öffnen Sie die Konfigurationsdatei in einem Texteditor.

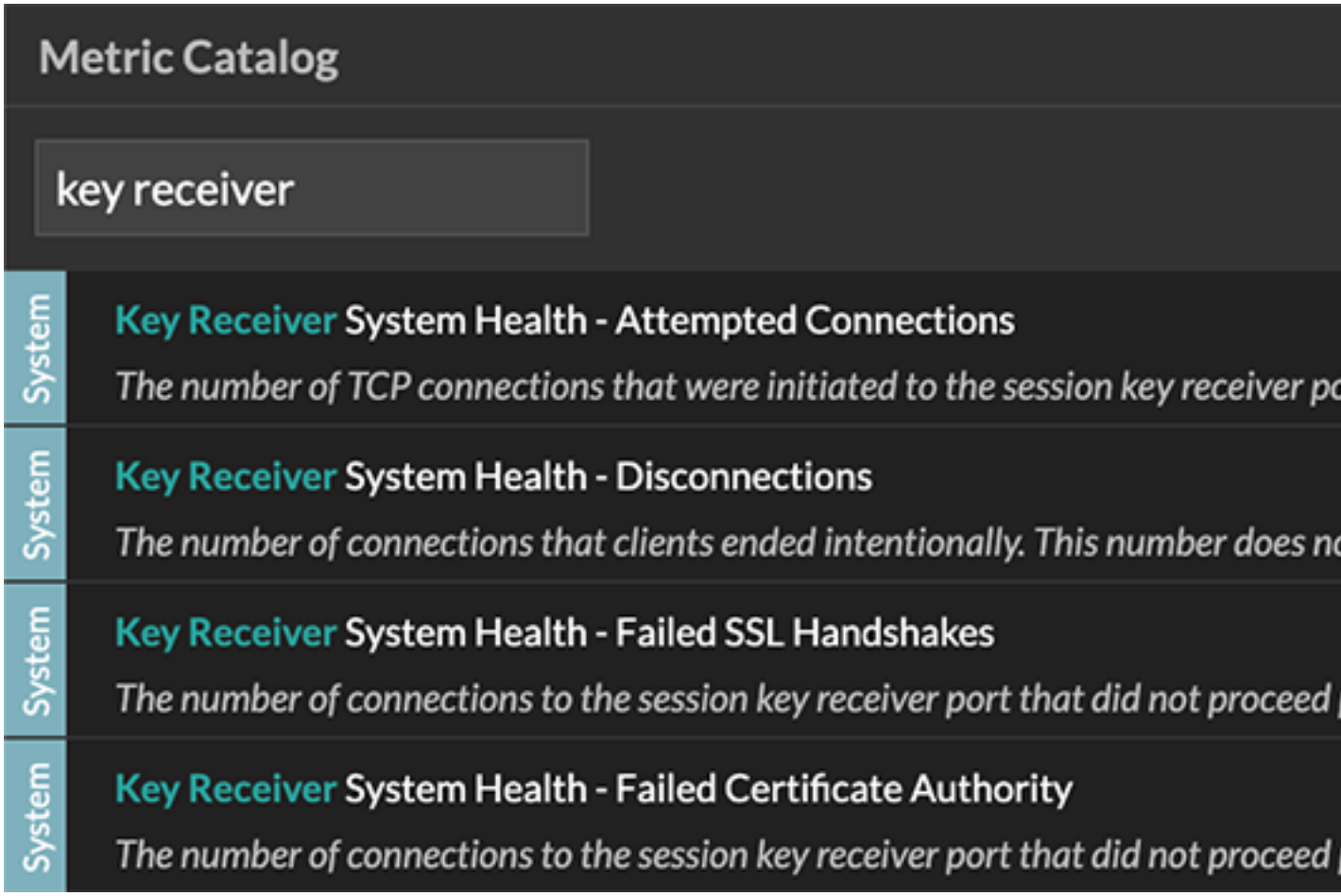
   ```
   vi /opt/extrahop/etc/extrahop-key-forwarder.conf
   ```
3. Füge ein `SERVER_NAME_OVERRIDE` Parameter mit dem Wert des Namens, der im TLS-Zertifikat des ExtraHop-Systems gefunden wurde, ähnlich dem folgenden Beispiel:

   ```
   SERVER_NAME_OVERRIDE=altname.example.com
   ```
4. Speichern Sie die Datei und beenden Sie den Texteditor.
5. Starte den `extrahop-key-forwarder` Service.

   ```
   sudo service extrahop-key-forwarder start
   ```

Wichtige Kennzahlen zum Zustand des Empfängersystems
Das ExtraHop-System bietet wichtige Empfängermetriken, die Sie zu einem Dashboard-Diagramm hinzufügen können, um den Zustand und die Funktionalität der wichtigsten Empfänger zu überwachen.

Um eine Liste der verfügbaren Messwerte anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen ⚙ und dann klicken **Metrischer Katalog**. Typ `Schlüsselempfänger` im Filterfeld, um alle verfügbaren wichtigen Empfängermetriken anzuzeigen.



Hinweis: Informationen zum Erstellen eines neuen Dashboard-Diagramms finden Sie unter Ein Diagramm mit dem Metric Explorer bearbeiten.

Schlüsselweiterleitungen verbundener Sitzungen anzeigen
Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den TLS-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Geteilte SSL-Geheimnisse**.

Deinstalliere die Software
Wenn Sie die ExtraHop Session Key Forwarder-Software nicht mehr installieren möchten, führen Sie die folgenden Schritte aus.

1. Melden Sie sich beim Linux-Server an.
2. Öffnen Sie eine Terminalanwendung und wählen Sie eine der folgenden Optionen, um die Software zu entfernen.
   - Führen Sie für RPM-basierte Server den folgenden Befehl aus:

```
sudo rpm --erase extrahop-key-forwarder
```

- Führen Sie für Debian- und Ubuntu-Server den folgenden Befehl aus:

```
sudo apt-get --purge remove extrahop-key-forwarder
```

  Typ Y wenn Sie aufgefordert werden, das Entfernen der Software zu bestätigen, und drücken Sie dann die EINGABETASTE.

3. klicken **Ja** zur Bestätigung.
4. Nachdem die Software entfernt wurde, klicken Sie auf **Ja** um das System neu zu starten

Allgemeine Fehlermeldungen
Fehler, die vom Sitzungsschlüssel-Forwarder verursacht wurden, werden in der Linux-Systemprotokolldatei protokolliert.

Nachricht	Ursache	Lösung
`connect: dial tcp <IP address>:4873: connectex: A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond`	Der überwachte Server kann keinen Datenverkehr an den weiterleiten Sensor.	Stellen Sie sicher, dass die Firewallregeln das Initiieren von Verbindungen durch den überwachten Server zum TCP-Port 4873 auf dem Sensor.
`connect: dial tcp <IP address>:4873: connectex: No connection could be made because the target machine actively refused it`	Der überwachte Server kann den Verkehr an den weiterleiten Sensor, aber der Empfangsvorgang hört nicht zu.	Stellen Sie sicher, dass Sensor ist sowohl für die Funktionen TLS Decryption als auch TLS Shared Secrets lizenziert.
`connect: x509: certificate signed by unknown authority`	Der überwachte Server ist nicht in der Lage, die zu verketten Sensor Zertifikat für eine vertrauenswürdige Zertifizierungsstelle (CA).	Stellen Sie sicher, dass der Linux-Zertifikatsspeicher für das Computerkonto über vertrauenswürdige Stammzertifizierungsstellen verfügt, die eine Vertrauenskette für den Sensor.
`connect: x509: cannot validate certificate for <IP address> because it doesn't contain any IP SANs`	Eine IP-Adresse wurde als angegeben SERVER Parameter bei der Installation des Forwarders, aber das vom Sensor vorgelegte TLS-Zertifikat enthält keine IP-Adresse als Subject Alternate Name (SAN).	Wählen Sie aus den folgenden drei Lösungen. • Ersetzen Sie die IP-Adresse für SERVER Wert in der `/etc/init.d/extrahop-key-forwarder` Datei mit einem Hostnamen. Der Hostname muss mit dem Betreffnamen im Sensorzertifikat übereinstimmen. • Wenn der Server eine Verbindung zum herstellen muss Sensor nach IP-

Nachricht	Ursache	Lösung
		Adresse, deinstallieren Sie den Forwarder und installieren Sie ihn erneut, wobei Sie den Betreffnamen aus dem Sensorzertifikat als Wert von angeben `server-name-override`.
		• Neuauflage der Sensor Zertifikat, das einen IP Subject Alternative Name (SAN) für die angegebene IP-Adresse enthält.

Unterstützte TLS-Verschlüsselungssammlungen
Das ExtraHop-System kann TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher-Suites verschlüsselt wurde. Alle unterstützten Cipher-Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites für RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln — mit oder ohne Sitzungsschlüsselweiterleitung.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste von Cipher-Suites, die das ExtraHop-System kann entschlüsseln zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP**: das ExtraHop-System kann diese Verschlüsselungssammlungen mit Sitzungsschlüsselweiterleitung entschlüsseln und Zuordnung von globalem Protokoll zu Port
- **PFS + Zertifikat**: Das ExtraHop-System kann diese Cipher-Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und Zertifikat und privater Schlüssel
- **RSA + Zertifikat**: das ExtraHop-System kann diese Cipher-Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, solange Sie die Datei hochgeladen haben Zertifikat und privater Schlüssel

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 0A	TLS_RSA_MIT_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_MIT_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0x35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0x6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat
0x9C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9D	TLS_RSA_MIT_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0x9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_MIT_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_MIT_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat

Optionen für die Weiterleitung von Sitzungsschlüsseln
Sie können den Session Key Forwarder konfigurieren, indem Sie den `/opt/extrahop/etc/extrahop-key-forwarder.conf` Datei.

In der folgenden Tabelle sind alle konfigurierbaren Optionen aufgeführt.

Wichtig: Wenn Sie Optionen hinzufügen `extrahop-key-forwarder.conf` die keine dedizierten Variablen haben, sie müssen sich in der `ADDITIONAL_ARGS` Feld. Zum Beispiel:

```
ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so
-libcrypto=/some/other/path/libcrypto.so"
```

Option	Beschreibung
`-cert <path>`	Gibt den Pfad zum Serverzertifikat an. Geben Sie diese Option nur an, wenn das Serverzertifikat nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert wurde.
`-containerd-enable`	Aktiviert die Aufzählung von Containern, die mit der Containerd-Laufzeit verwaltet werden. Diese Option ist standardmäßig deaktiviert. Sie müssen eingeben `-containerd-enable` um die Containerd-Unterstützung zu aktivieren.
`-containerd-socket <string>`	Der vollständige Pfad der enthaltenen Socket-Datei.
`-containerd-state <string>`	Der vollständige Pfad des Containerd-State-Verzeichnisses.
`-containerd-state-rootfs-subdir <string>`	Der relative Pfad des `rootfs` Unterverzeichnis des Containerd-State-Verzeichnisses.
`-docker-enable`	Aktiviert die Aufzählung von Docker-Containern. Diese Option ist standardmäßig aktiviert. Sie müssen eingeben `-docker-enable=falsch` um die Docker-Unterstützung zu deaktivieren.
`-docker-envoy <path>`	Gibt zusätzliche Envoy-Pfade innerhalb von Docker-Containern an. Sie können diese Option mehrfach angeben.
`-docker-go-binary <value>`	Gibt Glob-Muster an, um Go-Binärdateien in Docker-Containern zu finden. Sie können diese Option mehrfach angeben.
`-docker-libcrypto <path>`	Gibt den Pfad zu libcrypto in Docker-Containern an. Sie können diese Option mehrfach angeben.
`-envoy <path>`	Gibt zusätzliche Envoy-Pfade auf dem Host an. Sie können diese Option mehrfach angeben.
`-go-binary <value>`	Gibt Glob-Muster an, um Go-Binärdateien zu finden. Sie können diese Option mehrfach angeben.
`-hearbeat-interval`	Gibt das Zeitintervall in Sekunden zwischen Heartbeat-Nachrichten an. Das Standardintervall beträgt 30 Sekunden.
`-host-mount-path <path>`	Gibt den Pfad an, in dem das Host-Dateisystem gemountet wird, wenn die Sitzungsschlüsselweiterleitung in einem Container ausgeführt wird.
`-hosted <platform>`	Gibt an, dass der Agent auf der angegebenen gehosteten Plattform ausgeführt wird. Die Plattform ist derzeit beschränkt auf `aws`.

Option	Beschreibung
`-ldconfig-cache <path>`	Gibt den Pfad zum ldconfig-Cache an, ld.so.cache. Der Standardpfad ist `/etc/ld.so.cache`. Sie können diese Option mehrfach angeben.
`-libcrypto <path>`	Gibt den Pfad zur OpenSSL-Bibliothek an, `libcrypto`. Sie können diese Option mehrfach angeben, wenn Sie mehrere Installationen von OpenSSL haben.
`-no-docker-envoy`	Deaktiviert die Envoy-Unterstützung in Docker-Containern.
`-no-envoy`	Deaktiviert die Envoy-Unterstützung auf dem Host.
`-openssl-discover`	Erkennt automatisch `libcrypto` Implementierungen. Der Standardwert ist „true“. Sie müssen eingeben `-openssl-discover=falsch` um die OpenSSL-Entschlüsselung zu deaktivieren.
`-pidfile <path>`	Gibt die Datei an, in der dieser Server seine Prozess-ID (PID) aufzeichnet.
`-port <value>`	Gibt den TCP-Port an, den der Sensor lauscht auf weitergeleitete Sitzungsschlüssel. Der Standardport ist 4873.
`-server <string>`	Gibt den vollqualifizierten Domänenname des Paket an. Sensor.
`-server-name-override <value>`	Gibt den Betreffnamen aus dem Sensor Zertifikat. Geben Sie diese Option an , wenn dieser Server nur eine Verbindung zu dem Paket herstellen kann Sensor nach IP-Adresse.
`-syslog <facility>`	Gibt die Einrichtung an, die vom Schlüsselweiterleiter gesendet wurde. Die Standardeinrichtung ist local3.
`-t`	Führen Sie einen Konnektivitätstest durch. Sie müssen eingeben `-t=wahr` um mit dieser Option zu laufen.
`-tcp-listen-port <value>`	Gibt den TCP-Port an, auf dem die Schlüsselweiterleitung auf weitergeleitete Sitzungsschlüssel wartet.
`-username <string>`	Gibt den Benutzer an, unter dem der Sitzungsschlüssel-Forwarder nach der Installation der Forwarder-Software ausgeführt wird.
`-v`	Aktivieren Sie die ausführliche Protokollierung. Sie müssen eingeben `-v=true` um mit dieser Option zu laufen.

Linux-Umgebungsvariablen

Die folgenden Umgebungsvariablen ermöglichen es Ihnen, den Session Key Forwarder ohne Benutzerinteraktion zu installieren.

Variabel	Beschreibung	Beispiel
EXTRAHOP_CONNECTION_MODE	Gibt den Verbindungsmodus zum Sitzungsschlüsselempfänger an. Optionen sind richten für selbstverwaltete Sensoren und gehostet für von ExtraHop verwaltete Sensoren.	sudo EXTRAHOP_CONNECTION_MODE=hosted rpm --install extrahop-key-forwarder.x86_64.rpm
EXTRAHOP_EDA_HOSTNAME	Gibt den vollqualifizierten Domänenname des Selbstverwalters an Sensor.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c dpkg --install extrahop-key-forwarder_amd64.deb
EXTRAHOP_LOCAL_LISTENER_PORT	Der Key Forwarder empfängt Sitzungsschlüssel lokal aus der Java-Umgebung über einen TCP-Listener auf localhost (127.0.0.1) und den in der LOCAL_LISTENER_PORT Feld. Wir empfehlen, für diesen Port die Standardeinstellung 598 beizubehalten . Wenn Sie die Portnummer ändern, müssen Sie die ändern -javaagent Argument, um den neuen Port zu berücksichtigen.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_LOCAL_LISTENER_PORT=900 rpm --install extrahop-key-forwarder.x86_64.rpm
EXTRAHOP_SYSLOG	Gibt die Einrichtung oder den Maschinenprozess an, der das Syslog-Ereignis erstellt hat. Die Standardeinrichtung ist local3, das sind Systemdaemon-Prozesse.	sudo EXTRAHOP_CONNECTION_MODE=direct EXTRAHOP_EDA_HOSTNAME=host.example.c EXTRAHOP_SYSLOG=local1 dpkg --install extrahop-key-forwarder_amd64.deb
EXTRAHOP_ADDITIONAL_ARGS	Gibt zusätzliche Optionen für die Schlüsselweiterleitung an.	sudo EXTRAHOP_CONNECTION_MODE=hosted EXTRAHOP_ADDITIONAL_ARGS="-v=true -libcrypto=/some/path/libcrypto.so libcrypto=/some/other/path/libcrypto.so" rpm --install extrahop-key-forwarder.x86_64.rpm

Unterstützte TLS-Verschlüsselungssammlungen
Das ExtraHop-System kann TLS-Verkehr entschlüsseln, der mit PFS- oder RSA-Cipher-Suites verschlüsselt wurde. Alle unterstützten Cipher-Suites können entschlüsselt werden, indem der Session Key Forwarder auf einem Server installiert und das ExtraHop-System konfiguriert wird.

Cipher Suites für RSA können den Datenverkehr auch mit einem Zertifikat und einem privaten Schlüssel entschlüsseln — mit oder ohne Sitzungsschlüsselweiterleitung.

Entschlüsselungsmethoden

Die folgende Tabelle enthält eine Liste von Cipher-Suites, die das ExtraHop-System kann entschlüsseln zusammen mit den unterstützten Entschlüsselungsoptionen.

- **PFS + GPP**: das ExtraHop-System kann diese Verschlüsselungssammlungen mit Sitzungsschlüsselweiterleitung entschlüsseln und Zuordnung von globalem Protokoll zu Port
- **PFS + Zertifikat**: Das ExtraHop-System kann diese Cipher-Suites mit Sitzungsschlüsselweiterleitung entschlüsseln und Zertifikat und privater Schlüssel
- **RSA + Zertifikat**: das ExtraHop-System kann diese Cipher-Suites ohne Weiterleitung des Sitzungsschlüssels entschlüsseln, solange Sie die Datei hochgeladen haben Zertifikat und privater Schlüssel

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0 x 04	TLS_RSA_MIT_RC4_128_MD5	RC4-MD5	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 05	TLS_RSA_MIT_RC4_128_SHA	RC4-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 0A	TLS_RSA_MIT_3DES_EDE_CBC_SHA	DES-CBC3-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 16	TLS_DHE_RSA_MIT_3DES_EDE_CBC_SHA	EDH-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0x2F	TLS_RSA_MIT_AES_128_CBC_SHA	AES128-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0 x 33	TLS_DHE_RSA_MIT_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0x35	TLS_RSA_MIT_AES_256_CBC_SHA	AES256-SHA	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x39	TLS_DHE_RSA_MIT_AES_256_CBC_SHA	DHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0x3C	TLS_RSA_MIT_AES_128_CBC_SHA256	AES128-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x3D	TLS_RSA_MIT_AES_256_CBC_SHA256	AES256-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x67	TLS_DHE_RSA_MIT_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0x6 B	TLS_DHE_RSA_MIT_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256	PFS + GPP PFS + Zertifikat
0x9C	TLS_RSA_MIT_AES_128_GCM_SHA256	AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat RSA + Zertifikat
0x9D	TLS_RSA_MIT_AES_256_GCM_SHA384	AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat RSA + Zertifikat

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0x9E	TLS_DHE_RSA_MIT_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0x9F	TLS_DHE_RSA_MIT_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0 x 1301	TLS_AES_128_GCM_SHA256	TLS_AES_128_GCM_SHA256	PFS + GPP PFS + Zertifikat
0 x 1302	TLS_AES_256_GCM_SHA384	TLS_AES_256_GCM_SHA384	PFS + GPP PFS + Zertifikat
0 x 1303	TLS_CHACHA20_POLY1305_SHA256	TLS_CHACHA20_POLY1305_SHA256	PFS + GPP PFS + Zertifikat
0xC007	TLS_ECDHE_ECDSA_MIT_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA	PFS + GPP
0xC008	TLS_ECDHE_ECDSA_MIT_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA	PFS + GPP
0xC009	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA	PFS + GPP
0xC00A	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA	PFS + GPP
0xC011	TLS_ECDHE_RSA_MIT_RC4_128_SHA	ECDHE-RSA-RC4-SHA	PFS + GPP PFS + Zertifikat
0xC012	TLS_ECDHE_RSA_MIT_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA	PFS + GPP PFS + Zertifikat
0xC013	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA	PFS + GPP PFS + Zertifikat
0xC014	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA	PFS + GPP PFS + Zertifikat
0xC023	TLS_ECDHE_ECDSA_MIT_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256	PFS + GPP
0xC024	TLS_ECDHE_ECDSA_MIT_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384	PFS + GPP
0xC027	TLS_ECDHE_RSA_MIT_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256	PFS + GPP PFS + Zertifikat
0xC028	TLS_ECDHE_RSA_MIT_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384	PFS + GPP PFS + Zertifikat
0xC02B	TLS_ECDHE_ECDSA_MIT_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	PFS + GPP
0xC02C	TLS_ECDHE_ECDSA_MIT_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	PFS + GPP

Hex-Wert	Vorname (IANA)	Nome (OpenSSL)	Unterstützte Entschlüsselung
0xC02F	TLS_ECDHE_RSA_MIT_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	PFS + GPP PFS + Zertifikat
0xC030	TLS_ECDHE_RSA_MIT_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384	PFS + GPP PFS + Zertifikat
0xCCA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat
0xCCA9	TLS_ECDHE_ECDSA_MIT_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305	PFS + GPP
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305	PFS + GPP PFS + Zertifikat

Speichern Sie TLS-Sitzungsschlüssel in verbundenen Paketspeichern

Wenn die Weiterleitung von Sitzungsschlüsseln auf einem ExtraHop-System konfiguriert ist, das mit einem Packetstore verbunden ist, kann das ExtraHop-System verschlüsselte Sitzungsschlüssel zusammen mit den gesammelten Paketen speichern.

Bevor Sie beginnen
Erfahre mehr über Entschlüsseln von Paketen mit gespeicherten Schlüsseln.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. Klicken Sie **Speicher für SSL-Sitzungsschlüssel**.
4. Wählen **SSL-Sitzungsschlüsselspeicher aktivieren**.
5. Klicken Sie **Speichern**.

Nächste Schritte

Weitere Hinweise zum Herunterladen von Sitzungsschlüsseln finden Sie unter Laden Sie Sitzungsschlüssel mit Paket herunter.

Schlüsselweiterleitungen verbundener Sitzungen anzeigen

Sie können kürzlich verbundene Sitzungsschlüsselweiterleitungen anzeigen, nachdem Sie die Sitzungsschlüsselweiterleitung auf Ihrem Server installiert und den TLS-Sitzungsschlüsselempfängerdienst auf dem ExtraHop-System aktiviert haben. Beachten Sie, dass auf dieser Seite nur Sitzungsschlüsselweiterleitungen angezeigt werden, die in den letzten Minuten eine Verbindung hergestellt haben, nicht alle Sitzungsschlüsselweiterleitungen, die derzeit verbunden sind.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Geteilte SSL-Geheimnisse**.

Entschlüsseln Sie den Domänenverkehr mit einem Windows-Domänencontroller

Das ExtraHop-System kann so konfiguriert werden, dass Domänenschlüssel von einem oder mehreren Domänencontrollern abgerufen und gespeichert werden. Wenn das System verschlüsselten Verkehr beobachtet, der den gespeicherten Schlüsseln entspricht, wird der gesamte Kerberos-verschlüsselte Verkehr in der Domäne für unterstützte Protokolle entschlüsselt. Das System synchronisiert nur Kerberos- und NTLM-Entschlüsselungsschlüssel und ändert keine anderen Eigenschaften in der Domäne.

Ein Domänencontroller wie Active Directory ist ein häufiges Ziel von Angreifern, da eine erfolgreiche Angriffskampagne hochwertige Ziele hervorbringt. Kritische Angriffe wie Golden Ticket, PrintNightmare und Bloodhound können durch Kerberos- oder NTLM-Entschlüsselung verdeckt werden. Die Entschlüsselung dieser Art von Datenverkehr kann tiefere Einblicke in Sicherheitserkennungen liefern.

Sie können die Entschlüsselung für eine Person aktivieren Sensor oder durch eine Integration auf RevealX 360. Sie können mehr als eine Domänencontroller-Verbindung von einem Sensor hinzufügen, um den Datenverkehr von mehreren Domänen zu entschlüsseln.

Für die Entschlüsselung müssen die folgenden Anforderungen erfüllt sein:

- Sie müssen über einen Active Directory Directory-Domänencontroller (DC) verfügen, der nicht als schreibgeschützter Domänencontroller (RODC) konfiguriert ist.
- Nur Windows Server 2016, Windows Server 2019 und Windows Server 2022 werden unterstützt.
- Das ExtraHop-System synchronisiert Schlüssel für bis zu 50.000 Konten in einer konfigurierten Domain. Wenn Ihr DC mehr als 50.000 Konten hat, wird ein Teil des Datenverkehrs nicht entschlüsselt.
- Das ExtraHop-System muss den Netzwerkverkehr zwischen dem DC und den angeschlossenen Clients und Servern beobachten.
- Das ExtraHop-System muss über die folgenden Ports auf den Domänencontroller zugreifen können: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC) und TCP-Ports 49152-65535 (RPC-Dynamikbereich).

Warnung: Wenn Sie diese Einstellungen aktivieren, erhält das ExtraHop-System Zugriff auf alle Kontoschlüssel in der Windows-Domäne. Das ExtraHop-System sollte auf derselben Sicherheitsstufe wie der Domänencontroller bereitgestellt werden. Hier sind einige bewährte Methoden, die Sie berücksichtigen sollten:

- Beschränken Sie den Endbenutzerzugriff strikt auf Sensoren die mit Zugriff auf den Domänencontroller konfiguriert sind. Erlauben Sie im Idealfall nur Endbenutzern den Zugriff auf ein verbundenes Konsole.
- Konfiguriere Sensoren mit einem Identitätsanbieter, der über starke Authentifizierungsfunktionen wie Zweifaktor- oder Multi-Faktor-Authentifizierung verfügt.
- Beschränken Sie den eingehenden und ausgehenden Verkehr zum und vom Sensor nur auf das, was benötigt wird.
- Beschränken Sie in Active Directory die Logon-Workstations für das Konto so, dass sie nur mit dem Domänencontroller kommunizieren, mit dem das ExtraHop-System konfiguriert ist.

Einen Domänencontroller an einen Sensor anschließen

Bevor Sie beginnen
Sie benötigen ein Benutzerkonto bei Setup oder System- und Zugriffsadministrationsrechte auf dem Sensor.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Domänencontroller**.
4. Klicken Sie **Domänencontroller-Verbindung hinzufügen**.

5. Füllen Sie die folgenden Felder aus, um Anmeldedaten für den Microsoft Active Directory-Domänencontroller anzugeben, den Sie mit diesem Sensor verbinden möchten:
   - **Gastgeber:** Der vollqualifizierte Domänenname des Domänencontroller.
   - **Computername (sAMAccountName):** Der Name des Domänencontroller.
   - **Bereichsname:** Der Name des Kerberos-Bereichs, in dem der Domänencontroller autorisiert ist .
   - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domänen-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
   - **Passwort:** Das Passwort des privilegierten Benutzers.
6. Klicken Sie **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
7. Klicken Sie **Speichern**.
   Der Verbindungsstatus und ein Zeitstempel der letzten erfolgreichen Synchronisierung werden angezeigt.

Nächste Schritte

- Klicken Sie **Domänencontroller-Verbindung hinzufügen** um eine Verbindung zu einem anderen Domänencontroller herzustellen.
- Klicken Sie **Benutzeranmeldedaten ändern** von einer gespeicherten Verbindung, um die mit der Verbindung verknüpften Anmeldedaten zu ändern.
- Klicken Sie **Verbindung entfernen** um alle mit der Verbindung verknüpften Anmeldedaten zu löschen und den Domänencontroller vom Sensor zu trennen.

Verbinden Sie einen Domänencontroller mit einem RevealX 360-Sensor

Bevor Sie beginnen
Ihr Benutzerkonto muss Privilegien auf RevealX 360 für System- und Zugriffsadministration.

1. Loggen Sie sich in RevealX 360 ein.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Integrationen**.
3. Klicken Sie auf **Entschlüsselung des Microsoft-Protokolls** Kachel.
4. klicken **Anmeldeinformationen hinzufügen**.
5. Füllen Sie die folgenden Felder aus, um Anmeldedaten für den Microsoft Active Directory-Domänencontroller anzugeben, den Sie mit einem RevealX 360-Sensor verbinden möchten:
   - **Gastgeber:** Der vollqualifizierte Domänenname des Domänencontroller.
   - **Computername (sAMAccountName):** Der Name des Domänencontroller.
   - **Bereichsname:** Der Name des Kerberos-Bereichs, in dem der Domänencontroller autorisiert ist .
   - **Nutzername:** Der Name eines Benutzers, der Mitglied der integrierten Administratorgruppe für die Domain ist (nicht zu verwechseln mit der Gruppe Domänen-Admins). Um mögliche Verbindungsfehler zu vermeiden, geben Sie ein Benutzerkonto an, das nach der Einrichtung des Domänencontrollers erstellt wurde.
   - **Passwort:** Das Passwort des privilegierten Benutzers.
6. Wählen Sie aus der Dropdownliste den RevealX 360-Sensor aus, mit dem der Domänencontroller eine Verbindung herstellen soll.
7. klicken **Verbindung testen** um zu bestätigen, dass der Sensor mit dem Domänencontroller kommunizieren kann.
8. klicken **Verbinde**.
   Der Verbindungsstatus und ein Zeitstempel der letzten erfolgreichen Synchronisierung werden angezeigt.

Nächste Schritte

- klicken **Domänencontroller-Verbindung hinzufügen** um eine Verbindung zu einem anderen Domänencontroller herzustellen.
- klicken **Benutzeranmeldedaten ändern** von einer gespeicherten Verbindung, um die mit der Verbindung verknüpften Anmeldedaten zu ändern.
- klicken **Anmeldeinformationen löschen** um alle mit der Verbindung verknüpften Anmeldedaten zu löschen und den Domänencontroller vom Sensor zu trennen.

Überprüfen Sie die Konfigurationseinstellungen

Um zu überprüfen, ob das ExtraHop-System in der Lage ist, Datenverkehr mit konfigurierten Domänencontrollern zu entschlüsseln, rufen Sie das integrierte Microsoft Protocol Decryption Dashboard auf, um erfolgreiche Entschlüsselungsversuche zu identifizieren.

Jedes Diagramm im Microsoft Protocol Decryption-Dashboard enthält Visualisierungen der Kerberos-Entschlüsselungsdaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Das Microsoft Protocol Decryption-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsam genutzten Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Microsoft Protocol Decryption-Dashboard und fügen Sie es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Hinweis: Das Microsoft Protocol Decryption-Dashboard kann nur auf einer Konsole angezeigt werden.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Kerberos-Entschlüsselungsversuche

Beachten Sie die Anzahl der Kerberos-Entschlüsselungsversuche in Ihrer Umgebung in den folgenden Diagrammen:

- **Erfolgreiche Kerberos-Entschlüsselungsversuche:** Gesamtzahl der erfolgreichen Kerberos-Entschlüsselungsversuche und deren Zeitpunkt.
- **Gesamtzahl erfolgreicher Versuche:** Gesamtzahl der erfolgreichen Kerberos-Entschlüsselungsversuche.
- **Erfolglose Kerberos-Entschlüsselungsversuche:** Gesamtzahl der erfolglosen Kerberos-Entschlüsselungsversuche und deren Zeitpunkt, aufgeführt nach dem Grund, warum der Versuch fehlgeschlagen ist.
- **Gesamtzahl erfolgloser Versuche:** Gesamtzahl der erfolglosen Kerberos-Entschlüsselungsversuche, aufgelistet nach dem Grund, warum der Versuch fehlgeschlagen ist.

Details zur erfolglosen Kerberos-Entschlüsselung

Beachten Sie die Details zu erfolglosen Kerberos-Entschlüsselungsversuchen in den folgenden Diagrammen:

- **Unbekannte Serverprinzipalnamen:** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines unbekannten Serverprinzipalnamens (SPN) fehlgeschlagen sind, aufgeführt im SPN. Wird als Balkendiagramm und Listendiagramm angezeigt.
- **Ungültige Kerberos-Schlüssel:** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines ungültigen Kerberos-Schlüssels fehlgeschlagen sind, aufgeführt im SPN, der den Versuch unternommen hat. Wird als Balkendiagramm und Listendiagramm angezeigt.
- **Kerberos-Entschlüsselungsfehler :** Gesamtzahl der Kerberos-Entschlüsselungsversuche, die aufgrund eines Fehlers fehlgeschlagen sind, aufgeführt im SPN, der den Versuch unternommen hat. Wird als Balkendiagramm und Listendiagramm angezeigt.

Einzelheiten zum Serverprinzipalnamen

Beachten Sie in den folgenden Diagrammen den wichtigsten SPN, der Kerberos-Entschlüsselungsversuche unternommen hat:

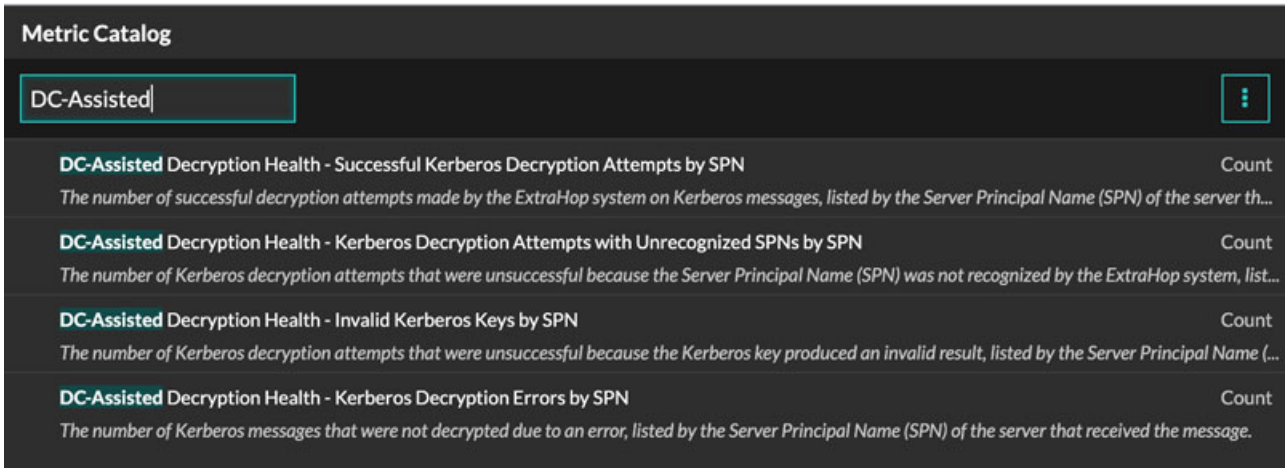
• **Die wichtigsten Serverprinzipalnamen:** Die 50 wichtigsten SPNs, die Kerberos-Entschlüsselungsversuche unternommen haben, und die folgenden Details:

- Die Anzahl erfolgreicher Entschlüsselungsversuche.
- Die Anzahl der erfolglosen Versuche aufgrund eines ungültigen Kerberos-Schlüssels.
- Die Anzahl der erfolglosen Versuche aufgrund eines Fehlers.
- Die Anzahl der erfolglosen Versuche aufgrund eines unbekannten SPN.

Zusätzliche Metriken zur Systemintegrität

Das ExtraHop-System bietet Metriken, die Sie einem Dashboard hinzufügen können, um den Zustand und die Funktionalität der DC-gestützten Entschlüsselung zu überwachen.

Um eine Liste der verfügbaren Metriken anzuzeigen, klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Metrischer Katalog**. Typ `DC-unterstützt` im Filterfeld, um alle verfügbaren DC-unterstützten Entschlüsselungsmetriken anzuzeigen.



Importieren Sie externe Daten in Ihr ExtraHop-System

Die ExtraHop Open Data Context API ermöglicht es Ihnen, Daten von einem externen Host in die Sitzungstabelle auf Ihrem ExtraHop zu importieren. Sensor. Auf diese Daten kann dann zugegriffen werden, um benutzerdefinierte Messwerte zu erstellen , die Sie zu ExtraHop-Diagrammen hinzufügen, in Datensätzen in einem Recordstore speichern oder in ein externes Analysetool exportieren können.

Nachdem Sie die Open Data Context API auf Ihrem aktiviert haben Sensor, können Sie Daten importieren, indem Sie ein Python-Skript von einem Memcache-Client auf einem externen Host ausführen. Diese externen Daten werden in Schlüssel-Wert-Paaren gespeichert und können durch Schreiben eines Auslöser abgerufen werden.

Sie könnten beispielsweise ein Memcached-Client-Skript auf einem externen Host ausführen, um CPU-Lastdaten in die Sitzungstabelle auf Ihrem Sensor. Anschließend können Sie einen Auslöser schreiben, der auf die Sitzungstabelle zugreift und die Daten als benutzerdefinierte Metriken festschreibt.

Warnung: Die Verbindung zwischen dem externen Host und dem ExtraHop-System ist nicht verschlüsselt und sollte keine vertraulichen Informationen übertragen.

Aktivieren Sie die Open Data Context API

Sie müssen die Open Data Context API auf Ihrem aktivieren Sensor bevor es Daten von einem externen Host empfangen kann.

Bevor Sie beginnen

- Sie müssen eingerichtet haben oder System- und Zugriffsadministrationsrechte um auf die Administrationsseite Ihres ExtraHop-Systems zuzugreifen.

- Wenn Sie über eine Firewall verfügen, müssen Ihre Firewallregeln externen Hosts den Zugriff auf die angegebenen TCP- und UDP-Ports ermöglichen. Die Standard-Portnummer ist 11211.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Datenkontext-API öffnen**.
4. klicken **Open Data Context API aktivieren**.
5. Konfigurieren Sie jedes Protokoll, über das Sie externe Datenübertragungen zulassen möchten:

Option	Description
TCP	1. Wählen Sie die **TCP-Port aktiviert** Ankreuzfeld. 2. In der **TCP-Anschluss** In diesem Feld geben Sie die Portnummer ein, die externe Daten empfangen soll.
UDP	1. Wählen Sie die **UDP-Port aktiviert** Ankreuzfeld. 2. In der **UDP-Anschluss** In diesem Feld geben Sie die Portnummer ein, die externe Daten empfangen soll.

6. klicken **Speichern Sie die Aufnahme und starten Sie sie neu**.

   Wichtig: Der Sensor erfasst keine Messwerte, während er neu gestartet wird.

7. Klicken Sie **Erledigt**.

Schreiben Sie ein Python-Skript, um externe Daten zu importieren
Bevor Sie externe Daten in die Sitzungstabelle auf Ihrem importieren können Sensor, Sie müssen ein Python-Skript schreiben, das Ihre identifiziert Sensor und enthält die Daten, die Sie in die Sitzungstabelle importieren möchten. Das Skript wird dann von einem Memcache-Client auf dem externen Host ausgeführt.

Dieses Thema enthält Anleitungen zur Syntax und bewährte Methoden für das Schreiben des Python-Skripts. Ein vollständiges Skriptbeispiel ist am Ende dieses Handbuchs verfügbar.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie einen Memcached-Client auf dem externen Host-Computer haben. Sie können jede Standard-Memcached-Clientbibliothek installieren, z. B. http://libmemcached.org/ oder https://pypi.python.org/pypi/pymemcache. Der Sensor fungiert als Memcached-Server der Version 1.4.

Hier sind einige wichtige Überlegungen zur Open Data Context API:

- Die Open Data Context API unterstützt die meisten Memcached-Befehle, wie `get`, `set`, und `increment`.
- Alle Daten müssen als Zeichenketten eingefügt werden, die lesbar sind für Sensor. Einige Memcached-Clients versuchen, Typinformationen in den Werten zu speichern. Die Python-Memcache-Bibliothek speichert beispielsweise Floats als ausgewählte Werte, die beim Aufrufen zu ungültigen Ergebnissen führen `Session.lookup` in Auslösern. Die folgende Python-Syntax fügt einen Float korrekt als Zeichenfolge ein:

```
mc.set("my_float", str(1.5))
```

- Obwohl die Größe von Sitzungstabellenwerten nahezu unbegrenzt sein kann, kann das Festschreiben großer Werte in die Sitzungstabelle zu Leistungseinbußen führen. Darüber hinaus müssen Metriken,

die an den Datenspeicher übergeben werden, 4096 Byte oder weniger groß sein, und zu große Tabellenwerte können zu verkürzten oder ungenauen Metriken führen.
- Einfache Statistikberichte werden unterstützt, detaillierte Statistikberichte nach Elementgröße oder Schlüsselpräfix werden jedoch nicht unterstützt.
- Das Festlegen des Ablaufs von Artikeln beim Hinzufügen oder Aktualisieren von Artikeln wird unterstützt, aber das Massenablaufdatum wird über die `flush` Befehl wird nicht unterstützt.
- Schlüssel laufen in 30-Sekunden-Intervallen ab. Wenn ein Schlüssel beispielsweise so eingestellt ist, dass er in 50 Sekunden abläuft, kann es zwischen 50 und 79 Sekunden dauern, bis er abläuft.
- Alle mit der Open Data Context API festgelegten Schlüssel werden über die verfügbar gemacht `SESSION_EXPIRE` lösen ein Ereignis aus, wenn sie ablaufen. Dieses Verhalten steht im Gegensatz zur Trigger-API, die ablaufende Schlüssel nicht über die `SESSION_EXPIRE` Ereignis.

1. Öffnen Sie in einem Python-Editor eine neue Datei.
2. Fügen Sie die IP-Adresse Ihres Sensor und die Portnummer, an die der Memcached-Client Daten sendet, ähnlich der folgenden Syntax:

   ```
   client = memcache.Client(["eda_ip_address:eda_port"])
   ```
3. Fügen Sie die Daten, die Sie importieren möchten, über Memcached zur Sitzungstabelle hinzu `set` Befehl, formatiert in Schlüssel-Wert-Paaren, ähnlich der folgenden Syntax:

   ```
   client.set("some_key", "some_value")
   ```
4. Speichern Sie die Datei.
5. Führen Sie das Python-Skript vom Memcached-Client auf dem externen Host aus.

Schreiben Sie einen Auslöser für den Zugriff auf importierte Daten
Sie müssen einen Auslöser schreiben, bevor Sie auf die Daten in der Sitzungstabelle zugreifen können.

Bevor Sie beginnen
In diesem Thema wird Erfahrung mit dem Schreiben von Triggern vorausgesetzt. Wenn Sie mit Triggern nicht vertraut sind, schauen Sie sich die folgenden Themen an:

- Trigger
- Einen Auslöser erstellen
- Erfahren Sie, wie Sie einen Auslöser zum Sammeln benutzerdefinierter Metriken erstellen

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Neu**, und klicken Sie dann auf Konfiguration Registerkarte.
4. In der **Name** Feld, geben Sie einen eindeutigen Namen für den Auslöser ein.
5. In der **Ereignisse** Feld, beginnen Sie mit der Eingabe eines Veranstaltungsnamens und wählen Sie dann ein Ereignis aus der gefilterten Liste aus.
6. Klicken Sie auf **Herausgeber** Registerkarte.
7. In der Trigger-Skript Textfeld, schreiben Sie ein Triggerskript, das auf die Daten der Sitzungstabelle zugreift und diese anwendet. EIN vollständiges Skriptbeispiel ist am Ende dieses Handbuchs verfügbar.

   Das Skript muss das enthalten `Session.lookup` Methode, um einen bestimmten Schlüssel in der Sitzungstabelle zu finden und den entsprechenden Wert zurückzugeben.

   Der folgende Code sucht beispielsweise nach einem bestimmten Schlüssel in der Sitzungstabelle, um den entsprechenden Wert zurückzugeben, und überträgt den Wert dann als benutzerdefinierte Metrik an eine Anwendung:

   ```
   var key_lookup = Session.lookup("some_key");
                    Application("My
    App").metricAddDataset("my_custom_metric",
   ```

```
                key_lookup);
```

Hinweis: Sie können Schlüssel-Wert-Paare in der Sitzungstabelle auch mithilfe der Methoden hinzufügen, ändern oder löschen, die in der Session Klasse der ExtraHop Trigger API-Referenz .

8. klicken **Speichern und schließen**.

Nächste Schritte
Sie müssen den Auslöser einem Gerät oder einer Gerätegruppe zuweisen. Der Auslöser wird erst ausgeführt, wenn er zugewiesen wurde.

Beispiel für eine Open Data Context API
In diesem Beispiel erfahren Sie, wie Sie den Reputationswert und das potenzielle Risiko von Domains überprüfen, die mit Geräten in Ihrem Netzwerk kommunizieren. Zunächst zeigt Ihnen das Python-Beispielskript, wie Sie Domain-Reputationsdaten in die Sitzungstabelle auf Ihrem importieren Sensor. Anschließend zeigt Ihnen das Beispiel-Triggerskript, wie Sie IP-Adressen bei DNS-Ereignissen mit den importierten Domain-Reputationsdaten vergleichen und wie Sie aus den Ergebnissen eine benutzerdefinierte Metrik erstellen.

Beispiel für ein Python-Skript

Dieses Python-Skript enthält eine Liste von 20 beliebten Domainnamen und kann auf Domain-Reputationswerte verweisen, die aus einer Quelle wie Domain-Tools.

Dieses Skript ist eine REST-API, die eine POST-Operation akzeptiert, bei der der Hauptteil der Domänenname ist. Bei einem POST-Vorgang aktualisiert der Memcached-Client die Sitzungstabelle mit den Domäneninformationen.

```
#!/usr/bin/python
import flask
import flask_restful
import memcache
import sqlite3

top20 = { "google.com", "facebook.com", "youtube.com", "twitter.com",
          "microsoft.com", "wikipedia.org", "linkedin.com",
          "apple.com","adobe.com", "wordpress.org", "instagram.com",
          "wordpress.com", "vimeo.com", "blogspot.com", "youtu.be",
          "pinterest.com", "yahoo.com", "goo.gl", "amazon.com", "bit.ly}

dnsnames = {}

mc = memcache.Client(['10.0.0.115:11211'])

for dnsname in top20:
    dnsnames[dnsname] = 0.0

dbc = sqlite3.Connection('./dnsreputation.db')
cur = dbc.cursor()
cur.execute('select dnsname, score from dnsreputation;')
for row in cur:
    dnsnames[row[0]] = row[1]
dbc.close()

app = flask.Flask(__name__)
api = flask_restful.Api(app)

class DnsReputation(flask_restful.Resource):
    def post(self):
        dnsname = flask.request.get_data()
        #print dnsname
```

```
        mc.set(dnsname, str(dnsnames.get(dnsname, 50.0)), 120)
        return 'added to session table'

api.add_resource(DnsReputation, '/dnsreputation')

if __name__ == '__main__':
     app.run(debug=True,host='0.0.0.0')
```

Beispiel für ein Trigger-Skript

Dieses Beispiel-Triggerskript kanonisiert (oder konvertiert) IP-Adressen, die bei DNS-Ereignissen zurückgegeben werden, in Domänennamen und sucht dann in der Sitzungstabelle nach der Domain und ihrem Reputationswert. Wenn der Punktewert größer als 75 ist, fügt der Auslöser die Domain einem Anwendungscontainer mit dem Namen „DNSReputation“ als Detail-Metrik namens „Bad DNS reputation“ hinzu.

```
//Configure the following trigger settings:
//Name: DNSReputation
//Debugging: Enabled
//Events: DNS_REQUEST, DNS_RESPONSE

if (DNS.errorNum != 0 || DNS.qname == null
    || DNS.qname.endsWith("in-addr.arpa") || DNS.qname.endsWith("local")
    || DNS.qname.indexOf('.') == -1 ) {
    // error or null or reverse lookup, or lookup of local namereturn
    return;
}

//var canonicalname = DNS.qname.split('.').slice(-2).join('.');
var canonicalname = DNS.qname.substring(DNS.qname.lastIndexOf('.',
 DNS.qname.lastIndexOf('.')-1)+1)

//debug(canonicalname);


//Look for this DNS name in the session table
var score = Session.lookup(canonicalname)
if (score === null) {
    // Send to the service for lookup
    Remote.HTTP("dnsrep").post({path: "/dnsreputation", payload:
 canonicalname});
} else {
    debug(canonicalname + ':' +score);
    if (parseFloat(score) > 75) {
  //Create an application in the ExtraHop system and add custom metrics
        //Note: The application is not displayed in the ExtraHop system
 after the
  //initial request, but is displayed after subsequent requests.
        Application('DNSReputation').metricAddDetailCount('Bad DNS
 reputation', canonicalname + ':' + score, 1);
    }
}
```

Installieren Sie den Paket Forwarder auf einem Linux-Server

Sie müssen die Paketweiterleitungssoftware auf jedem Server installieren, der überwacht werden soll, um Pakete an das ExtraHop-System weiterzuleiten.

RPCAP-Installationsdateien und Anweisungen finden Sie unter ExtraHop Downloads und Ressourcen Webseite.

Herunterladen und Installieren auf RPM-basierten Systemen

1. Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter Downloads und Ressourcen Webseite.
2. Installieren Sie die Software auf dem Server, indem Sie den folgenden Befehl ausführen:

   ```
   sudo rpm -i rpcapd-<extrahop_firmware_version>.x86_64.rpm
   ```

3. Öffne und bearbeite den `rpcapd.ini` Datei in einem Texteditor, indem Sie einen der folgenden Befehle ausführen:

   ```
   vim /opt/extrahop/etc/rpcapd.ini
   ```

   ```
   nano /opt/extrahop/etc/rpcapd.ini
   ```

   Beispiel für eine Ausgabe:

   ```
   #ActiveClient = <TARGETIP>,<TARGETPORT>
   NullAuthPermit = YES
   UserName = rpcapd
   ```

   Ersetzen `<TARGETIP>` mit der IP-Adresse des ExtraHop-Systems und `<TARGETPORT>` mit `2003`. Entkommentieren Sie die Zeile zusätzlich, indem Sie das Nummernzeichen löschen (#) am Anfang der Zeile.

   Zum Beispiel:

   ```
   ActiveClient = 10.10.10.10,2003
   NullAuthPermit = YES
   UserName = rpcapd
   ```

4. Starten Sie das Senden des Datenverkehrs an das ExtraHop-System, indem Sie den folgenden Befehl ausführen:

   ```
   sudo /etc/init.d/rpcapd start
   ```

5. Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie den folgenden Befehl ausführen:

   ```
   sudo service rpcapd status
   ```

Downloaden und auf anderen Linux-Systemen installieren

1. Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter Downloads und Ressourcen Webseite.
2. Installieren Sie die Software auf dem Server, indem Sie die folgenden Befehle ausführen:
   a) Extrahieren Sie die Paket Forwarder-Dateien aus der Archivdatei:

   ```
   tar xf rpcapd-<extrahop_firmware_version>.tar.gz
   ```

   b) Wechseln Sie zu `rpcapd` Verzeichnis:

   ```
   cd rpcapd
   ```

   c) Führen Sie das Installationsskript aus:

   ```
   sudo ./install.sh <extrahop_ip> 2003
   ```

3. Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie den folgenden Befehl ausführen:

```
sudo /etc/init.d/rpcapd status
```

Informationen zum Ausführen der Software auf Servern mit mehreren Schnittstellen finden Sie unter Überwachung mehrerer Schnittstellen auf einem Linux-Server.

Downloaden und installieren Sie auf Debian-basierten Systemen
Um den Paketweiterleiter herunterzuladen und auf Debian-basierten Systemen zu installieren:

1. Laden Sie die RPCAP-Installationsdatei vom ExtraHop herunter Downloads und Ressourcen Webseite.
2. Installieren Sie die Software auf dem Server, indem Sie den folgenden Befehl ausführen:

```
sudo dpkg -i rpcapd_<extrahop_firmware_version>_amd64.deb
```

3. Geben Sie an der Eingabeaufforderung die ExtraHop-System-IP-Adresse ein, bestätigen Sie die Standardverbindung zu Port 2003 und drücken Sie die EINGABETASTE.
4. Optional: Stellen Sie sicher, dass das ExtraHop-System Datenverkehr empfängt, indem Sie die folgenden Befehle ausführen:

```
sudo dpkg --get-selections | grep rpcapd
```

```
sudo service rpcapd status
```

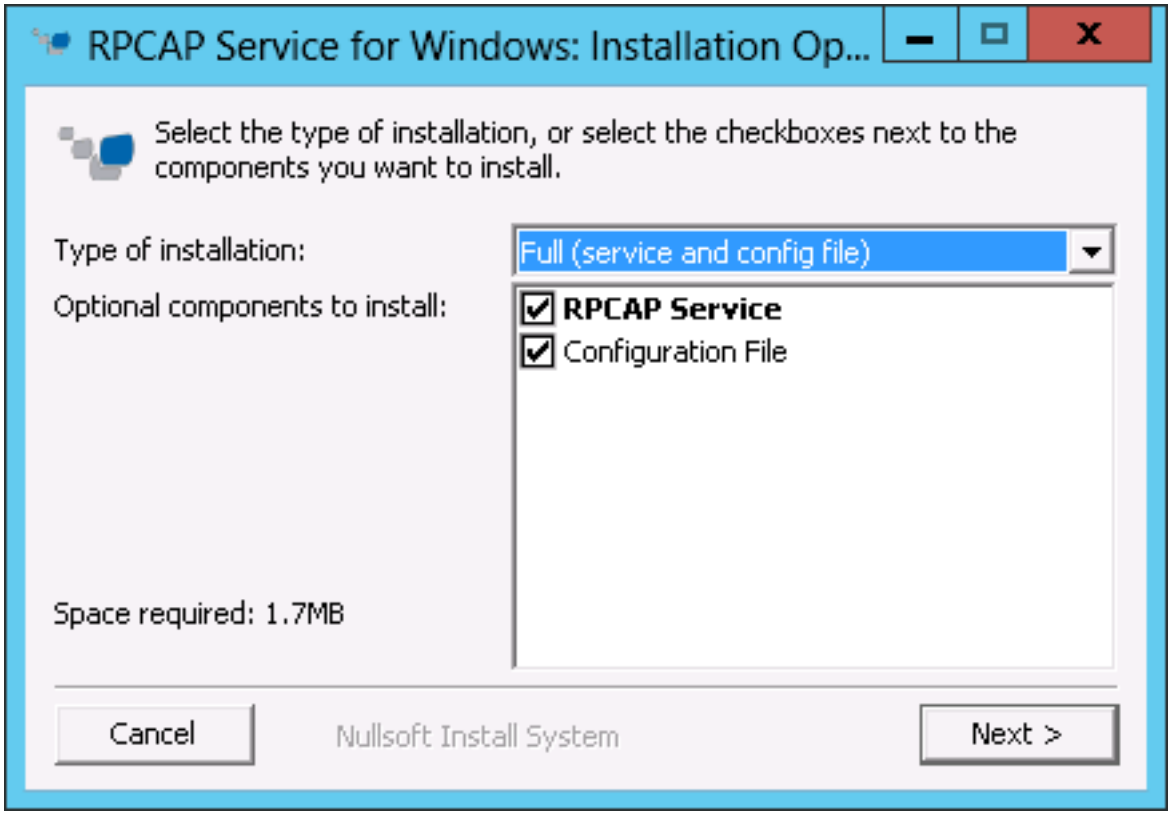
5. Optional: Führen Sie den folgenden Befehl aus, um die IP-Adresse, die Portnummer oder die Argumente des ExtraHop-Systems für den Dienst zu ändern:

```
sudo dpkg-reconfigure rpcapd
```

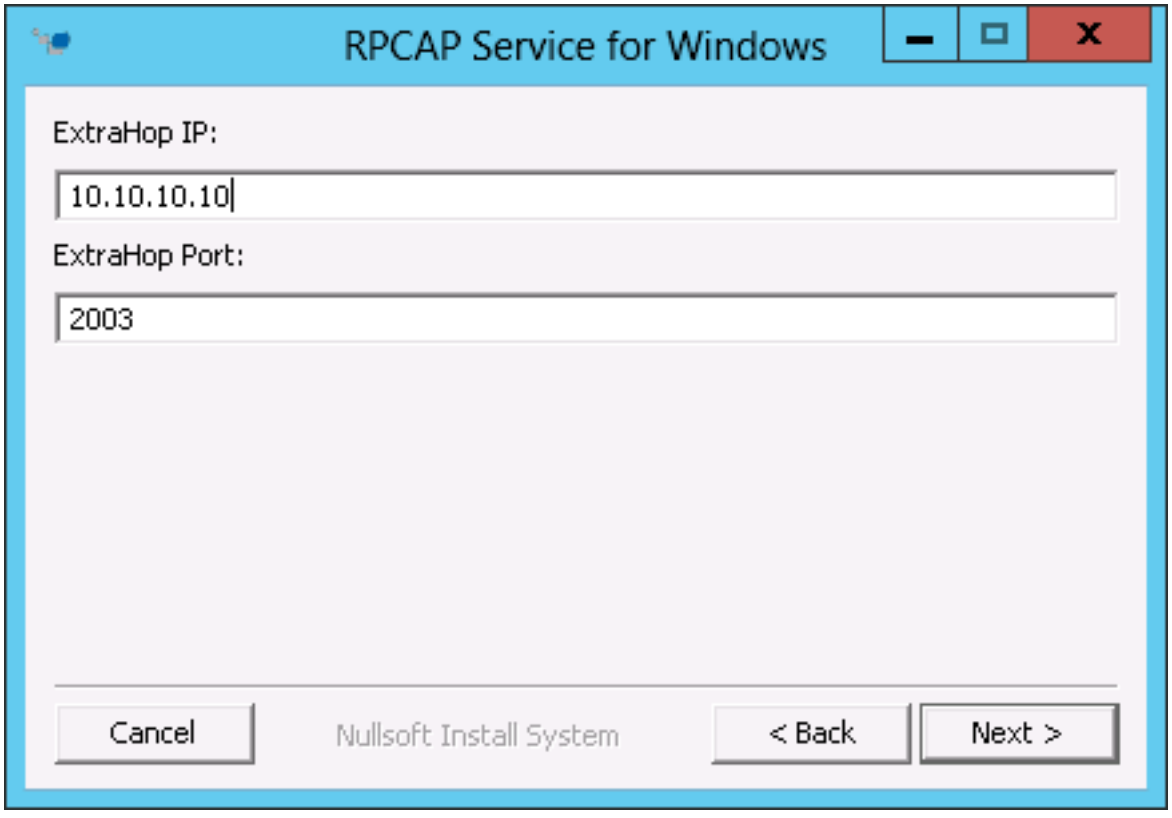
Installieren Sie den Paket Forwarder auf einem Windows-Server

Sie müssen die Paketweiterleitungssoftware auf jedem zu überwachenden Server installieren, um Pakete an das ExtraHop-System weiterzuleiten.

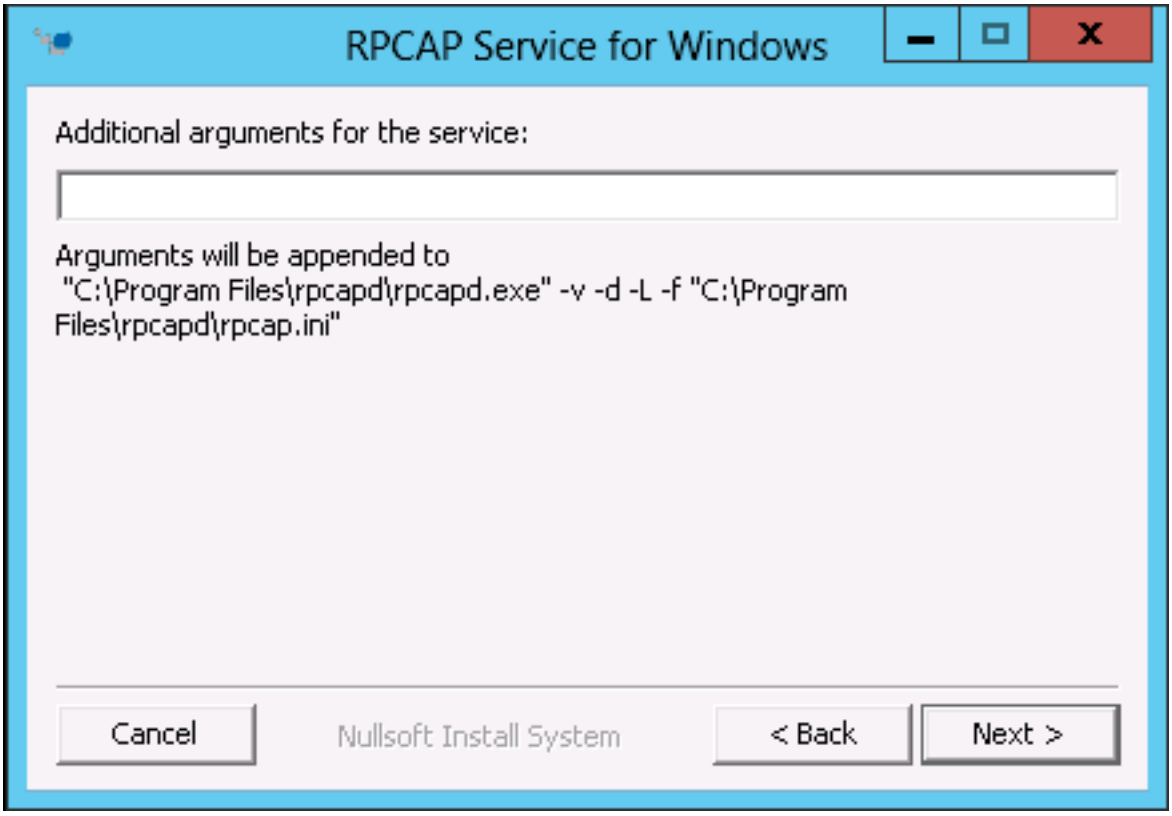
1. Laden Sie die Installationsdatei für den RPCAP-Service für Windows aus dem ExtraHop herunter Downloads und Ressourcen Webseite.
2. Doppelklicken Sie auf die Datei, um das Installationsprogramm zu starten.
3. Wählen Sie im Assistenten die zu installierenden Komponenten aus.



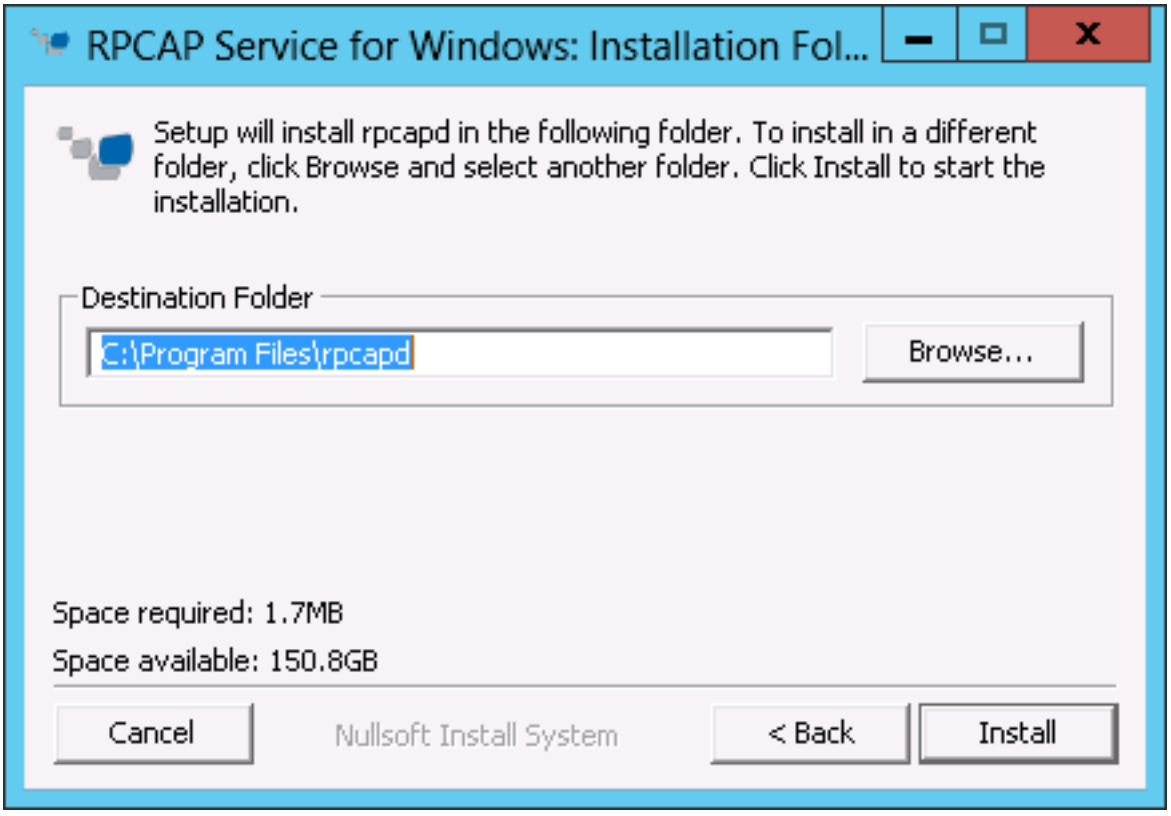
4. Vervollständigen Sie die **Extra Hop IP** und **ExtraHop-Anschluss** Felder und klicken **Weiter**. Der Standardport ist 2003.



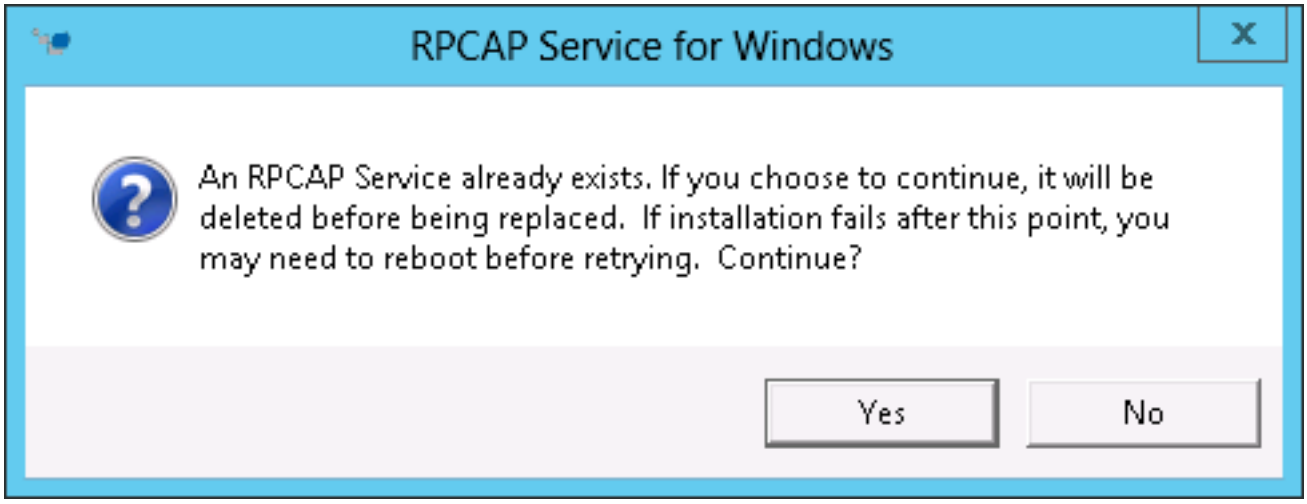
5. Optional: Geben Sie zusätzliche Argumente in das Textfeld ein und klicken Sie auf **Weiter**.



6. Navigieren Sie zum Zielordner, um den RPCAP Service zu installieren, und wählen Sie ihn aus.



7. Wenn der RPCAP-Dienst zuvor installiert war, klicken Sie auf **Ja** um den vorherigen Dienst zu löschen.



8. Wenn die Installation abgeschlossen ist, klicken Sie auf **Schliessen**.

Überwachung mehrerer Schnittstellen auf einem Linux-Server

Für Server mit mehreren Schnittstellen können Sie den Paketweiterleiter so konfigurieren, dass er Pakete von einer bestimmten Schnittstelle oder von mehreren Schnittstellen weiterleitet, indem Sie seine Konfigurationsdatei auf dem Server bearbeiten.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Öffnen Sie nach der Installation des Paketweiterleiters die Konfigurationsdatei, `/opt/extrahop/etc/rpcapd.ini`.

   Die Konfigurationsdatei enthält diesen oder einen ähnlichen Text:

   ```
   ActiveClient = 10.0.0.100,2003
   NullAuthPermit = YES
   UserName = rpcapd
   ```

   Hinweis Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

2. Ändern Sie das Bestehende `ActiveClient` Linie und erstelle eine `ActiveClient` Leitung für jede weitere zu überwachende Schnittstelle. Geben Sie jede Schnittstelle anhand ihres Schnittstellennamens oder ihrer IP-Adresse an.

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_name>
   ```

   oder

   ```
   ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_address>
   ```

   Wo *<interface_name>* ist der Name der Schnittstelle, von der Sie Pakete weiterleiten möchten, und *<interface_address>* ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden. Das *<interface_address>* Variable kann entweder die IP-Adresse selbst sein, z. B. 10.10.1.100, oder eine CIDR-Spezifikation (Netzwerk-IP-Adresse/Subnetzpräfixlänge), die die IP-Adresse enthält, z. B. 10.10.1.0/24.

   Für jeden `ActiveClient` Leitung, leitet der Paketweiterleiter unabhängig Pakete von der in der Zeile angegebenen Schnittstelle weiter.

   Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen anhand des Schnittstellennamens angegeben sind:

   ```
   ActiveClient = 10.10.6.45, 2003, ifname=eth0
   ```

```
ActiveClient = 10.10.6.45, 2003, ifname=eth1
NullAuthPermit = YES
UserName = rpcapd
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen anhand der Schnittstellen-IP-Adresse angegeben werden:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
UserName = rpcapd
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen mithilfe von CIDR-Spezifikationen angegeben werden, die die Schnittstellen-IP-Adresse enthalten:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
UserName = rpcapd
```

3. Speichern Sie die Konfigurationsdatei. Stellen Sie sicher, dass Sie die Datei im ASCII-Format speichern, um Fehler zu vermeiden.
4. Starten Sie den Paketweiterleiter neu, indem Sie den folgenden Befehl ausführen:

```
sudo /etc/init.d/rpcapd restart
```

Hinweis: Um den Paketweiterleiter nach dem Ändern der Konfigurationsdatei erneut zu installieren, führen Sie den Installationsbefehl aus und ersetzen Sie *<extrahop_ip>* und *<extrahop_port>* mit dem `–k` Flag, um die geänderte Konfigurationsdatei beizubehalten. Zum Beispiel:

```
sudo sh ./install-rpcapd.sh –k
```

Überwachung mehrerer Schnittstellen auf einem Windows-Server

Für Server mit mehreren Schnittstellen können Sie den Paketweiterleiter so konfigurieren, dass er Pakete von einer bestimmten Schnittstelle oder von mehreren Schnittstellen weiterleitet, indem Sie seine Konfigurationsdatei auf dem Server bearbeiten.

Gehen Sie wie folgt vor, um die Konfigurationsdatei zu bearbeiten.

1. Öffnen Sie nach der Installation des Paketweiterleiters auf dem Server die Konfigurationsdatei: `C:\Program Files\rpcapd\rpcapd.ini`

   Die Konfigurationsdatei enthält diesen oder einen ähnlichen Text:

```
ActiveClient = 10.0.0.100,2003
NullAuthPermit = YES
UserName = rpcapd
```

   Hinweis: Ändern Sie nicht die `NullAuthPermit` oder `UserName` Felder.

2. Ändern Sie die vorhandene ActiveClient-Zeile und erstellen Sie eine ActiveClient-Zeile für jede weitere Schnittstelle, die überwacht werden soll. Geben Sie jede Schnittstelle anhand ihres Schnittstellennamens oder ihrer IP-Adresse an.

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifname=<interface_address>
```

   Wo *<interface_address>* ist die IP-Adresse der Schnittstelle, von der die Pakete weitergeleitet werden und *<interface_address>* kann entweder die IP-Adresse selbst sein, z. B. 10.10.1.100, oder eine

CIDR-Spezifikation (Netzwerk-IP-Adresse/Subnetzpräfixlänge), die die IP-Adresse enthält, z. B. 10.10.1.0/24.

oder

```
ActiveClient = <extrahop_ip>, <extrahop_port>, ifaddr=<interface_name>
```

Wo *<interface_name>* ist der Name der Schnittstelle, von der die Pakete weitergeleitet werden. Der Name ist formatiert als `\Device\NPF_{<GUID>}`, wo *<GUID>* ist der Globally Unique Identifier (GUID) der Schnittstelle. Zum Beispiel, wenn die Schnittstellen-GUID `2C2FC212-701D-42E6-9EAE-BEE969FEFB3F`, der Schnittstellenname ist `\Device\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}`.

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen mit der Schnittstellen-IP-Adresse angegeben sind:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.100
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.100
NullAuthPermit = YES
UserName = rpcapd
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen mit CIDR-Spezifikationen angegeben sind, die die Schnittstellen-IP-Adresse enthalten:

```
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.1.0/24
ActiveClient = 10.10.6.45, 2003, ifaddr=10.10.2.0/24
NullAuthPermit = YES
UserName = rpcapd
```

Im Folgenden finden Sie ein Beispiel für die Konfigurationsdatei, in der zwei Schnittstellen mit dem Schnittstellennamen angegeben sind:

```
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{2C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
ActiveClient = 10.10.6.45, 2003, ifname=\Device
\NPF_{3C2FC212-701D-42E6-9EAE-BEE969FEFB3F}
NullAuthPermit = YES
UserName = rpcapd
```

3. Speichern Sie die Konfigurationsdatei (.ini). Stellen Sie sicher, dass Sie die Datei im ASCII-Format speichern, um Fehler zu vermeiden.
4. Starten Sie den Paketweiterleiter neu, indem Sie den folgenden Befehl ausführen:

```
restart-service rpcapd
```

Hinweis: Um die Paketweiterleitungssoftware nach dem Ändern der Konfigurationsdatei erneut zu installieren, führen Sie den Installationsbefehl aus und ersetzen Sie `-RpcapIp` und `-RpcapPort` mit dem `-KeepConfig` Flag , um die geänderte Konfigurationsdatei beizubehalten. Zum Beispiel:

```
.\install-rpcapd.ps1 -MgmtIp <extrahop_ip> -KeepConfig
```

oder

```
.\install-rpcapd.ps1 –InputDir . -KeepConfig
```

Netzwerk-Overlay-Dekapselung aktivieren

Die Netzwerk-Overlay-Kapselung umhüllt Standard-Netzwerkpakete in äußere Protokoll Header für spezielle Funktionen wie intelligentes Routing und Netzwerkmanagement virtueller Maschinen. Die Netzwerk-Overlay-Dekapselung ermöglicht es dem ExtraHop-System, diese äußeren Kapselungsheader zu entfernen und dann die inneren Pakete zu verarbeiten.

Hinweis: Wenn Sie Generic Routing Encapsulation (GRE), Netzwerkvirtualisierung mit Generic Routing Encapsulation (NVGRE), VXLAN und GENEVE-Entkapselung auf Ihrem ExtraHop-System aktivieren, können Sie die Anzahl Ihrer Gerät erhöhen, da virtuelle Geräte im Netzwerk erkannt werden. Die Erkennung dieser virtuellen Geräte kann die Kapazität von Erweiterte Analyse und Standard Analysis beeinträchtigen, und die zusätzliche Verarbeitung von Metriken kann in extremen Fällen zu Leistungseinbußen führen.

MPLS-, TRILL- und Cisco FabricPath-Protokolle werden automatisch vom ExtraHop-System entkapselt.

GRE- oder NVGRE-Dekapselung aktivieren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Netzwerk-Overlay-Dekapselung**.
4. In der Einstellungen Abschnitt, wählen Sie den **Aktiviert** Checkbox neben **NVGRE** oder **GRE**.

   Hinweis: Wenn Sie GRE auswählen, wird NVGRE auch aktiviert, wenn Sie das Kontrollkästchen NVGRE nicht aktivieren.
5. Klicken Sie **Speichern**.
6. Klicken Sie **OK**.

VXLAN-Dekapselung aktivieren

VXLAN ist ein UDP-Tunneling-Protokoll, das für bestimmte Zielports konfiguriert ist. Eine Entkapselung wird nur versucht, wenn der Zielport in einem Paket mit dem oder den UDP-Zielports übereinstimmt, die in den VXLAN-Dekapselungseinstellungen aufgeführt sind.

Informationen zur Konfiguration des ExtraHop-Systems als Endpunkt für VXLAN-gekapselten Datenverkehr finden Sie unter Eine Schnittstelle konfigurieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Netzwerk-Overlay-Dekapselung**.
4. In der Einstellungen Abschnitt, wählen Sie den **Aktiviert** Checkbox neben **VXLAN**.
5. In der **VXLAN UDP-Zielport** Geben Sie in das Feld eine Portnummer ein und klicken Sie auf das grüne Plus (+).

   Standardmäßig Port `4789` wird der Liste der UDP-Zielports hinzugefügt. Sie können bis zu acht Zielports hinzufügen.
6. Klicken Sie **Speichern**.
7. Klicken Sie **OK**.

GENEVE-Entkapselung aktivieren

Informationen zur Konfiguration des ExtraHop-Systems als Endpunkt für Geneve-gekapselten Verkehr finden Sie unter Eine Schnittstelle konfigurieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Erfassen**.
3. Klicken Sie **Netzwerk-Overlay-Dekapselung**.

4. In der Einstellungen Abschnitt, wählen Sie den **Aktiviert** Checkbox neben **GENF**.
   Der Standard-Zielport ist 6081.
5. Klicken Sie **Speichern**.
6. Klicken Sie **OK**.

Analysieren Sie eine Paketerfassungsdatei

Der Offline-Erfassungsmodus ermöglicht es Administratoren, eine mit einer Paketanalyse-Software wie Wireshark oder tcpdump aufgezeichnete Capture-Datei in das ExtraHop-System hochzuladen und zu analysieren.

Hier sind einige wichtige Überlegungen, bevor Sie den Offline-Aufnahmemodus aktivieren:

- Wenn die Erfassung in den Offline-Modus versetzt wird, wird der Systemdatenspeicher zurückgesetzt. Alle zuvor aufgezeichneten Metriken werden aus dem Datenspeicher gelöscht. Wenn das System in den Online-Modus versetzt wird, wird der Datenspeicher erneut zurückgesetzt.
- Im Offline-Modus werden keine Metriken von der Erfassungsoberfläche erfasst, bis das System wieder in den Online-Modus versetzt wird.
- Es werden nur Erfassungsdateien im PCAP-Format unterstützt. Andere Formate wie pcapng werden nicht unterstützt.

Stellen Sie den Offline-Aufnahmemodus ein

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erfassen**.
3. klicken **Offline-Capture-Datei**.
4. Wählen **Upload** und dann klicken **Speichern**.
5. klicken **OK** um das Zurücksetzen des Datenspeichers zu bestätigen.
   Der Erfassungsvorgang wird gestoppt, der Erfassungsstatus wird auf Offline gesetzt und der Datenspeicher wird von allen Daten gelöscht. Wenn das System die Erfassung in den Offline-Modus versetzt hat, Offline-Capture-Datei Seite erscheint.
6. klicken **Wählen Sie Datei**, navigieren Sie zu der Capture-Datei, die Sie hochladen möchten, wählen Sie die Datei aus, und klicken Sie dann auf **Öffnen**.
7. klicken **Upload**.
   Das ExtraHop-System zeigt die Seite mit den Offline-Capture-Ergebnissen an , wenn die Capture-Datei erfolgreich hochgeladen wurde.
8. klicken **Ergebnisse ansehen** um die Paketerfassungsdatei so zu analysieren, als ob sich das System im Live-Capture-Modus befindet.

Bringen Sie das System in den Live-Aufnahmemodus zurück

1. In der Konfiguration des Systems Abschnitt, klicken **Aufnehmen (offline)**.
2. klicken **Capture neu starten**.
3. Wählen **Lebe**, und klicken Sie dann auf **Speichern**.

Das System entfernt die Leistungskennzahlen, die aus der vorherigen Erfassungsdatei gesammelt wurden, und bereitet den Datenspeicher für die Echtzeitanalyse über die Erfassungsoberfläche vor.

Datenspeicher

Das ExtraHop-System umfasst einen eigenständigen Streaming-Datenspeicher zum Speichern und Abrufen von Leistungs- und Integritätskennzahlen in Echtzeit. Dieser lokale Datenspeicher umgeht das Betriebssystem und greift direkt auf die zugrunde liegenden Blockgeräte zu, anstatt eine herkömmliche relationale Datenbank zu verwenden.

Lokale und erweiterte Datenspeicher

Das ExtraHop-System umfasst einen eigenständigen Streaming-Datenspeicher zum Speichern und Abrufen von Leistungs- und Gesundheitsmetriken in Echtzeit. Dieser lokale Datenspeicher umgeht das Betriebssystem und greift direkt auf die zugrunde liegenden Blockgeräte zu, anstatt eine herkömmliche relationale Datenbank zu verwenden.

Der lokale Datenspeicher verwaltet Einträge für alle vom ExtraHop-System erkannten Geräte sowie Metriken für diese Geräte. Durch das Speichern dieser Informationen ist das ExtraHop-System in der Lage, sowohl schnellen Zugriff auf die neueste Netzwerkaufnahme als auch auf historische und trendbasierte Informationen zu ausgewählten Geräten zu ermöglichen.

Erweiterter Datenspeicher

Das ExtraHop-System kann eine Verbindung zu einem externen Speichergerät herstellen, um Ihren Metrik Speicher zu erweitern. Standardmäßig speichert das ExtraHop-System schnelle (30 Sekunden), mittlere (5 Minuten) und langsame (1 Stunde) Messwerte lokal. Sie können jedoch Messwerte für 5 Minuten, 1 Stunde und 24 Stunden in einem erweiterten Datenspeicher speichern.

Um Metriken extern zu speichern, müssen Sie zuerst Mounten Sie einen externen Datenspeicher, und konfigurieren Sie dann das ExtraHop-System so, dass Daten im bereitgestellten Verzeichnis gespeichert werden. Sie können einen externen Datenspeicher über NFS v4 (mit optionaler Kerberos-Authentifizierung) oder SMB (mit optionaler Authentifizierung) mounten.

Beachten Sie, dass Sie jeweils nur einen aktiven erweiterten Datenspeicher konfigurieren können, um alle konfigurierten Metrikzyklen zu erfassen. Wenn Sie Ihren erweiterten Datenspeicher beispielsweise so konfigurieren, dass er 5-Minuten-Metriken, 1-Stunden- und 24-Stunden-Metriken erfasst, werden alle drei Metrikzyklen im gleichen erweiterten Datenspeicher gespeichert. Darüber hinaus können Sie einen erweiterten Datenspeicher archivieren und diese Metriken sind für schreibgeschützte Anfragen von mehreren ExtraHop-Systemen verfügbar.

Hier sind einige wichtige Dinge, die Sie über die Konfiguration eines externen Datenspeichers wissen sollten:

- Wenn ein erweiterter Datenspeicher mehrere Dateien mit überlappenden Zeitstempeln enthält, sind die Metriken falsch.
- Wenn ein erweiterter Datenspeicher Metriken enthält, die von einem ExtraHop-System mit einer neueren Firmware-Version festgeschrieben wurden, kann das System mit der älteren Firmware diese Metriken nicht lesen.
- Wenn ein erweiterter Datenspeicher nicht mehr erreichbar ist, puffert das ExtraHop-System die Metriken, bis der zugewiesene Speicher voll ist. Wenn der Speicher voll ist, überschreibt das System ältere Blöcke, bis die Verbindung wiederhergestellt ist. Wenn der Mount die Verbindung wieder herstellt, werden alle im Speicher gespeicherten Metriken in den Mount geschrieben.
- Wenn eine erweiterte Datenspeicherdatei verloren geht oder beschädigt wird, gehen die in dieser Datei enthaltenen Metriken verloren. Andere Dateien im erweiterten Datenspeicher bleiben intakt.
- Aus Sicherheitsgründen gewährt das System keinen Zugriff auf das gespeicherte Klartextpasswort für den Datenspeicher.

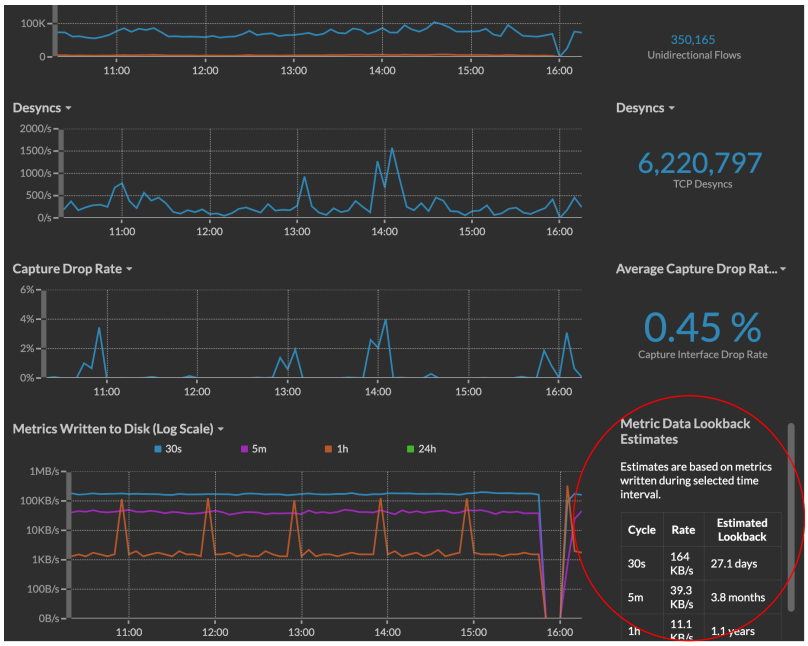
Berechnen Sie die Größe, die für Ihren erweiterten Datenspeicher benötigt wird

Der erweiterte Datenspeicher muss über ausreichend Speicherplatz verfügen, um die vom ExtraHop-System generierte Datenmenge aufzunehmen. Das folgende Verfahren erklärt, wie Sie ungefähr berechnen können, wie viel freien Speicherplatz Sie für Ihren erweiterten Datenspeicher benötigen.

Bevor Sie beginnen
Machen Sie sich mit ExtraHop vertraut Datenspeicher-Konzepte.

Im folgenden Beispiel zeigen wir Ihnen, wie Sie die Menge an Speicherplatz berechnen, die für 5-Minuten-Metriken im Wert von 30 Tagen benötigt wird.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf Systemeinstellungen Symbol, und klicken Sie dann auf **Systemzustand**.
3. Scrollen Sie nach unten zum Datenfeed Abschnitt.
4. In der Lookback-Schätzungen für metrische Daten Diagramm, beachten Sie das Rate und geschätzter Lookback für jeden Metrikzyklus (oder Zeitraum), den Sie im externen Datenspeicher speichern möchten. Schätzungen basieren auf Metriken, die während des ausgewählten Zeitintervalls geschrieben wurden.



5. Berechnen Sie den benötigten Speicherplatz, indem Sie die folgende Formel anwenden: `<rate> x <lookback_time>`, und rechnen Sie den Wert dann in Standardeinheiten um.
   In der Abbildung oben beträgt die Rate für 5-Minuten-Metriken beispielsweise 39,3 KB/s.
   1. Rechnen Sie die Rate von Sekunden nach Tagen um: `39.3 * 60 (seconds) * 60 (minutes) * 24 (hours) * 30 (days) = 101865600 KB` für 30 Tage Rückblick.
   2. Wandle die Rate von Kilobyte nach Megabyte um: `101865600 / 1024 = 99478 MB` für 30 Tage Rückblick.
   3. Rechnen Sie die Rate von Megabyte nach Gigabyte um:`99478 / 1024 = 97 GB` für 30 Tage Rückblick.

   Um alle 5-Minuten-Metriken dieses ExtraHop-Systems 30 Tage lang zu speichern, benötigen Sie 97 GB freien Speicherplatz.

Nächste Schritte
Konfigurieren Sie einen erweiterten SMB- oder NFS-Datenspeicher.

Konfigurieren Sie einen erweiterten SMB- oder NFS-Datenspeicher

Die folgenden Verfahren zeigen Ihnen, wie Sie einen externen Datenspeicher für das ExtraHop-System konfigurieren.

Bevor Sie beginnen
Berechnen Sie die Größe, die für Ihren erweiterten Datenspeicher benötigt wird

Um einen erweiterten Datenspeicher zu konfigurieren, führen Sie die folgenden Schritte aus:

- Zuerst mounten Sie die NFS- oder SMB-Freigabe, auf der Sie Daten speichern möchten.

- Für NFS konfigurieren Sie optional die Kerberos-Authentifizierung, bevor Sie den NFS-Mount hinzufügen.
- Geben Sie abschließend den neu hinzugefügten Mount als aktiven Datenspeicher an.

Fügen Sie einen SMB-Mount hinzu

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken **Erweiterten Datenspeicher konfigurieren**.
4. Klicken Sie **Mount hinzufügen**.
5. Klicken Sie **CIFS-Mount hinzufügen**.
6. Auf dem CIFS-Mount konfigurieren Seite, geben Sie die folgenden Informationen ein:

   Name des Mounts

   Ein Name für die Halterung, z. B. `EXDS_CIFS`.

   Pfad zum Teilen per Fernzugriff

   Der Pfad für die Aktie im folgenden Format:

   ```
   \\host\mountpoint
   ```

   Zum Beispiel:

   ```
   \\herring\extended-datastore
   ```

   SMB-Version

   Die SMB-Version, die mit Ihrem Dateiserver kompatibel ist.

   Domäne

   Die Domain der Standort.
7. Wenn ein Passwortschutz erforderlich ist, gehen Sie wie folgt vor:
   a) Aus dem Authentifizierung Dropdownliste, wählen **Passwort**.
   b) In der Nutzer und Passwort Felder, geben Sie einen gültigen Benutzernamen und ein Passwort ein.
8. Klicken Sie **Speichern**.

(Optional) Kerberos für NFS konfigurieren

Sie müssen jede gewünschte Kerberos-Authentifizierung konfigurieren, bevor Sie einen NFS-Mount hinzufügen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher und Anpassungen**.
3. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
4. Klicken Sie **Kerberos Config hinzufügen**.
5. In der Admin-Server Geben Sie in dieses Feld die IP-Adresse oder den Hostnamen des Kerberos-Masterservers ein, der Tickets ausstellt.
6. In der Hauptverteilungszentrum (KDC) Feld, geben Sie die IP-Adresse oder den Hostnamen des Server ein, der die Schlüssel enthält.
7. In der Reich Feld, geben Sie den Namen des Kerberos-Realms für Ihre Konfiguration ein.
8. In der Domäne In diesem Feld geben Sie den Namen der Kerberos-Domäne für Ihre Konfiguration ein.
9. In der Keytab-Datei Abschnitt, klicken **Wählen Sie Datei**, wählen Sie eine gespeicherte Keytab-Datei aus, und klicken Sie dann auf **Offen**.

10. Klicken Sie **Upload**.

Einen NFS-Mount hinzufügen

Bevor Sie beginnen

- Konfigurieren Sie alle anwendbaren Kerberos-Authentifizierungen, bevor Sie einen NFS-Mount hinzufügen.
- Erlauben Sie entweder allen Benutzern auf dem Share Lese-/Schreibzugriff oder weisen Sie den Benutzer „Extrahop“ als Eigentümer des Shares zu und gewähren Sie Lese-/Schreibzugriff.
- Sie müssen NFS Version 4 haben.

1. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
2. In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken **Erweiterten Datenspeicher konfigurieren**.
3. Klicken Sie **NFSv4-Mount hinzufügen**.
4. Auf dem NFSv4-Mount konfigurieren Seite, vervollständigen Sie die folgenden Informationen:
5. In der Name des Mounts Feld, geben Sie einen Namen für den Mount ein, z. B. `EXDS`.
6. In der Remote-Share-Point Feld, geben Sie den Pfad für den Mount im folgenden Format ein: `host:/mountpoint`, wie `herring:/mnt/extended-datastore`.
7. Aus dem **Authentifizierung** Wählen Sie im Dropdownmenü eine der folgenden Optionen aus:
   - **Keine**, ohne Authentifizierung.
   - **Kerberos**, für krb5-Sicherheit.
   - **Kerberos (sichere Authentifizierung und Datenintegrität)**, für krb5i-Sicherheit.
   - **Kerberos (sichere Authentifizierung, Datenintegrität, Datenschutz)** , für krb5p-Sicherheit.
8. Klicken Sie **Speichern**.

Geben Sie einen Mount als aktiven erweiterten Datenspeicher an

Nachdem Sie einen SMB- oder NFS-Mount hinzugefügt haben, legen Sie den Mount als Ihren aktiven erweiterten Datenspeicher fest. Denken Sie daran, dass jeweils nur ein Datenspeicher Metriken erfassen kann.

Hinweis: Wenn Sie sich dafür entscheiden, 5-Minuten-und 1-Stunden-Metriken im erweiterten Datenspeicher zu speichern, bewirkt diese Option, dass alle 5-Minuten- und 1-Stunden-Metriken, die aus dem lokalen ExtraHop-Systemdatenspeicher erfasst wurden, in den erweiterten Datenspeicher migriert werden. Durch die Migration von 5-Sekunden-Metriken und 1-Stunden-Metriken auf einen erweiterten Datenspeicher bleibt mehr Platz zum Speichern von 30-Sekunden-Metriken im lokalen Datenspeicher, wodurch die Menge an verfügbarem Lookback mit hoher Auflösung erhöht wird.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken **Erweiterten Datenspeicher konfigurieren**.
4. Aus dem Name des Mounts Wählen Sie in der Dropdownliste den Namen des Mounts aus, das Sie als erweiterten Datenspeicher angeben möchten.
5. In der Datenspeicher-Verzeichnis Feld, geben Sie einen Namen für das Datenspeicherverzeichnis ein.
   Das Verzeichnis wird automatisch vom ExtraHop-System auf dem Mount-Point erstellt.
6. Für Konfigurieren als, wählen **Aktiv**.
7. In der Datenspeichergröße (GB) Feld, geben Sie die maximale Datenmenge an, die im Datenspeicher gespeichert werden kann.
8. Wählen Sie die **Fügen Sie 5-Minuten-und 1-Stunden-Metriken hinzu** Kontrollkästchen zum Speichern von 5-Minuten- und 1-Stunden-Metriken im erweiterten Datenspeicher.

24-Stunden-Metriken werden immer im erweiterten Datenspeicher gespeichert.

9. Geben Sie an, ob vorhandene Metriken in den erweiterten Datenspeicher migriert werden sollen, indem Sie eine der folgenden Optionen auswählen:
   - Um bestehende Metriken zu migrieren, wählen Sie **Verschieben Sie vorhandene Metriken in den erweiterten Datenspeicher**.
   - Um vorhandene Metriken im lokalen Datenspeicher beizubehalten, wählen Sie **Bestehende Metriken im ExtraHop beibehalten**.

     Warnung: Während der Datenmigration hört das ExtraHop-System auf, Daten zu sammeln, und die Systemleistung wird beeinträchtigt. Der Migrationsvorgang nimmt unter den folgenden Umständen mehr Zeit in Anspruch:
     - Wenn eine große Datenmenge migriert werden muss
     - Wenn die Netzwerkverbindung zum NAS-Gerät, das den Datenspeicher hostet, langsam ist
     - Wenn die Schreibleistung des NAS-Geräts, das den Datenspeicher hostet, langsam ist
10. Wählen **Verschieben Sie vorhandene Metriken in den erweiterten Datenspeicher**.
11. Für **Wenn der Datenspeicher voll ist**, geben Sie an, was das System tun soll, wenn der Datenspeicher voll wird, indem Sie eine der folgenden Optionen auswählen.
    - Um ältere Daten zu überschreiben, wenn der Datenspeicher voll ist, klicken Sie auf **Überschreiben**.
    - Um das Speichern neuer Metriken im erweiterten Datenspeicher zu beenden, wenn der Datenspeicher voll ist, klicken Sie auf **Hör auf zu schreiben**.
12. Klicken Sie **Konfiguriere**.

Nachdem der Speicher hinzugefügt wurde, wird der Status angezeigt `Nominal`.

Nächste Schritte

- Probleme mit einem erweiterten Datenspeicher beheben
- Archivieren Sie einen erweiterten Datenspeicher für schreibgeschützten Zugriff

Archivieren Sie einen erweiterten Datenspeicher für schreibgeschützten Zugriff

Indem Sie einen aktiven Datenspeicher von einem ExtraHop-System trennen, können Sie ein schreibgeschütztes Archiv der gespeicherten Metrikdaten erstellen. Eine beliebige Anzahl von ExtraHop-Systemen kann aus einem archivierten Datenspeicher lesen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken Sie **Erweiterten Datenspeicher konfigurieren**.
4. Klicken Sie auf den Namen des Mounts, das den Datenspeicher enthält, den Sie archivieren möchten.
5. Klicken Sie in der Zeile dieses Datenspeichers auf **Trennen Sie den erweiterten Datenspeicher**.
6. Typ `JA` zur Bestätigung.
7. Klicken Sie **OK**.

Der Datenspeicher ist vom System getrennt und für den Nur-Lese-Zugriff markiert. Warten Sie mindestens zehn Minuten, bevor Sie andere ExtraHop-Systeme mit dem Archiv verbinden.

Verbinden Sie Ihr ExtraHop-System mit dem archivierten Datenspeicher

Warnung: Um eine Verbindung zu einem archivierten Datenspeicher herzustellen, muss das ExtraHop-System die im Datenspeicher enthaltenen Daten durchsuchen. Abhängig von der Menge der im archivierten Datenspeicher gespeicherten Daten kann das Herstellen

einer Verbindung zum archivierten Datenspeicher lange dauern. Wenn eine Verbindung zum archivierten Datenspeicher hergestellt wird, erfasst das System keine Daten und die Systemleistung wird beeinträchtigt. Der Verbindungsvorgang dauert unter den folgenden Umständen länger:

- Wenn der Datenspeicher eine große Datenmenge enthält
- Wenn die Netzwerkverbindung zum NAS-Gerät, das den Datenspeicher hostet, langsam ist
- Wenn die Leseleistung des NAS-Geräts, das den Datenspeicher hostet, langsam ist

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken Sie **Erweiterten Datenspeicher konfigurieren**.
4. Klicken Sie auf den Namen des Mounts, das den archivierten Datenspeicher enthält.
5. In der Datenspeicher-Verzeichnis Feld, geben Sie den Pfad des archivierten Datenspeicherverzeichnisses ein.
6. Klicken Sie **Archivieren (Nur lesen)**.
7. Klicken Sie **Konfiguriere**.

Ihre erweiterte Datenbank ist jetzt ein schreibgeschütztes Archiv, auf das mehrere ExtraHop-Systeme zugreifen können.

Metriken aus einem erweiterten Datenspeicher importieren

Wenn Sie Metrikdaten in einem erweiterten Datenspeicher gespeichert haben, der mit Ihrem ExtraHop-System verbunden ist, können Sie diese Daten während eines Upgrades oder eines Datenspeicher-Resets verschieben.

Kontakt ExtraHop-Unterstützung wenn Sie Metriken aus einem erweiterten Datenspeicher übertragen müssen.

Setzen Sie den lokalen Datenspeicher zurück und entfernen Sie alle Geräte-Metriken aus dem ExtraHop-System

Unter bestimmten Umständen, z. B. beim Umzug eines Sensor Von einem Netzwerk zum anderen müssen Sie möglicherweise die Metriken in den lokalen und erweiterten Datenspeichern löschen. Durch das Zurücksetzen des lokalen Datenspeichers werden alle Metriken, Baselines, Trendanalysen und erkannten Geräte entfernt — und dies wirkt sich auf alle Anpassungen an Ihrem ExtraHop-System aus.

Warnung: Dieses Verfahren löscht Geräte-IDs und Geräte-Metriken aus dem ExtraHop-System.

Hier sind einige wichtige Überlegungen zum Zurücksetzen des lokalen Datenspeichers:

- Machen Sie sich mit ExtraHop vertraut Datenbankkonzepte.
- Anpassungen sind Änderungen, die an den Standardeinstellungen im System vorgenommen wurden, z. B. an Triggern, Dashboards, Warnungen und benutzerdefinierten Messwerten. Diese Einstellungen werden in einer Datei auf dem System gespeichert, und diese Datei wird auch gelöscht, wenn der Datenspeicher zurückgesetzt wird.
- Das Reset-Verfahren beinhaltet eine Option zum Speichern und Wiederherstellen Ihrer Anpassungen.
- Die meisten Anpassungen werden auf Geräte angewendet, die durch eine ID auf dem System identifiziert werden. Wenn der lokale Datenspeicher zurückgesetzt wird, können sich diese IDs ändern und alle gerätebasierten Zuweisungen müssen den Geräten mit ihren neuen IDs neu zugewiesen werden.
- Wenn Ihre Geräte-IDs im erweiterten Datenspeicher gespeichert sind und dieser Datenspeicher getrennt wird, wenn der lokale Datenspeicher zurückgesetzt und später wieder verbunden

wird, werden diese Geräte-IDs im lokalen Datenspeicher wiederhergestellt, und Sie müssen Ihre wiederhergestellten Anpassungen nicht erneut zuweisen.
- Das Reset-Verfahren bewahrt historische Daten zur Geräteanzahl auf, um die Genauigkeit der Metriken in der Anzahl und Limit der aktiven Geräte Diagramm.
- Konfigurierte Warnungen werden im System beibehalten, sind jedoch deaktiviert und müssen aktiviert und erneut auf das richtige Netzwerk, Gerät oder die richtige Gerätegruppe angewendet werden. Systemeinstellungen und Benutzerkonten sind nicht betroffen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. Trennen Sie Ihren erweiterten Datenspeicher, indem Sie die folgenden Schritte ausführen:
   a) In der Erweiterte Datenspeicher-Einstellungen Abschnitt, klicken **Erweiterten Datenspeicher konfigurieren**.
   b) Klicken Sie auf den Namen des Mounts, das den Datenspeicher enthält, den Sie trennen möchten .
   c) Klicken Sie in der Zeile dieses Datenspeichers auf **Trennen Sie den erweiterten Datenspeicher**.
   d) Typ `JA` zur Bestätigung.
   e) Klicken Sie **OK**.
4. Navigiere zurück zum Datenspeicher und Anpassungen Seite.
5. In der Lokale Datenspeichereinstellungen Abschnitt, klicken **Datenspeicher zurücksetzen**.
6. Auf dem Datenspeicher zurücksetzen Seite, geben Sie an, ob Anpassungen gespeichert werden sollen, bevor Sie den Datenspeicher zurücksetzen.
   - Um die aktuellen Anpassungen nach dem Zurücksetzen des Datenspeichers beizubehalten, wählen Sie das **Anpassungen speichern** Ankreuzfeld.
   - Um die aktuellen Anpassungen nach dem Zurücksetzen des Datenspeichers zu löschen, löschen Sie das **Anpassungen speichern** Ankreuzfeld.
7. Typ `JA` im Bestätigungstextfeld.
8. Klicken Sie **Datenspeicher zurücksetzen**.
   Wenn Sie sich dafür entschieden haben, Ihre Anpassungen zu speichern, wird nach etwa einer Minute eine Aufforderung mit einer detaillierten Liste angezeigt. Klicken Sie **OK** um die gespeicherten Anpassungen wiederherzustellen.

Probleme mit dem erweiterten Datenspeicher beheben

Gehen Sie wie folgt vor, um den Status Ihrer Mounts und Datenspeicher einzusehen und die entsprechenden Schritte zur Problembehandlung zu ermitteln.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenspeicher**.
3. In der Erweiterte Datenspeichereinstellungen Abschnitt, klicken **Erweiterten Datenspeicher konfigurieren**.
4. In der Erweiterte Datenspeicher Tabelle, zeigen Sie den Eintrag in der Status-Spalte für jeden Mount oder Datenspeicher an.

Die folgenden Tabellen enthalten Anleitungen zu den einzelnen Einträgen und identifizieren alle anwendbaren Maßnahmen.

Tabelle 1: Halterungen

Status	Beschreibung	Aktion des Benutzers
Montiert	Die Mount-Konfiguration war erfolgreich.	Keine erforderlich

Status	Beschreibung	Aktion des Benutzers
NICHT MONTIERT	Die Mount-Konfiguration war nicht erfolgreich.	• Stellen Sie sicher, dass die Informationen zur Mount-Konfiguration korrekt sind und die Schreibweise korrekt ist. • Stellen Sie sicher, dass das Remotesystem verfügbar ist. • Stellen Sie sicher, dass der Server ein unterstützter Typ und eine unterstützte Version ist. • Überprüfen Sie die Anmeldedaten, wenn Sie eine Authentifizierung verwenden.
NICHT LESBAR	Der Mount hat Berechtigungen oder Netzwerkprobleme, die das Lesen verhindern.	• Stellen Sie sicher, dass die richtigen Berechtigungen für das Share festgelegt sind. • Überprüfen Sie die Netzwerkverbindung und Verfügbarkeit.
KEIN PLATZ VERFÜGBAR	Auf der Halterung ist kein Platz mehr vorhanden.	Nehmen Sie die Halterung ab und erstellen Sie eine neue.
UNZUREICHENDER SPEICHERPLATZ	• Erster Eindruck: Das System geht davon aus, dass nicht genügend Speicherplatz verfügbar ist. • Zweiter Auftritt: Weniger als 128 MB Speicherplatz sind verfügbar.	Nehmen Sie die Halterung ab und erstellen Sie eine neue.
WARNUNG VOR VERFÜGBAREM SPEICHERPLATZ	Weniger als 1 GB Speicherplatz ist verfügbar.	Nehmen Sie die Halterung ab und erstellen Sie eine neue.
NICHT BESCHREIBBAR	Der Mount hat Berechtigungen oder Netzwerkprobleme, die das Schreiben verhindern.	• Überprüfen Sie die Berechtigungen. • Überprüfen Sie die Netzwerkverbindung und Verfügbarkeit.

Tabelle 2: Datenspeicher

Status	Beschreibung	Aktion des Benutzers
Nennwert	Der Datenspeicher befindet sich in einem normalen Zustand.	Keine erforderlich
UNZUREICHENDER SPEICHERPLATZ auf: <MOUNT NAME>	Der Datenspeicher hat auf dem benannten Mount nicht genügend Speicherplatz und es kann nicht darauf geschrieben werden.	Erstellen Sie einen neuen Datenspeicher. Erwägen Sie für den neuen Datenspeicher die

Status	Beschreibung	Aktion des Benutzers
		Auswahl der `Overwrite` Option, falls zutreffend.
NICHT LESBAR	Der Datenspeicher hat Berechtigungen oder Netzwerkprobleme, die das Lesen verhindern.	• Überprüfen Sie die Berechtigungen. • Überprüfen Sie die Netzwerkverbindung und Verfügbarkeit.
NICHT BESCHREIBBAR	Der Datenspeicher hat Berechtigungen oder Netzwerkprobleme, die das Schreiben verhindern.	• Überprüfen Sie die Berechtigungen. • Überprüfen Sie die Netzwerkverbindung und Verfügbarkeit.

Vorrang des Gerätenamens

Entdeckte Geräte werden automatisch anhand mehrerer Netzwerkdatenquellen benannt. Wenn mehrere Namen für ein Gerät gefunden werden, wird eine Standardprioritätsreihenfolge angewendet. Sie können die Rangfolge ändern.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Die gesamte Verwaltung**.
3. In der Konfiguration des Systems Abschnitt, klicken Sie **Rangfolge des Gerätenamens**.
4. Klicken und ziehen Sie die Gerätenamen, um eine neue Rangfolge zu erstellen.
5. Klicken Sie **Speichern**.
6. Optional: Klicken Sie **Zur Standardeinstellung zurückkehren** um Ihre Änderungen rückgängig zu machen.

Inaktive Quellen

Geräte und Anwendungen werden in den Suchergebnissen angezeigt, bis sie länger als 90 Tage inaktiv sind. Wenn Sie Quellen vor Ablauf der 90 Tage aus den Suchergebnissen entfernen möchten, können Sie bei Bedarf alle Quellen entfernen, die zwischen 1 und 90 Tagen inaktiv waren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Geben Sie in das Feld Inaktive Tage einen Wert zwischen 1 und 90 ein.
3. Klicken Sie **entfernen**.

Erkennungsverfolgung aktivieren

Mit der Erkennungsverfolgung können Sie einem Benutzer eine Erkennung zuweisen, den Status festlegen und Notizen hinzufügen. Sie können Erkennungen direkt im ExtraHop-System, mit einem externen Ticketsystem eines Drittanbieters oder mit beiden Methoden verfolgen.

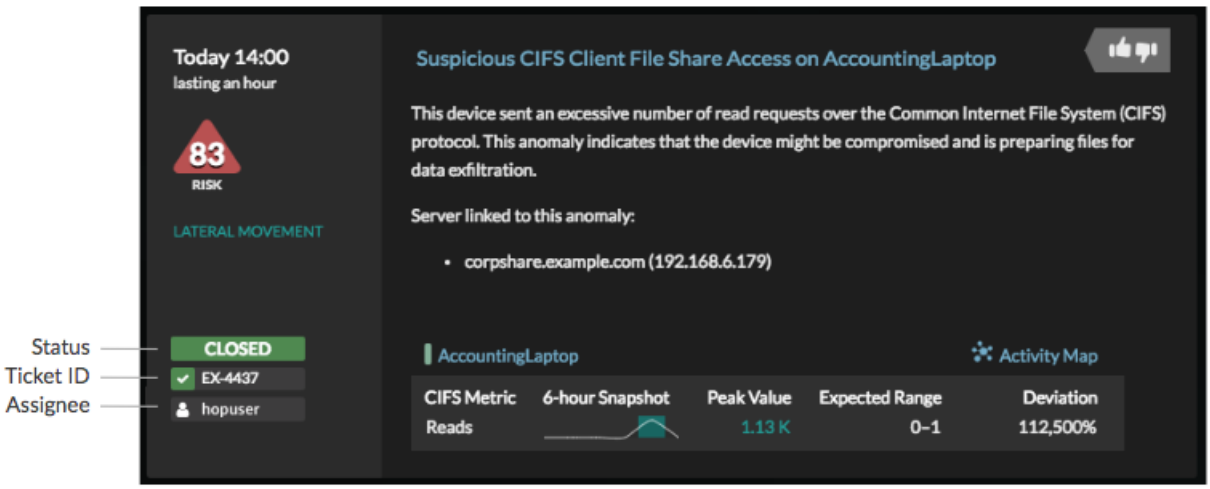
Hinweis: Sie müssen die Ticketverfolgung auf allen angeschlossenen Sensoren aktivieren.

Bevor Sie beginnen

- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das Administratorrechte.
- Nachdem Sie die externe Ticketverfolgung aktiviert haben, müssen Sie Ticket-Tracking von Drittanbietern konfigurieren indem Sie einen Auslöser schreiben, um Tickets in Ihrem Ticketsystem zu erstellen und zu aktualisieren, und dann Ticketaktualisierungen auf Ihrem ExtraHop-System über die REST-API aktivieren.
- Wenn Sie das externe Ticket-Tracking deaktivieren, werden zuvor gespeicherte Status- und Empfänger-Ticketinformationen in das ExtraHop-Erkennungs-Tracking umgewandelt. Wenn das Erkennungs-Tracking innerhalb des ExtraHop-Systems aktiviert ist, können Sie Tickets einsehen, die bereits existierten, als Sie das externe Ticket-Tracking deaktiviert haben, aber Änderungen an diesem externen Ticket werden nicht im ExtraHop-System angezeigt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Erkennungsverfolgung**.
3. Wählen Sie eine oder beide der folgenden Methoden für die Nachverfolgung von Erkennungen aus:
   - Wählen **Ermöglichen Sie ExtraHop-Benutzern, Erkennungen aus dem ExtraHop-System heraus zu verfolgen**.
   - Wählen **Ermöglichen Sie externe Integrationen wie SOAR oder Ticket-Tracking-Systeme, um Erkennungen über die ExtraHop Rest API zu verfolgen** .
4. Optional: Nachdem Sie die Option zum Aktivieren externer Integrationen ausgewählt haben, geben Sie die URL-Vorlage für Ihr Ticketsystem an und fügen Sie die *$ Ticket_ID* variabel an der entsprechenden Stelle. Geben Sie beispielsweise eine vollständige URL ein, z. B. `https://jira.example.com/browse/$ticket_id`. Das *$ Ticket_ID* Die Variable wird durch die Ticket-ID ersetzt, die der Erkennung zugeordnet ist.

   Nachdem die URL-Vorlage konfiguriert ist, können Sie in einer Erkennung auf die Ticket-ID klicken, um das Ticket in einem neuen Browser-Tab zu öffnen.



Nächste Schritte
Wenn Sie externe Ticket-Tracking-Integrationen aktiviert haben, müssen Sie mit der folgenden Aufgabe fortfahren:

- Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Ticket-Tracking von Drittanbietern für Erkennungen konfigurieren

Mit der Ticketverfolgung können Sie Tickets, Alarme oder Fälle in Ihrem Work-Tracking-System mit ExtraHop-Erkennungen verknüpfen. Jedes Ticketsystem von Drittanbietern, das Open Data Stream (ODS) - Anfragen annehmen kann, wie Jira oder Salesforce, kann mit ExtraHop-Erkennungen verknüpft werden.

Bevor Sie beginnen

- Das musst du haben hat in den Verwaltungseinstellungen die Option zum Nachverfolgen der Erkennung durch Dritte ausgewählt.
- Sie müssen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto haben, das System- und Zugriffsadministrationsrechte.
- Sie müssen mit dem Schreiben von ExtraHop-Triggern vertraut sein. siehe Trigger und die Verfahren in Einen Auslöser erstellen.
- Sie müssen ein ODS-Ziel für Ihren Ticket-Tracking-Server erstellen. Weitere Informationen zur Konfiguration von ODS-Zielen finden Sie in den folgenden Themen : HTTP, Kafka, MongoDB, Syslog, oder Rohdaten.
- Sie müssen mit dem Schreiben von REST-API-Skripten vertraut sein und über einen gültigen API-Schlüssel verfügen, um die folgenden Verfahren ausführen zu können. siehe Generieren Sie einen API-Schlüssel.

Schreiben Sie einen Auslöser, um Tickets zu Erkennungen in Ihrem Ticketsystem zu erstellen und zu aktualisieren
Dieses Beispiel zeigt Ihnen, wie Sie einen Auslöser erstellen, der die folgenden Aktionen ausführt:

- Erstellen Sie jedes Mal, wenn eine neue Erkennung im ExtraHop-System erscheint, ein neues Ticket im Ticketsystem.
- Weisen Sie einem Benutzer mit dem Namen neue Tickets zu `escalations_team` im Ticketsystem.
- Wird jedes Mal ausgeführt, wenn eine Erkennung auf dem ExtraHop-System aktualisiert wird.
- Senden Sie Erkennungsaktualisierungen über einen HTTP Open Data Stream (ODS) an das Ticketsystem.

Das vollständige Beispielskript ist am Ende dieses Themas verfügbar.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf das Symbol Systemeinstellungen und dann klicken **Auslöser**.
3. klicken **Neu**.
4. Geben Sie einen Namen und eine optionale Beschreibung für den Auslöser an.
5. Wählen Sie in der Liste Ereignisse **ERKENNUNGSUPDATE**.

   Das Ereignis DETECTION_UPDATE wird jedes Mal ausgeführt, wenn eine Erkennung im ExtraHop-System erstellt oder aktualisiert wird.
6. Geben Sie im rechten Bereich Folgendes an Erkennungsklasse Parameter in einem JavaScript-Objekt. Diese Parameter bestimmen die Informationen, die an Ihr Ticketsystem gesendet werden.

   Der folgende Beispielcode fügt die Erkennungs-ID, die Beschreibung, den Titel, die Kategorien, die MITRE-Techniken und -Taktiken sowie die Risikoscore zu einem JavaScript-Objekt mit dem Namen hinzu `payload`:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
```

```
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};
```

7. Definieren Sie als Nächstes die HTTP-Anforderungsparameter in einem JavaScript-Objekt unter dem vorherigen JavaScript-Objekt.

   Der folgende Beispielcode definiert eine HTTP-Anfrage für die im vorherigen Beispiel beschriebene Nutzlast: definiert eine Anfrage mit einer JSON-Payload:

   ```
   const req = {
       'path': '/rest/api/issue',
       'headers': {
           'Content-Type': 'application/json'
       },
       'payload': JSON.stringify(payload)
   };
   ```

   Weitere Hinweise zu ODS-Anforderungsobjekten finden Sie unter Offene Datenstromklassen.

8. Geben Sie abschließend die HTTP-POST-Anfrage an, die die Informationen an das ODS-Ziel sendet. Der folgende Beispielcode sendet die im vorherigen Beispiel beschriebene HTTP-Anfrage an ein ODS-Ziel namens Ticket-Server:

   ```
   Remote.HTTP('ticket-server').post(req);
   ```

Der vollständige Triggercode sollte dem folgenden Beispiel ähneln:

```
const summary = "ExtraHop Detection: " + Detection.id + ": " +
 Detection.title;
const description = "ExtraHop has detected the following event on your
 network: " + Detection.description
const payload = {
    "fields": {
        "summary": summary,
        "assignee": {
            "name": "escalations_team"
        },
        "reporter": {
            "name": "ExtraHop"
        },
        "priority": {
            "id": Detection.riskScore
        },
        "labels": Detection.categories,
        "mitreCategories": Detection.mitreCategories,
        "description": description
    }
};

const req = {
    'path': '/rest/api/issue',
    'headers': {
        'Content-Type': 'application/json'
    },
    'payload': JSON.stringify(payload)
};

Remote.HTTP('ticket-server').post(req);
```

Ticketinformationen über die REST-API an Erkennungen senden
Nachdem Sie einen Auslöser konfiguriert haben, um Tickets für Erkennungen in Ihrem Ticket-Tracking-System zu erstellen, können Sie die Ticketinformationen in Ihrem ExtraHop-System über die REST-API aktualisieren.

Ticketinformationen werden bei Erkennungen auf der Seite „Entdeckungen“ im ExtraHop-System angezeigt. Weitere Informationen finden Sie in der Erkennungen Thema.

Das folgende Python-Beispielskript entnimmt Ticketinformationen aus einem Python-Array und aktualisiert die zugehörigen Erkennungen auf dem ExtraHop-System.

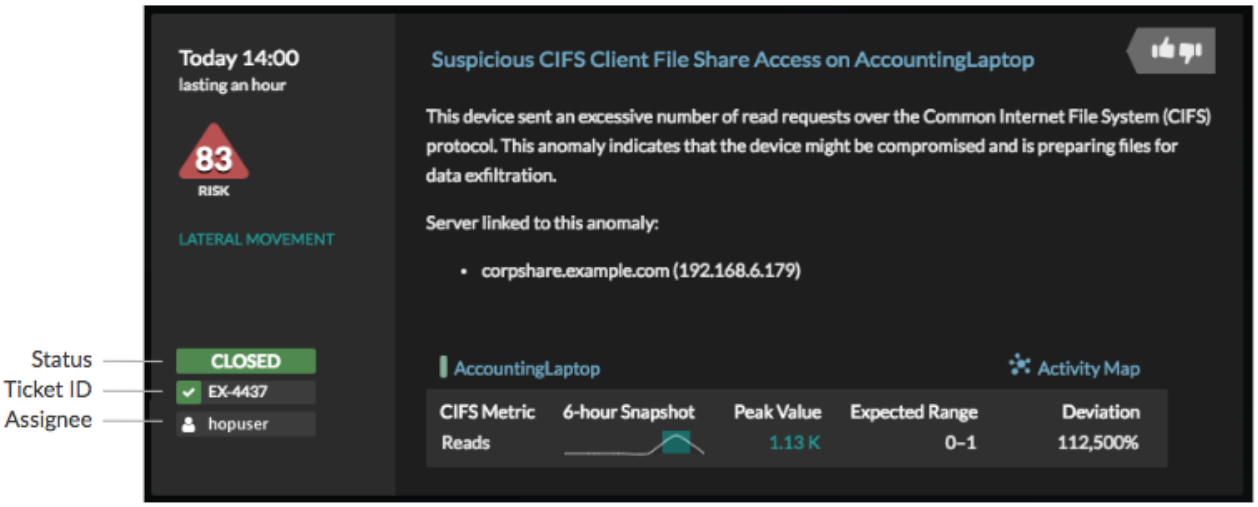
```
#!/usr/bin/python3

import json
import requests
import csv

API_KEY = '123456789abcdefghijklmnop'
HOST = 'https://extrahop.example.com/'

# Method that updates detections on an ExtraHop system
def updateDetection(detection):
    url = HOST + 'api/v1/detections/' + detection['detection_id']
    del detection['detection_id']
    data = json.dumps(detection)
    headers = {'Content-Type': 'application/json',
               'Accept': 'application/json',
               'Authorization': 'ExtraHop apikey=%s' % API_KEY}
    r = requests.patch(url, data=data, headers=headers)
    print(r.status_code)
    print(r.text)

# Array of detection information
detections = [
                {
                    "detection_id": "1",
                    "ticket_id": "TK-16982",
                    "status": "new",
                    "assignee": "sally",
                    "resolution": None,
                },
                {
                    "detection_id": "2",
                    "ticket_id": "TK-2078",
                    "status": None,
                    "assignee": "jim",
                    "resolution": None,
                },
                {
                    "detection_id": "3",
                    "ticket_id": "TK-3452",
                    "status": None,
                    "assignee": "alex",
                    "resolution": None,
                }
            ]

for detection in detections:
    updateDetection(detection)
```

Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die TLS-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdiges Zertifikat hinzugefügt. Alternativ können Sie das hinzufügen

`verify=False` Option zur Umgehung der Zertifikatsüberprüfung. Diese Methode ist jedoch nicht sicher und wird nicht empfohlen. Der folgende Code sendet eine HTTP GET-Anfrage ohne Zertifikatsüberprüfung:

```
requests.get(url, headers=headers, verify=False)
```

Nachdem die Ticketverfolgung konfiguriert wurde, werden Ticketdetails im linken Bereich der Erkennungsdetails angezeigt, ähnlich der folgenden Abbildung:



Status

Der Status des Tickets, das mit der Erkennung verknüpft ist. Das Ticket-Tracking unterstützt die folgenden Status:

- Neu
- Im Gange
- geschlossen
- Mit ergriffenen Maßnahmen geschlossen
- Geschlossen, ohne dass Maßnahmen ergriffen wurden

Ticket-ID

Die ID des Tickets in Ihrem Work-Tracking-System, das mit der Erkennung verknüpft ist. Wenn Sie eine Vorlagen-URL konfiguriert haben, können Sie auf die Ticket-ID klicken, um das Ticket in Ihrem Work-Tracking-System zu öffnen.

Abtretungsempfänger

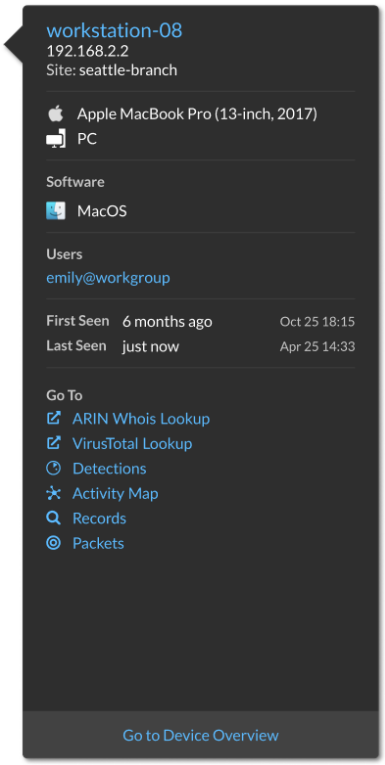
Der Benutzername, der dem Ticket zugewiesen wurde, das mit der Erkennung verknüpft ist. Graue Benutzernamen weisen auf ein Konto hin, das kein ExtraHop-Konto ist.

Endpunkt-Suchlinks konfigurieren

Mit der Endpunktsuche können Sie Tools für externe IP-Adressen angeben, die zum Abrufen von Informationen über Endpunkte innerhalb des ExtraHop-Systems verfügbar sind. Wenn Sie beispielsweise auf eine IP-Adresse klicken oder den Mauszeiger darüber bewegen, werden Links zum Suchtool angezeigt, sodass Sie leicht Informationen zu diesem Endpunkt finden können.

Die folgenden Suchlinks sind standardmäßig konfiguriert und können geändert oder gelöscht werden:

- ARIN Whois-Suche
- VirusTotal-Suche



1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Aus dem Konfiguration des Systems Abschnitt, klicken Sie **Endpunktsuche**.
3. In der **URL-Vorlage** Feld, geben Sie die URL des Suchtools ein.

   Die URL muss enthalten `$ip` Variable, die bei der Suche durch die IP-Adresse des Endpunkt ersetzt wird. Zum Beispiel `https://search.arin.net/rdap/?query=$ip`
4. In der **Name anzeigen** Feld, geben Sie den Namen Link so ein, wie er angezeigt werden soll.
5. Wählen Sie eine der folgenden Optionen Optionen anzeigen:
   - Diesen Link auf allen Endpunkten anzeigen
   - Diesen Link auf externen Endpunkten anzeigen
   - Diesen Link auf internen Endpunkten anzeigen
   - Diesen Link nicht anzeigen
6. Klicken Sie auf Speichern.

Geomap-Datenquelle

Im Produkt zugeordnete geografische Standorte und Trigger verweisen auf eine GeoIP-Datenbank, um den ungefähren Standort einer IP-Adresse zu ermitteln.

Ändern Sie die GeoIP-Datenbank

Sie können Ihre eigene GeoIP-Datenbank in das ExtraHop-System hochladen, um sicherzustellen, dass Sie über die neueste Version der Datenbank verfügen oder ob Ihre Datenbank interne IP-Adressen enthält, deren Standort nur Sie oder Ihr Unternehmen kennen.

Sie können eine Datenbankdatei im MaxMind-DB-Format (.mmdb) hochladen, die Details auf Stadt- und Länderebene enthält .

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Geomap-Datenquelle**.
3. Klicken Sie **GeoIP-Datenbank**.
4. In der Datenbank auf Stadtebene Abschnitt, auswählen **Neue Datenbank hochladen**.
5. Klicken Sie **Wählen Sie Datei** und navigieren Sie zur neuen Datenbankdatei auf Stadtebene auf Ihrem Computer.
6. Klicken Sie **Speichern**.

Einen IP-Standort überschreiben

Sie können fehlende oder falsche IP-Adressen in der GeoIP-Datenbank überschreiben. Sie können eine durch Kommas getrennte Liste oder eine Liste mit Tabulatoren von Überschreibungen in das Textfeld eingeben.

Jede Überschreibung muss einen Eintrag in den folgenden sieben Spalten enthalten:

- IP-Adresse (eine einzelne IP-Adresse oder CIDR-Notation)
- Breitengrad
- Längengrad
- Stadt
- Bundesland oder Region
- Name des Landes
- ISO-Alpha-2-Ländercode

Sie können Elemente nach Bedarf bearbeiten und löschen, müssen jedoch sicherstellen, dass für jede der sieben Spalten Daten vorhanden sind. Weitere Informationen zu ISO-Ländercodes finden Sie unter https://www.iso.org/obp/ui/#search und klicken Sie **Ländercodes**.

1. Unter Konfiguration des Systems, klicken **Geomap-Datenquelle** .
2. klicken **IP-Standort überschreiben**.
3. Geben Sie in das Textfeld eine tabulatorgetrennte oder kommagetrennte Liste von Überschreibungen im folgenden Format ein oder fügen Sie sie ein:

```
IP address, latitude, longitude, city, state or region, country name, ISO alpha-2 country code
```

Zum Beispiel:

```
10.10.113.0/24, 38.907231, -77.036464, Washington, DC, United States, US
10.10.225.25, 47.6204, -122.3491, Seattle, WA, United States, US
```

4. Klicken Sie **Speichern**.

Offene Datenströme

Durch die Konfiguration eines offenen Datenstroms können Sie die von Ihrem ExtraHop-System gesammelten Daten an ein externes Drittanbietersystem wie Syslog-Systeme, MongoDB-Datenbanken, HTTP-Server und Kafka-Server senden. Darüber hinaus können Sie Rohdaten an jeden externen Server senden, indem Sie das Ziel mit Port- und Protokollspezifikationen konfigurieren.

Sie können bis zu 16 offene Datenstromziele für jeden externen Systemtyp konfigurieren.

Wichtig: Nachdem Sie einen Open Data Stream (ODS) für ein externes System konfiguriert haben, müssen Sie einen Auslöser erstellen, der angibt, welche Daten über den Stream verwaltet werden sollen.

Ebenso sollten Sie beim Löschen eines offenen Datenstroms auch den zugehörigen Auslöser löschen, um zu vermeiden, dass Systemressourcen unnötig beansprucht werden.

Weitere Informationen finden Sie unter Offene Datenstromklassen in der ExtraHop Trigger API-Referenz.

Konfigurieren Sie ein HTTP-Ziel für einen offenen Datenstrom

Sie können Daten auf einem ExtraHop-System zur Langzeitarchivierung und zum Vergleich mit anderen Quellen auf einen Remote-HTTP-Server exportieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Datenströme öffnen**.
3. Klicken Sie **Ziel hinzufügen**.
4. Aus dem Zieltyp Dropdownliste, wählen **HTTP**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Remote-HTTP-Servers ein.
7. In der Hafen Feld, geben Sie die Portnummer des Remote-HTTP-Servers ein.
8. Aus dem Typ Wählen Sie in der Dropdownliste eines der folgenden Protokolle aus:
   - **HTTP**
   - **HTTPS**
9. Wenn Sie HTTPS ausgewählt haben, wählen Sie **Zertifikatsüberprüfung überspringen** um die Zertifikatsüberprüfung verschlüsselter Daten zu umgehen. Daten können durch vertrauenswürdige Zertifikate verifiziert werden, die Sie in das ExtraHop-System hochladen.

   Hinweis Sichere Verbindungen zum HTTPS-ODS-Server können überprüft werden über vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.
10. Wählen Sie **Mehrere Verbindungen** um gleichzeitige Anfragen über mehrere Verbindungen zu ermöglichen, was die Durchsatzgeschwindigkeit verbessern kann.
11. In der Zusätzlicher HTTP-Header Feld, geben Sie einen zusätzlichen HTTP-Header ein.

    Das Format für den zusätzlichen Header ist *Kopfzeile* : *Wert*.

    Hinweis In einem Auslöser konfigurierte Header haben Vorrang vor einem zusätzlichen Header. Zum Beispiel, wenn die Zusätzlicher HTTP-Header Feld spezifiziert `Inhaltstyp: Text/Einfach` aber ein Trigger-Skript für dasselbe ODS-Ziel spezifiziert `Inhaltstyp: Anwendung/json` , dann `Inhaltstyp: Anwendung/json` ist in der HTTP-Anfrage enthalten.
12. Optional: Aus dem Authentifizierung Wählen Sie in der Dropdownliste die Art der Authentifizierung aus den folgenden Optionen aus.

Option	Beschreibung
Grundlegend	Authentifiziert sich über einen Benutzernamen und ein Passwort.
Amazon AWS	Authentifiziert sich über Amazon Web Services.
Microsoft Azure-Speicher	Authentifiziert sich über Microsoft Azure.
Microsoft Entra ID	Authentifiziert sich über Microsoft Entra ID (v1.0). **Hinweis** Die Microsoft Identity Platform (v2.0) wird nicht unterstützt.
Crowdstrike	Authentifiziert sich über CrowdStrike.

13. Wählen Sie **Verbindung über globalen Proxy herstellen** um Anfragen über das zu senden globaler Proxyserver konfiguriert für das ExtraHop-System.
14. Optional: Klicken Sie **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-HTTP-Server herzustellen und eine Testnachricht an den Server zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.
15. Optional: Senden Sie eine Testanfrage an den Remote-HTTP-Server.

    Die Anfrage dient nur zu Testzwecken; sie ist in keinem Triggerskript enthalten.

    a) Aus dem Methode Wählen Sie in der Dropdownliste eine der folgenden HTTP-Anforderungsmethoden aus:

    - **LÖSCHEN**
    - **BEKOMMEN**
    - **KOPF**
    - **OPTIONEN**
    - **SETZEN**
    - **BEITRAG**
    - **SPUR**

    b) In der Optionen Feld, geben Sie die Parameter der HTTP-Anfrage im folgenden Format an:

```
    "headers": {},
    "payload": "",
    "path": "/"
}
```

    Die Parameter sind wie folgt definiert:

    Kopfzeilen

    Die Header der HTTP-Anfrage. Sie müssen Header als Array angeben, auch wenn Sie nur einen Header angeben. Zum Beispiel:

```
"headers": {"content-type":["application/json"]},
```

    Pfad

    Der Pfad, auf den die HTTP-Anfrage angewendet wird.

    Nutzlast

    Die Nutzlast der HTTP-Anfrage.

    c) klicken **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Server herzustellen und die Anfrage zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Anfrage erfolgreich war oder fehlgeschlagen ist, und zeigt alle angeforderten Inhalte an.
16. Klicken Sie **Speichern**.

Nächste Schritte
Erstellen Sie einen Auslöser, der angibt, welche HTTP-Nachrichtendaten gesendet werden sollen, und der die Übertragung der Daten an das Ziel initiiert. Weitere Informationen finden Sie in der Remote.HTTP Klasse in der ExtraHop Trigger API-Referenz.

Konfigurieren Sie ein Kafka-Ziel für einen offenen Datenstrom

Sie können Daten auf einem ExtraHop-System auf jeden Kafka-Server exportieren, um sie langfristig zu archivieren und mit anderen Quellen zu vergleichen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenströme öffnen**.
3. Klicken Sie **Ziel hinzufügen**.
4. Aus dem Typ des Ziels Dropdownliste, wählen **Kafka**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. Aus dem Kompression Wählen Sie in der Dropdownliste eine der folgenden Komprimierungsmethoden aus, die auf die übertragenen Daten angewendet werden sollen:
   - **Keine**
   - **GZIP**
   - **Bissig**
7. Aus dem Partitionsstrategie Wählen Sie in der Dropdownliste eine der folgenden Partitionierungsmethoden aus, die auf die übertragenen Daten angewendet werden:
   - **Standard (Hash-Schlüssel)**
   - **Manuell**
   - **Zufällig**
   - **Round Robin**
8. Optional: Konfigurieren Sie die SASL/SCRAM-Authentifizierung.
   a) Aus dem Authentifizierung Dropdownliste, wählen **SASL/SCRAM**.
   b) In der Nutzername Feld, geben Sie den Namen des SASL/SCRAM-Benutzers ein.
   c) In der Passwort Feld, geben Sie das Passwort des SASL/SCRAM-Benutzers ein.
   d) Aus dem **Hashing-Algorithmus** Wählen Sie in der Dropdownliste den Hashing-Algorithmus für die SASL-Authentifizierung aus.
9. Aus dem **Protokoll** Wählen Sie in der Dropdownliste eines der folgenden Protokolle aus, über das Daten übertragen werden sollen:
   - **TCP**
   - **TLS**
10. Optional: Wenn Sie das ausgewählt haben **TLS** Protokoll, geben Sie die Zertifikatsoptionen an.
    a) Wenn der Kafka-Server eine Client-Authentifizierung erfordert, finden Sie in der **Client-Zertifikat** Feld, geben Sie ein TLS-Client-Zertifikat an, das an den Server gesendet werden soll.
    b) Wenn Sie ein Client-Zertifikat angegeben haben, in **Kundenschlüssel** Feld, geben Sie den privaten Schlüssel des Zertifikats an.
    c) Wenn Sie das Zertifikat des Kafka-Servers nicht verifizieren möchten, wählen Sie **Überspringen Sie die Überprüfung Server Serverzertifikats**.
    d) Wenn Sie das Zertifikat des Kafka-Servers verifizieren möchten, das Zertifikat jedoch nicht von einer gültigen Zertifizierungsstelle (CA) signiert wurde, finden Sie im **CA-Zertifikate (optional)** Feld, geben Sie vertrauenswürdige Zertifikate im PEM-Format an, mit denen das Serverzertifikat überprüft werden soll. Wenn diese Option nicht angegeben ist, wird das Serverzertifikat mit der integrierten Liste gültiger CA-Zertifikate validiert.
11. Geben Sie mindestens einen Kafka-Broker an, der in einem Kafka-Cluster auch als Knoten bezeichnet wird und übertragene Daten empfangen kann.

    Hinweis: Sie können mehrere Broker hinzufügen, die Teil desselben Kafka-Clusters sind, um die Konnektivität sicherzustellen, falls ein einzelner Broker nicht verfügbar ist. Alle Broker müssen Teil desselben Cluster sein.

    a) In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Kafka-Brokers ein.
    b) In der Hafen In diesem Feld geben Sie die Portnummer des Kafka-Brokers ein.
    c) Klicken Sie auf das Plus (**+**) Symbol.

12. Optional: Klicken Sie **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Kafka-Server herzustellen und eine Testnachricht an den Server zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist.

    Hinweis Wenn der Test fehlschlägt, überprüfen Sie die Protokolle auf Ihrem Kafka-Server auf detailliertere Informationen zum Fehler, bearbeiten Sie dann die Zielkonfiguration und testen Sie die Verbindung erneut.

13. Klicken Sie **Speichern**.

Nächste Schritte
Erstellen Sie einen Auslöser, der festlegt, welche Kafka-Nachrichtendaten gesendet werden sollen, und der die Übertragung der Daten an das Ziel initiiert. Weitere Informationen finden Sie in der Remote.Kafka Klasse in der ExtraHop Trigger API-Referenz.

Konfigurieren Sie ein MongoDB-Ziel für einen offenen Datenstrom

Sie können Daten auf einem ExtraHop-System in ein System exportieren, das empfängt MongoDB Eingabe für die Langzeitarchivierung und den Vergleich mit anderen Quellen.

Wichtig: Auf dem System muss MongoDB 6.0 oder früher ausgeführt werden, um exportierte Daten zu empfangen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenströme öffnen**.
3. Klicken Sie **Ziel hinzufügen**.
4. Aus dem Typ des Ziels Dropdownliste, wählen **MongoDB**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Remote-MongoDB-Servers ein.
7. In der Hafen Feld, geben Sie die Portnummer des Remote-MongoDB-Servers ein.
8. Wählen **TLS-Verschlüsselung** um übertragene Daten zu verschlüsseln.
9. Wählen **Zertifikatsüberprüfung überspringen** um die Zertifikatsüberprüfung verschlüsselter Daten zu umgehen.

    Hinweis Sichere Verbindungen zum MongoDB-Zielserver können verifiziert werden durch vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.

10. Optional: Fügen Sie Benutzer hinzu, die die Berechtigung haben, in eine MongoDB-Datenbank auf dem Zielserver zu schreiben.
    a) In der Datenbank Feld, geben Sie den Namen der MongoDB-Datenbank ein.
    b) In der Nutzername Feld, geben Sie den Benutzernamen des Benutzers ein.
    c) In der Passwort Feld, geben Sie das Passwort des Benutzers ein.
    d) Klicken Sie auf das Plus (**+**) Symbol.
11. Optional: Klicken Sie **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem entfernten MongoDB-Server herzustellen und eine Testnachricht an den Server zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.
12. Klicken Sie **Speichern**.

Nächste Schritte
Erstellen Sie einen Auslöser, der angibt, welche MongoDB-Nachrichtendaten gesendet werden sollen, und initiiert die Übertragung von Daten an das Ziel. Weitere Informationen finden Sie in der Remote.MongoDB Klasse in der ExtraHop Trigger API-Referenz.

Konfigurieren Sie ein Rohdatenziel für einen offenen Datenstrom

Sie können Rohdaten auf einem ExtraHop-System auf jeden Server exportieren, um sie langfristig zu archivieren und mit anderen Quellen zu vergleichen. Darüber hinaus können Sie eine Option zum Komprimieren der Daten über GZIP auswählen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken **Datenströme öffnen**.
3. klicken **Ziel hinzufügen**.
4. Aus dem Typ des Ziels Dropdownliste, wählen **Roh**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Remoteservers ein.
7. In der Hafen Feld, geben Sie die Portnummer des Remoteservers ein.
8. Aus dem Protokoll Wählen Sie in der Dropdownliste eines der folgenden Protokolle aus, über das Daten übertragen werden sollen:
   - **TCP**
   - **UDP**
9. Optional: Aktivieren Sie die GZIP-Komprimierung der übertragenen Daten.
   a) Wählen **GZIP-Komprimierung**.
   b) Geben Sie für jedes der folgenden Felder einen Wert an:

   Anzahl der Byte, nach denen GZIP aktualisiert werden soll
   Der Standardwert ist 64000 Byte.

   Anzahl der Sekunden, nach denen GZIP aktualisiert werden soll
   Der Standardwert ist 300 Sekunden.
10. Optional: klicken **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Server herzustellen und eine Testnachricht an den Server zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.
11. Klicken Sie **Speichern**.

Nächste Schritte
Erstellen Sie einen Auslöser, der festlegt, welche Rohdaten der Nachricht gesendet werden sollen, und der die Übertragung der Daten an das Ziel initiiert. Weitere Informationen finden Sie in der Remote.Raw Klasse in der ExtraHop Trigger API-Referenz.

Konfigurieren Sie ein Syslog-Ziel für einen offenen Datenstrom

Sie können Daten auf einem ExtraHop-System in jedes System exportieren, das Syslog-Eingaben empfängt (wie Splunk, ArcSight oder Q1 Labs), um sie langfristig zu archivieren und mit anderen Quellen zu vergleichen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
   Wiederholen Sie diese Schritte für jeden Sensor in Ihrer Umgebung.
2. In der Konfiguration des Systems Abschnitt, klicken Sie **Datenströme öffnen**.
3. Klicken Sie **Ziel hinzufügen**.
4. Aus dem Zieltyp Dropdownliste, wählen **Syslog**.
5. In der Name Feld, geben Sie einen Namen ein, um das Ziel zu identifizieren.
6. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Remote-Syslog-Servers ein.

7. In der Hafen Feld, geben Sie die Portnummer des Remote-Syslog-Servers ein.
8. Aus dem Protokoll Wählen Sie in der Dropdownliste eines der folgenden Protokolle aus, über das Daten übertragen werden sollen:
   - **TCP**
   - **UDP**
   - **TLS**
9. Optional: Wählen **Lokale Zeit** um Syslog-Informationen zu senden mit Zeitstempel in der lokalen Zeitzone des ExtraHop-Systems. Wenn diese Option nicht ausgewählt ist, werden Zeitstempel in GMT gesendet.
10. Optional: Wählen **Rahmen für Längenpräfix** um die Anzahl der Byte in einer Nachricht dem Anfang jeder Nachricht voranzustellen. Wenn diese Option nicht ausgewählt ist, wird das Ende jeder Nachricht durch einen abschließenden Zeilenumbruch begrenzt.
11. Optional: In der Mindestanzahl Byte im Stapel Feld, geben Sie die Mindestanzahl an Byte ein, die gleichzeitig an den Syslog-Server gesendet werden sollen.
12. Optional: In der Gleichzeitige Verbindungen Feld, geben Sie die Anzahl der gleichzeitigen Verbindungen ein, über die Nachrichten gesendet werden sollen.
13. Optional: Wenn Sie das ausgewählt haben **TLS** Protokoll, geben Sie die Zertifikatsoptionen an.
    a) Wenn der Syslog-Server eine Client-Authentifizierung erfordert, finden Sie im **Client-Zertifikat** Feld, geben Sie ein TLS-Client-Zertifikat an, das an den Server gesendet werden soll.
    b) Wenn Sie ein Client-Zertifikat angegeben haben, in **Kundenschlüssel** Feld, geben Sie den privaten Schlüssel des Zertifikats an.
    c) Wenn Sie das Zertifikat des Syslog-Servers nicht verifizieren möchten, wählen Sie **Überspringen Sie die Überprüfung Server Serverzertifikats**.
    d) Wenn Sie das Zertifikat des Kafka-Servers verifizieren möchten, das Zertifikat jedoch nicht von einer gültigen Zertifizierungsstelle (CA) signiert wurde, finden Sie in der **CA-Zertifikate (optional)** Feld, geben Sie vertrauenswürdige Zertifikate im PEM-Format an, mit denen das Serverzertifikat überprüft werden soll. Wenn diese Option nicht angegeben ist, wird das Serverzertifikat mit der integrierten Liste gültiger CA-Zertifikate validiert.
14. Optional: Klicken Sie **Testen** um eine Verbindung zwischen dem ExtraHop-System und dem Remote-Syslog-Server herzustellen und eine Testnachricht an den Server zu senden.
    Das Dialogfeld zeigt eine Meldung an, die angibt, ob die Verbindung erfolgreich war oder fehlgeschlagen ist. Wenn der Test fehlschlägt, bearbeiten Sie die Zielkonfiguration und testen Sie die Verbindung erneut.
15. Klicken Sie **Speichern**.

Nächste Schritte
Erstellen Sie einen Auslöser, der angibt, welche Syslog-Nachrichtendaten gesendet werden sollen, und der die Übertragung der Daten an das Ziel initiiert. Weitere Informationen finden Sie in der Remote.Syslog Klasse in der ExtraHop Trigger API-Referenz.

ODS-Einzelheiten

Die Detailseite von Open Data Stream (ODS) enthält Informationen über die Datenmenge, die an das ODS-Ziel gesendet wurde, und darüber, wie viele Fehler aufgetreten sind.

Hinweis: Die Seite „ODS-Details“ ist derzeit nur für HTTP-ODS-Ziele verfügbar.

Verbindungsversuche

Die Häufigkeit, mit der das ExtraHop-System versucht hat, eine Verbindung zum ODS-Ziel herzustellen.

Verbindungsfehler

Die Anzahl der Fehler, die bei Verbindungsversuchen mit dem ODS-Ziel aufgetreten sind.

IPC-Fehler

Die Anzahl der Fehler, die bei der Datenübertragung zwischen Triggern und dem exremote-Prozess aufgetreten sind. Wenn IPC-Fehler auftreten, wenden Sie sich an den ExtraHop Support, um Hilfe zu erhalten.

An das Ziel gesendete Byte

Die Anzahl der Byte, die vom exremote-Prozess an das ODS-Ziel weitergeleitet wurden.

An das Ziel gesendete Nachrichten

Die Anzahl der Nachrichten, die vom exremote-Prozess an das ODS-Ziel weitergeleitet wurden.

Von Triggern gesendete Bytes

Die Anzahl der Byte, die an den Exremote-Prozess gesendet werden, um an das ODS-Ziel weitergeleitet zu werden.

Von Triggern gesendete Nachrichten

Die Anzahl der Nachrichten, die auslösen, die an den Exremote-Prozess gesendet werden, um an das ODS-Ziel weitergeleitet zu werden.

Von exremote gelöschte Nachrichten

Die Anzahl der Nachrichten, die Trigger an den Exremote-Prozess gesendet, aber nie an das ODS-Ziel weitergeleitet wurden.

Details zum Fehler

Zeit

Die Uhrzeit, zu der der Fehler aufgetreten ist.

URL

Die URL des ODS-Ziels.

Status

Der vom ODS-Ziel zurückgegebene HTTP-Statuscode.

Header anfordern

Die Header der HTTP-Anfrage, die an das ODS-Ziel gesendet wurde.

Nachrichtentext anfordern

Der Hauptteil der HTTP-Anfrage, die an das ODS-Ziel gesendet wurde.

Antwort-Header

Die Header der HTTP-Antwort, die vom ODS-Ziel gesendet wurde.

Antworttext

Der Hauptteil der HTTP-Antwort, die vom ODS-Ziel gesendet wurde.

Tendenzen

Trendbasierte Warnmeldungen werden generiert, wenn eine überwachte Metrik von den normalen Trends abweicht, die vom ExtraHop-System beobachtet werden. Bei Bedarf können Sie alle konfigurierten Trends und trendbasierten Benachrichtigungen löschen.

- klicken **Trends zurücksetzen** um alle Trenddaten aus dem ExtraHop-System zu löschen.

Einen Sensor oder eine Konsole sichern und wiederherstellen

Nachdem Sie Ihren ExtraHop konfiguriert haben Konsole und Sensor Bei Anpassungen wie Bundles, Triggern und Dashboards oder administrativen Änderungen wie dem Hinzufügen neuer Benutzer empfiehlt ExtraHop, dass Sie Ihre Einstellungen regelmäßig sichern, um die Wiederherstellung nach einem Systemausfall zu erleichtern.

Tägliche Backups werden automatisch im lokalen Datenspeicher gespeichert. Wir empfehlen jedoch, vor der Aktualisierung der Firmware oder vor größeren Änderungen an Ihrer Umgebung (z. B. Änderung des Datenfeeds zum Sensor) manuell ein System-Backup zu erstellen. Laden Sie dann die Sicherungsdatei herunter und speichern Sie sie an einem sicheren Ort.

Einen Sensor oder eine Konsole sichern

Erstellen Sie eine Systemsicherung und speichern Sie die Sicherungsdatei an einem sicheren Ort.

> **Wichtig:** System-Backups enthalten vertrauliche Informationen, einschließlich TLS-Schlüssel. Wenn Sie eine Systemsicherung erstellen, stellen Sie sicher, dass Sie die Sicherungsdatei an einem sicheren Ort speichern.

Die folgenden Anpassungen und Ressourcen werden gespeichert, wenn Sie ein Backup erstellen.

- Benutzeranpassungen wie Bundles, Trigger und Dashboards.
- Konfigurationen, die aus Administrationseinstellungen vorgenommen wurden, z. B. lokal erstellte Benutzer und remote importierte Benutzergruppen, die Konfigurationsdateieinstellungen, TLS-Zertifikate und Verbindungen zu ExtraHop-Recordstores und Packetstores ausführen.

Die folgenden Anpassungen und Ressourcen werden nicht gespeichert, wenn Sie ein Backup erstellen oder zu einem neuen Ziel migrieren.

- Lizenzinformationen für das System. Wenn Sie Einstellungen für ein neues Ziel wiederherstellen, müssen Sie das neue Ziel manuell lizenzieren.
- Präzise Paketerfassung. Sie können gespeicherte Paketerfassungen manuell herunterladen, indem Sie die Schritte unter Paketerfassungen anzeigen und herunterladen.
- Bei der Wiederherstellung einer virtuellen Konsole, die über eine getunnelte Verbindung von einem Sensor, der Tunnel muss nach Abschluss der Wiederherstellung und aller Anpassungen an der Konsole dafür neu eingerichtet werden Sensor muss manuell neu erstellt werden.
- Vom Benutzer hochgeladene TLS-Schlüssel für die Entschlüsselung des Datenverkehrs.
- Sichere Keystore-Daten, die Passwörter enthalten. Wenn Sie eine Sicherungsdatei auf demselben Ziel wiederherstellen, das das Backup erstellt hat, und der Keystore intakt ist, müssen Sie die Anmeldedaten nicht erneut eingeben. Wenn Sie jedoch eine Sicherungsdatei auf einem neuen Ziel wiederherstellen oder zu einem neuen Ziel migrieren, müssen Sie die folgenden Anmeldedaten erneut eingeben:
  - Alle SNMP-Community-Zeichenketten, die für die SNMP-Abfrage von Flow-Netzwerken bereitgestellt werden.
  - Jedes Bindkennwort, das für die Verbindung mit LDAP für Fernauthentifizierungszwecke bereitgestellt wird.
  - Jedes Passwort, das für die Verbindung zu einem SMTP-Server bereitgestellt wird, für den eine SMTP-Authentifizierung erforderlich ist.
  - Jedes Passwort, das für die Verbindung zu einem externen Datenspeicher angegeben wurde.
  - Jedes Passwort, das für den Zugriff auf externe Ressourcen über den konfigurierten globalen Proxy bereitgestellt wird.
  - Jedes Passwort, das für den Zugriff auf ExtraHop Cloud Services über den konfigurierten ExtraHop-Cloud-Proxy angegeben wurde.
  - Alle Authentifizierungsdaten oder Schlüssel, die zur Konfiguration von Open Data Stream-Zielen bereitgestellt werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **System-Backup erstellen**, und klicken Sie dann auf **OK**.
   Eine Liste der vom Benutzer gespeicherten und automatischen Backups wird angezeigt.
4. Klicken Sie auf den Namen der neuen Sicherungsdatei. **Benutzer gespeichert <*Zeitstempel*> (neu)**.

Die Backup-Datei mit einem `.exbk` Dateierweiterung, wird automatisch am Standard-Download-Speicherort für Ihren Browser gespeichert.

Stellen Sie einen Sensor oder eine Konsole aus einem System-Backup wieder her

Sie können das ExtraHop-System anhand der vom Benutzer gespeicherten oder automatischen Backups wiederherstellen, die auf dem System gespeichert sind. Sie können zwei Arten von Wiederherstellungsvorgängen ausführen: nur Anpassungen (z. B. Änderungen an Warnungen, Dashboards, Triggern, benutzerdefinierten Metriken) oder sowohl Anpassungen als auch Systemressourcen.

Bevor Sie beginnen
Auf dem Ziel muss dieselbe Firmware-Version ausgeführt werden, die den ersten und zweiten Ziffern der Firmware entspricht, die die Backup-Datei generiert hat. Wenn die Versionen nicht identisch sind, schlägt der Wiederherstellungsvorgang fehl.

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um eine Sicherungsdatei auf demselben Sensor oder derselben Konsole wiederherzustellen, die die Sicherungsdatei erstellt hat. Wenn Sie die Einstellungen auf einen neuen Sensor oder eine neue Konsole migrieren möchten, finden Sie unter Einstellungen auf einen neuen Sensor oder eine neue Konsole übertragen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. klicken **System-Backups anzeigen oder wiederherstellen**.
4. klicken **Wiederherstellen** neben dem Benutzer-Backup oder dem automatischen Backup, das Sie wiederherstellen möchten.
5. Wählen Sie eine der folgenden Wiederherstellungsoptionen:

   Systemanpassungen wiederherstellen

   Wählen Sie diese Option, wenn beispielsweise ein Dashboard versehentlich gelöscht wurde oder eine andere Benutzereinstellung wiederhergestellt werden muss. Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden nicht überschrieben, wenn die Anpassungen wiederhergestellt werden.

   Systemanpassungen und Ressourcen wiederherstellen

   Wählen Sie diese Option, wenn Sie das System in den Zustand zurückversetzen möchten, in dem es sich bei der Erstellung des Backups befand.

   Warnung: Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden überschrieben, wenn die Anpassungen und Ressourcen wiederhergestellt werden.
6. Klicken Sie **OK**.
7. Optional: Wenn du ausgewählt hast **Systemanpassungen wiederherstellen**, klicken **Import-Protokoll anzeigen** um zu sehen, welche Anpassungen wiederhergestellt wurden.
8. Starten Sie das System neu.
   a) Kehren Sie zu den Administrationseinstellungen zurück.
   b) In der Appliance-Einstellungen Abschnitt, klicken Sie **Herunterfahren oder Neustarten**.
   c) In der Aktionen Spalte, für die System Eintrag, klicken **Neustarten**.
   d) klicken **Neustarten** zur Bestätigung.

Stellen Sie einen Sensor oder eine Konsole aus einer Sicherungsdatei wieder her

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um ein System aus einer Sicherungsdatei auf demselben Sensor oder derselben Konsole wiederherzustellen, die die Sicherungsdatei erstellt hat.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **Laden Sie die Sicherungsdatei hoch, um das System wiederherzustellen**.
4. Wählen Sie eine der folgenden Wiederherstellungsoptionen:

   Systemanpassungen wiederherstellen

   Wählen Sie diese Option, wenn beispielsweise ein Dashboard versehentlich gelöscht wurde oder eine andere Benutzereinstellung wiederhergestellt werden muss. Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden nicht überschrieben, wenn die Anpassungen wiederhergestellt werden.

   Systemanpassungen und Ressourcen wiederherstellen

   Wählen Sie diese Option, wenn Sie das System in den Zustand zurückversetzen möchten, in dem es sich bei der Erstellung des Backups befand.

   Warnung: Alle Anpassungen, die nach der Erstellung der Sicherungsdatei vorgenommen wurden, werden überschrieben, wenn die Anpassungen und Ressourcen wiederhergestellt werden.
5. Klicken Sie **Wählen Sie Datei** und navigieren Sie zu einer Sicherungsdatei, die Sie zuvor gespeichert haben.
6. Klicken Sie **Wiederherstellen**.
7. Optional: Wenn du ausgewählt hast **Systemanpassungen wiederherstellen**, klicken Sie **Importprotokoll anzeigen** um zu sehen, welche Anpassungen wiederhergestellt wurden.
8. Starten Sie das System neu.
   a) Kehren Sie zu den Administrationseinstellungen zurück.
   b) In der Appliance-Einstellungen Abschnitt, klicken **Herunterfahren oder Neustarten**.
   c) In der Aktionen Kolumne für die System Eintrag, klick **Neustart**.
   d) Klicken Sie **Neustart** zur Bestätigung.

Einstellungen auf einen neuen Sensor oder eine neue Konsole übertragen

Dieses Verfahren beschreibt die Schritte, die erforderlich sind, um eine Sicherungsdatei auf eine neue wiederherzustellen Konsole oder Sensor. Nur Systemeinstellungen von Ihrer vorhandenen Konsole oder Sensor werden übertragen. Metriken im lokalen Datenspeicher werden nicht übertragen.

Bevor Sie beginnen

- Erstellen Sie eine Systemsicherung und speichern Sie die Sicherungsdatei an einem sicheren Ort.
- Schalten Sie die Quelle aus Sensor oder Konsole um es vor der Übertragung der Einstellungen aus dem Netzwerk zu entfernen. Ziel und Quelle können nicht gleichzeitig im Netzwerk aktiv sein.

  Wichtig: Trennen Sie keine Sensoren die bereits mit einer Konsole verbunden sind.
- Bereitstellen und Register der Zielsensor oder die Zielkonsole.
  - Stellen Sie sicher, dass es sich bei dem Ziel um den gleichen Typ handelt Sensor oder Konsole (physisch oder virtuell) als Quelle.
  - Stellen Sie sicher, dass das Ziel dieselbe Größe oder größer hat (maximaler Durchsatz auf dem Sensor; CPU, RAM und Festplattenkapazität auf der Konsole) wie die Quelle.
  - Stellen Sie sicher, dass das Ziel über eine Firmware-Version verfügt, die der Firmware-Version entspricht, die die Sicherungsdatei generiert hat. Wenn die ersten beiden Ziffern der Firmware-Versionen nicht identisch sind, schlägt der Wiederherstellungsvorgang fehl.
- Nach der Übertragung der Einstellungen auf ein Ziel Konsole, Sie müssen alle manuell erneut verbinden Sensoren.
- Bei der Übertragung von Einstellungen auf ein Ziel Konsole das für eine getunnelte Verbindung zum konfiguriert ist Sensoren, wir empfehlen Ihnen, das Ziel zu konfigurieren Konsole mit demselben Hostnamen und derselben IP-Adresse wie die Quellkonsole.

1. Melden Sie sich bei den Administrationseinstellungen auf dem Zielsystem an über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Konfiguration des Systems Abschnitt, klicken **Sichern und Wiederherstellen**.
3. Klicken Sie **Laden Sie die Sicherungsdatei hoch, um das System wiederherzustellen**.
4. Wählen **Systemanpassungen und Ressourcen wiederherstellen**.
5. Klicken Sie **Wählen Sie Datei**, navigieren Sie zur gespeicherten Sicherungsdatei, und klicken Sie dann auf **Öffnen**.
6. Klicken Sie **Wiederherstellen**.

   Warnung: Wenn die Sicherungsdatei nicht mit dem lokalen Datenspeicher kompatibel ist, muss der Datenspeicher zurückgesetzt werden.

   Nach Abschluss der Wiederherstellung werden Sie vom System abgemeldet.
7. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin` und stellen Sie sicher, dass Ihre Anpassungen auf dem Zielsensor oder der Konsole korrekt wiederhergestellt wurden.

   Hinweis: Wenn der Quellsensor oder die Konsole mit ExtraHop Cloud Services verbunden war, müssen Sie das Ziel manuell mit ExtraHop Cloud Services verbinden.

Schließen Sie die Sensoren wieder an die Konsole an

Wenn Sie Einstellungen auf ein neues übertragen haben Konsole, Sie müssen alle zuvor verbundenen manuell erneut verbinden Sensoren.

Bevor Sie beginnen

Wichtig: Wenn Ihre Konsole und Ihre Sensoren für eine getunnelte Verbindung konfiguriert sind, empfehlen wir, die Quelle- und Zielkonsole mit derselben IP-Adresse und demselben Hostnamen zu konfigurieren. Wenn Sie nicht dieselbe IP-Adresse und denselben Hostnamen festlegen können, überspringen Sie dieses Verfahren und stellen Sie eine neue Tunnelverbindung zu der neuen IP-Adresse oder dem neuen Hostnamen der Konsole her.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Verwaltung verbundener Appliances Abschnitt, unter ExtraHop-Sensor-Einstellungen, klicken **Sensoren verwalten**.
3. In der Spalte Aktionen für die erste Sensor, klicken **Erneut verbinden**.
4. Geben Sie das Passwort für den Setup-Benutzer von Sensor.
5. Klicken Sie **Verbinden**.
6. Wiederholen Sie die Schritte 3—5 für alle verbleibenden Verbindungsabbrüche Sensoren.
   Alle getrennten Sensoren sind jetzt online.

Appliance-Einstellungen

Sie können die folgenden Komponenten der ExtraHop-Appliance im Appliance-Einstellungen Abschnitt.

Alle Geräte haben die folgenden Komponenten:

Konfiguration ausführen
Laden Sie die laufende Konfigurationsdatei herunter und ändern Sie sie.

Dienstleistungen
Aktivieren oder deaktivieren Sie die Web Shell, die Verwaltungs-GUI, den SNMP-Dienst, den SSH-Zugriff und den TLS-Sitzungsschlüsselempfänger. Die Option SSL Session Key Receiver wird nur auf Paketsensoren angezeigt.

Firmware
Aktualisieren Sie die ExtraHop-Systemfirmware.

Systemzeit
Konfigurieren Sie die Systemzeit.

Herunterfahren oder Neustarten
Halten Sie die Systemdienste an und starten Sie sie neu.

Lizenz
Aktualisieren Sie die Lizenz, um Zusatzmodule zu aktivieren.

Festplatten
Stellt Informationen zu den Festplatten in der Appliance bereit.

Die folgenden Komponenten sind nur auf den angegebenen Appliances enthalten:

Spitzname für die Konsole
Weisen Sie einer ExtraHop-Konsole einen Spitznamen zu. Diese Einstellung ist nur auf der Konsole verfügbar.

Packetstore zurücksetzen
Löschen Sie alle Pakete, die in ExtraHop-Paketstores gespeichert sind. Das Packetstore zurücksetzen Die Seite erscheint nur in Packetstores.

Konfiguration ausführen

Die laufende Konfigurationsdatei gibt die Standardsystemkonfiguration an. Wenn Sie Systemeinstellungen ändern, müssen Sie die laufende Konfigurationsdatei speichern, um diese Änderungen nach einem Systemneustart beizubehalten.

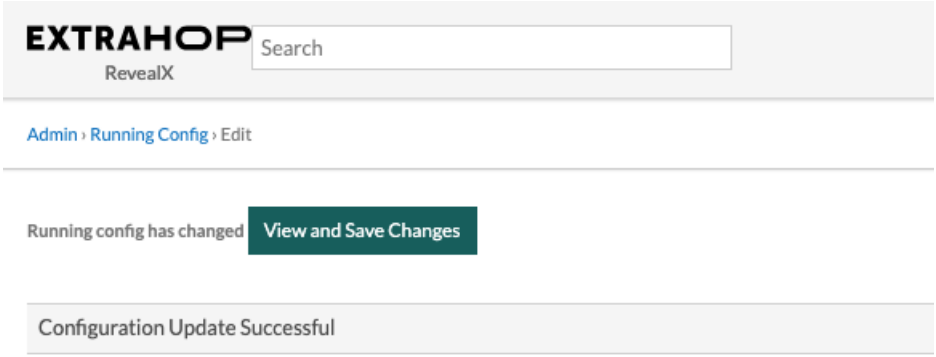
Hinweis: Es wird nicht empfohlen, Konfigurationsänderungen am Code von der Bearbeitungsseite aus vorzunehmen. Sie können die meisten Systemänderungen über andere Seiten in den Administrationseinstellungen vornehmen.

Speichern Sie die Systemeinstellungen in der laufenden Konfigurationsdatei

Wenn Sie eine der Systemkonfigurationseinstellungen auf einem ExtraHop-System ändern, müssen Sie die Aktualisierungen bestätigen, indem Sie die laufende Konfigurationsdatei speichern. Wenn Sie die Einstellungen nicht speichern, gehen die Änderungen verloren, wenn Ihr ExtraHop-System neu gestartet wird.

Um Sie daran zu erinnern, dass sich die aktuelle Konfiguration geändert hat, erscheint (Ungespeicherte Änderungen) neben dem Link Running Config auf der Hauptseite mit den Verwaltungseinstellungen sowie eine **Änderungen anzeigen und speichern** Schaltfläche auf allen Seiten mit Administrationseinstellungen.

1. Klicken Sie **Änderungen anzeigen und speichern**.



2. Prüfen Sie den Vergleich zwischen der alten laufenden Konfiguration und der aktuellen (nicht gespeicherten) laufenden Konfiguration und wählen Sie dann eine der folgenden Optionen aus:
   - Wenn die Änderungen korrekt sind, klicken Sie auf **Speichern**.
   - Wenn die Änderungen nicht korrekt sind, klicken Sie auf **Stornieren** und machen Sie dann die Änderungen rückgängig, indem Sie auf **Konfiguration zurücksetzen** .

Bearbeiten Sie die laufende Konfigurationsdatei

Die ExtraHop-Administrationseinstellungen bieten eine Schnittstelle zum Anzeigen und Ändern des Codes , der die Standardsystemkonfiguration spezifiziert. Zusätzlich zu den Änderungen an der laufenden Konfigurationsdatei über die Administrationseinstellungen können Sie auch Änderungen an der Konfiguration ausführen Seite.

Wichtig: Es wird nicht empfohlen, auf der Seite „Bearbeiten“ Konfigurationsänderungen am Code vorzunehmen. Sie können die meisten Systemänderungen über andere Administrationseinstellungen vornehmen.

Laden Sie die aktuelle Konfiguration als Textdatei herunter

Sie können die laufende Konfigurationsdatei auf Ihre Workstation herunterladen. Sie können diese Textdatei öffnen und lokal Änderungen daran vornehmen, bevor Sie diese Änderungen in die Konfiguration ausführen Fenster.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Konfiguration ausführen**.
3. Klicken Sie **Laden Sie die Konfiguration als Datei herunter**.

Die aktuell laufende Konfigurationsdatei wird als Textdatei an Ihren Standard-Download-Speicherort heruntergeladen.

ICMPv6-Nachrichten vom Typ Destination Unreachable deaktivieren

Sie können verhindern, dass das ExtraHop-System ICMPv6-Nachrichten vom Typ Destination Unreachable generiert. Möglicherweise möchten Sie ICMPv6-Nachrichten vom Typ Destination Unreachable aus Sicherheitsgründen gemäß RFC 4443 deaktivieren.

Um ICMPv6-Meldungen vom Typ Destination Unreachable zu deaktivieren, müssen Sie die Running Configuration bearbeiten. Wir empfehlen jedoch, die Running Configurations-Datei nicht manuell ohne Anweisung des ExtraHop-Supports zu bearbeiten. Wenn Sie die laufende Konfigurationsdatei manuell falsch bearbeiten, kann dies dazu führen, dass das System nicht mehr verfügbar ist oder die Erfassung von Daten beendet wird. Sie können Kontakt aufnehmen ExtraHop-Unterstützung.

Bestimmte ICMPv6-Echo-Antwortnachrichten deaktivieren

Sie können verhindern, dass das ExtraHop-System Echo-Antwortnachrichten als Antwort auf ICMPv6-Echoanforderungsnachrichten generiert, die an eine IPv6-Multicast- oder Anycast-Adresse gesendet werden. Möglicherweise möchten Sie diese Nachrichten deaktivieren, um unnötigen Netzwerkverkehr zu reduzieren.

Um bestimmte ICMPv6-Echo-Antwortnachrichten zu deaktivieren, müssen Sie die laufende Konfigurationsdatei bearbeiten. Wir empfehlen jedoch, die laufende Konfigurationsdatei nicht ohne Anweisung des ExtraHop-Supports manuell zu bearbeiten. Eine falsche manuelle Bearbeitung dieser Datei kann dazu führen, dass das System nicht mehr verfügbar ist oder keine Daten mehr erfasst werden. Sie können kontaktieren ExtraHop-Unterstützung.

Dienstleistungen

Diese Dienste werden im Hintergrund ausgeführt und führen Funktionen aus, für die keine Benutzereingaben erforderlich sind. Diese Dienste können über die Administrationseinstellungen gestartet und gestoppt werden.

Aktivieren oder deaktivieren Sie die Management-GUI

Die Management-GUI bietet browserbasierten Zugriff auf das ExtraHop-System. Standardmäßig ist dieser Dienst aktiviert, sodass ExtraHop-Benutzer über einen Webbrowser auf das ExtraHop-System zugreifen können. Wenn dieser Dienst deaktiviert ist, wird die Apache Web Server-Sitzung beendet und der gesamte browserbasierte Zugriff wird deaktiviert.

Warnung: Deaktivieren Sie diesen Dienst nur, wenn Sie ein erfahrener ExtraHop-Administrator sind und mit der ExtraHop-CLI vertraut sind.

SNMP-Dienst aktivieren oder deaktivieren

Aktivieren Sie den SNMP-Dienst auf dem ExtraHop-System, wenn Sie möchten, dass Ihre Netzwerkgeräteüberwachungssoftware Informationen über das ExtraHop-System sammelt. Dieser Dienst ist standardmäßig deaktiviert.

- Aktivieren Sie den SNMP-Dienst auf der Seite Dienste, indem Sie das Kontrollkästchen Deaktiviert aktivieren und dann auf **Speichern**. Nach dem Aktualisieren der Seite wird das Kontrollkästchen Aktiviert angezeigt.
- Konfigurieren Sie den SNMP-Dienst und laden Sie die ExtraHop MIB-Datei herunter

SSH-Zugriff aktivieren oder deaktivieren

Der SSH-Zugriff ist standardmäßig aktiviert, damit sich Benutzer sicher an der ExtraHop-Befehlszeilenschnittstelle (CLI) anmelden können.

Hinweis: Der SSH-Dienst und der Management GUI Service können nicht gleichzeitig deaktiviert werden. Mindestens einer dieser Dienste muss aktiviert sein, um Zugriff auf das System zu gewähren.

Den TLS Session Key Receiver aktivieren oder deaktivieren (nur Sensor)

Sie müssen den Sitzungsschlüsselempfängerdienst über die Verwaltungseinstellungen aktivieren, bevor das ExtraHop-System Sitzungsschlüssel vom Sitzungsschlüssel-Forwarder empfangen und entschlüsseln kann. Standardmäßig ist dieser Dienst deaktiviert.

Hinweis: Wenn Sie dieses Kontrollkästchen nicht sehen und die TLS-Entschlüsselungslizenz gekauft haben, wenden Sie sich an ExtraHop-Unterstützung um Ihre Lizenz zu aktualisieren.

SNMP-Dienst

Konfigurieren Sie den SNMP-Dienst auf Ihrem ExtraHop-System, sodass Sie Ihre Netzwerkgeräteüberwachungssoftware so konfigurieren können, dass Informationen über Ihr ExtraHop-System über das Simple Network Management Protocol (SNMP) erfasst werden.

Beispielsweise können Sie Ihre Monitoring-Software so konfigurieren, dass sie bestimmt, wie viel freier Speicherplatz auf einem ExtraHop-System verfügbar ist, und eine Alarm senden, wenn das System zu über 95% voll ist. Importieren Sie die ExtraHop SNMP MIB-Datei in Ihre Monitoring-Software, um alle ExtraHop-spezifischen SNMP-Objekte zu überwachen. Sie können Einstellungen für SNMPv1/SNMPv2 und SNMPv3 konfigurieren.

Konfigurieren Sie den SNMPv1- und SNMPv2-Dienst
Mit der folgenden Konfiguration können Sie das System mit einem SNMP-Manager überwachen, der SNMPv1 und SNMPv2 unterstützt.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Für SNMP-Dienst, klicken **Konfiguriere**.
4. Wählen Sie die **Aktiviert** Kontrollkästchen, um den SNMP-Dienst zu aktivieren.
5. Wählen Sie die **SNMPv1 und SNMPv2 aktiviert** Kontrollkästchen, um den SNMPv1- und SNMPv2-Dienst zu aktivieren.
6. In der SNMP-Gemeinschaft Feld, geben Sie einen benutzerfreundlichen Namen für die SNMP-Community ein.
7. In der SNMP-Systemkontakt Geben Sie in dieses Feld einen gültigen Namen oder eine gültige E-Mail-Adresse für den SNMP-Systemkontakt ein.
8. In der Standort des SNMP-Systems Feld, geben Sie einen Speicherort für das SNMP-System ein.
9. Klicken Sie **Einstellungen speichern**.

Nächste Schritte
Laden Sie die ExtraHop SNMP MIB-Datei von der Seite SNMP Service Configuration herunter.

Konfigurieren Sie den SNMPv3-Dienst
Mit der folgenden Konfiguration können Sie das System mit einem SNMP-Manager überwachen, der SNMPv3 unterstützt. Das SNMPv3-Sicherheitsmodell bietet zusätzliche Unterstützung für Authentifizierung - und Datenschutzprotokolle.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Dienstleistungen**.
3. Für SNMP-Dienst, klicken **Konfiguriere**.
4. Wählen Sie die **Aktiviert** Kontrollkästchen, um den SNMP-Dienst zu aktivieren.
5. Wählen Sie die **SNMPv3 aktiviert** Kontrollkästchen, um den SNMPv3-Dienst zu aktivieren.
6. In der SNMPv3-Benutzername Feld, geben Sie den Namen des Benutzers ein , der auf den SNMPv3-Dienst zugreifen kann.
7. Wählen Sie in der Dropdownliste Authentifizierung und Datenschutzmodus **Authentifizierung und Datenschutz** oder **Authentifizierung und kein Datenschutz**.

   Wenn du auswählst **Authentifizierung und Datenschutz**, müssen Sie auch das ausfüllen Datenschutz-Passwort Feld.

   Wichtig: ExtraHop-Systeme unterstützen die AES-128-Verschlüsselung für den Datenschutz von SNMPv3-Nachrichten.
8. In der Passwort für die Authentifizierung Geben Sie in dieses Feld ein Passwort ein, mit dem sich der Benutzer beim SNMPv3-Dienst authentifizieren kann.
9. Aus dem **Authentifizierungsalgorithmus** Dropdownliste, wählen **SHA-256** oder **SHA-1**.
10. Geben Sie im Feld Datenschutzkennwort das Passwort zum Entschlüsseln von SNMPv3-Traps ein.

    Dieses Feld ist erforderlich, wenn Sie **Authentifizierung und Datenschutz**.
11. Klicken Sie **Einstellungen speichern**.

Nächste Schritte
Laden Sie die ExtraHop SNMP MIB-Datei von der Konfiguration des SNMP-Dienstes Seite.

Firmware

Die Administrationseinstellungen bieten eine Schnittstelle zum Hochladen und Löschen der Firmware auf ExtraHop-Geräten. Die Firmware-Datei muss von dem Computer aus zugänglich sein, auf dem Sie das Upgrade durchführen werden.

Bevor Sie beginnen
Lesen Sie unbedingt die Versionshinweise für die Firmware-Version, die Sie installieren möchten. Die Versionshinweise enthalten Anleitungen zum Upgrade sowie bekannte Probleme, die sich auf kritische Workflows in Ihrem Unternehmen auswirken können.

Aktualisieren Sie die Firmware auf Ihrem ExtraHop-System

Das folgende Verfahren zeigt Ihnen, wie Sie Ihr ExtraHop-System auf die neueste Firmware-Version aktualisieren. Während der Firmware-Upgrade-Prozess für alle ExtraHop-Appliances ähnlich ist, müssen Sie bei einigen Appliances zusätzliche Überlegungen oder Schritte beachten, bevor Sie die Firmware in Ihrer Umgebung installieren. Wenn Sie Hilfe bei Ihrem Upgrade benötigen, wenden Sie sich an den ExtraHop Support.

Video: Sehen Sie sich die entsprechende Schulung an: Firmware aktualisieren

Wichtig: Wenn die Einstellungsmigration während des Firmware-Upgrades fehlschlägt, werden die zuvor installierte Firmware-Version und die ExtraHop-Systemeinstellungen wiederhergestellt.

Checkliste vor dem Upgrade
Im Folgenden finden Sie einige wichtige Überlegungen und Anforderungen zum Upgrade von ExtraHop-Appliances.

- Ein Systemhinweis erscheint auf Konsolen und Sensoren mit ExtraHop Cloud Services verbunden , wenn eine neue Firmware-Version verfügbar ist.
- Stellen Sie sicher, dass Ihr RevealX 360-System auf Version aktualisiert wurde 9,9 bevor Sie Ihr selbstverwaltetes Gerät aktualisieren Sensoren.
- Wenn Sie ein Upgrade von der Firmware-Version 8.7 oder früher durchführen, wenden Sie sich an den ExtraHop-Support, um weitere Informationen zum Upgrade zu erhalten.
- Wenn Sie einen virtuellen ExtraHop-Sensor aktualisieren, der auf einem VMware ESXi/ESX, Microsoft Hyper-V, oder Linux-KVM Für Plattformen ab Firmware-Version 9.6 oder früher muss die VM Streaming SIMD Extensions 4.2 (SSE4.2) und POPCNT-Anweisungen unterstützen; andernfalls schlägt das Upgrade fehl.
- Wenn Sie mehrere Typen von ExtraHop-Appliances haben, müssen Sie diese in der folgenden Reihenfolge aktualisieren:
  1. Konsole
  2. Sensoren (EDA und Ultra)
  3. Plattenläden
  4. Paketshops

Hinweis: Ihr Browser könnte nach 5 Minuten Inaktivität das Timeout beenden. Aktualisieren Sie die Browserseite, wenn das Update unvollständig erscheint.

Wenn die Browsersitzung abläuft, bevor das ExtraHop-System den Aktualisierungsvorgang abschließen kann, können Sie die folgenden Konnektivitätstests durchführen, um den Status während des Upgrade-Vorgangs zu bestätigen:

- Pingen Sie die Appliance von der Kommandozeile einer anderen Appliance oder Client-Workstation aus.

- Sehen Sie sich in den Administrationseinstellungen auf einer Konsole den Appliance-Status auf der Verbundene Geräte verwalten Seite.
- Stellen Sie über die iDRAC-Schnittstelle eine Verbindung zur Appliance her.

Konsolen-Upgrades

- Bei großen Konsolenbereitstellungen (Verwaltung von 50.000 Geräten oder mehr) sollten Sie sich mindestens eine Stunde Zeit nehmen, um das Upgrade durchzuführen.
- Die Firmware-Version der Konsole muss größer oder gleich der Firmware-Version aller angeschlossenen Geräte sein. Um die Funktionskompatibilität sicherzustellen, sollte auf allen angeschlossenen Geräten die Firmware-Version 8.7 oder höher ausgeführt werden.

Recordstore-Aktualisierungen

- Aktualisieren Sie Recordstores nicht auf eine Firmware-Version, die neuer ist als die Version, die auf den angeschlossenen Konsolen und Sensoren installiert ist.
- Nach dem Upgrade der Konsole und Sensoren, Deaktivieren Sie die Aufnahme von Datensätzen im Recordstore bevor Sie den Recordstore aktualisieren.
- Sie müssen alle Recordstore-Knoten in einem Recordstore-Cluster aktualisieren. Der Cluster funktioniert nicht richtig, wenn die Knoten unterschiedliche Firmware-Versionen verwenden.

  Wichtig: Die Nachrichten `Could not determine ingest status on some nodes` und `Error` werden auf der Seite Cluster-Datenverwaltung in den Verwaltungseinstellungen der aktualisierten Knoten angezeigt, bis alle Knoten im Cluster aktualisiert wurden. Diese Fehler werden erwartet und können ignoriert werden.
- Sie müssen die Aufnahme von Datensatz und die Neuzuweisung von Shards aus dem aktivieren Cluster-Datenmanagement Seite, nachdem alle Knoten im Recordstore-Cluster aktualisiert wurden.

Packetstore-Upgrades

- Aktualisieren Sie Packetstores nicht auf eine Firmware-Version, die neuer ist als die auf den angeschlossenen Konsolen installierte Version und Sensoren.

Aktualisieren Sie die Firmware auf einer Konsole und einem Sensor

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Firmware**.
3. Aus dem **Verfügbare Firmware** Wählen Sie in der Dropdownliste die Version der Firmware aus, die Sie installieren möchten. Die empfohlene Version ist standardmäßig ausgewählt.

   Hinweis: Für Sensoren enthält die Liste nur Firmware-Versionen, die mit der Version kompatibel sind, die auf der angeschlossenen Konsole ausgeführt wird.
4. Klicken Sie **Downloaden und installieren**.

Nachdem das Firmware-Upgrade erfolgreich installiert wurde, wird die ExtraHop-Appliance neu gestartet.

Aktualisieren Sie die Firmware auf Recordstores

1. Laden Sie die Firmware für die Appliance von der ExtraHop Kundenportal auf deinen Computer.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. Klicken Sie **Cluster-Datenmanagement**.
4. Klicken Sie **Record Ingest deaktivieren**.
5. Klicken Sie **Admin** um zur Haupt-Administrationsseite zurückzukehren.
6. Klicken Sie **Firmware**.

7. Klicken Sie **eine Datei aktualisieren oder eine URL angeben**.
8. Auf dem Firmware aktualisieren Seite, wählen Sie eine der folgenden Optionen:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigieren Sie zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie auf **Öffnen**.
   - Um Firmware von einem HTTP (s) -Staging-Server in Ihrem Netzwerk hochzuladen, klicken Sie auf **stattdessen von der URL abrufen** und geben Sie dann die URL in das Firmware-URL Feld.
9. Klicken Sie **Aufrüsten**.
   Das ExtraHop-System initiiert das Firmware-Upgrade. Sie können den Fortschritt des Upgrades mit dem Aktualisierung Fortschrittsbalken. Die Appliance wird nach der Installation der Firmware neu gestartet.
10. Wiederholen Sie die Schritte 6-9 auf allen verbleibenden Recordstore-Clusterknoten.

Nächste Schritte
Nachdem alle Knoten im Recordstore-Cluster aktualisiert wurden, aktivieren Sie die Datensatzaufnahme und die Shard-Neuzuweisung auf dem Cluster erneut. Sie müssen diese Schritte nur auf einem Recordstore-Knoten ausführen.

1. Klicken Sie im Abschnitt Recordstore Cluster Settings auf **Cluster-Datenmanagement**.
2. Klicken Sie **Datensatzaufnahme aktivieren**.
3. Klicken Sie **Shard-Neuzuweisung aktivieren**.

Aktualisieren Sie die Firmware auf Packetstores

1. Laden Sie die Firmware für die Appliance von der ExtraHop Kundenportal auf deinen Computer.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. klicken **eine Datei hochladen oder eine URL angeben**.
4. Auf dem Firmware aktualisieren Seite, wählen Sie eine der folgenden Optionen:
   - Um Firmware aus einer Datei hochzuladen, klicken Sie auf **Wählen Sie Datei**, navigieren Sie zum `.tar` Datei, die Sie hochladen möchten, und klicken Sie auf **Öffnen**.
   - Um Firmware von einem HTTP (s) -Staging-Server in Ihrem Netzwerk hochzuladen, klicken Sie auf **stattdessen von der URL abrufen** und geben Sie dann die URL in das Firmware-URL Feld.
5. Optional: Wenn Sie die Appliance nach der Installation der Firmware nicht automatisch neu starten möchten, löschen Sie das **Gerät nach der Installation automatisch neu starten** Ankreuzfeld.
6. klicken **Aufrüsten**.
   Das ExtraHop-System initiiert das Firmware-Upgrade. Sie können den Fortschritt des Upgrades mit dem Aktualisierung Fortschrittsbalken. Die Appliance wird nach der Installation der Firmware neu gestartet.
7. Wenn Sie sich nicht dafür entschieden haben, die Appliance automatisch neu zu starten, klicken Sie auf **Neustarten** um das System neu zu starten.

   Nachdem das Firmware-Update erfolgreich installiert wurde, zeigt die ExtraHop-Appliance die Versionsnummer der neuen Firmware in den Administrationseinstellungen an.

Rüsten Sie die angeschlossenen Sensoren in RevealX 360 auf
Administratoren können ein Upgrade durchführen Sensoren die mit RevealX 360 verbunden sind.

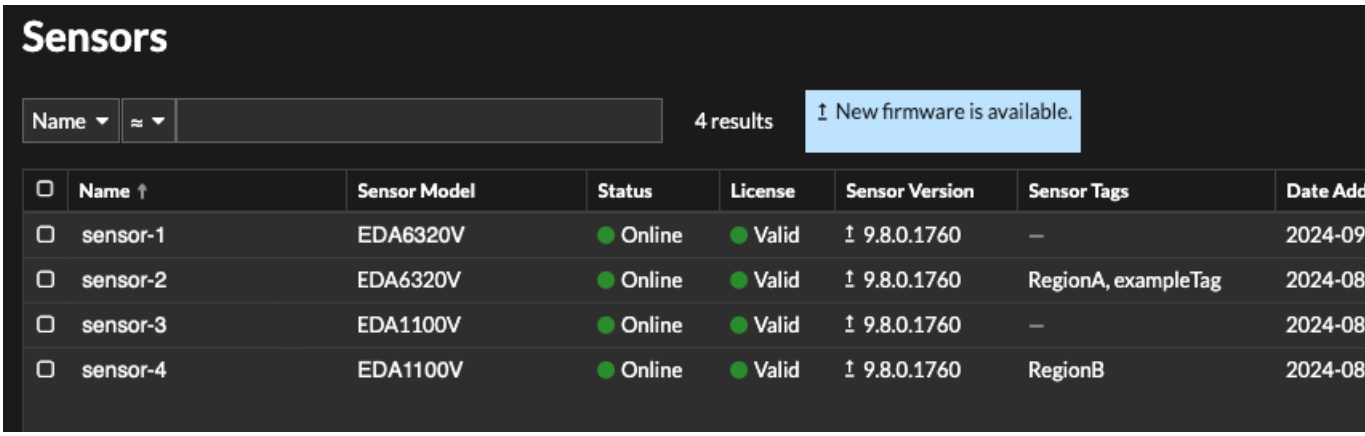
Bevor Sie beginnen

- Ihr Benutzerkonto muss über Rechte auf RevealX 360 für System- und Zugriffsadministration oder Systemadministration verfügen.

Hier sind einige Überlegungen zur Aufrüstung von Sensoren:

- Sensoren müssen mit ExtraHop Cloud Services verbunden sein
- Benachrichtigungen werden angezeigt, wenn eine neue Firmware-Version verfügbar ist
- Sie können mehrere upgraden Sensoren zur gleichen Zeit

1. Klicken Sie auf der Übersichtsseite auf **Systemeinstellungen** und klicken Sie dann **Fühler**.
   Sensoren, die für ein Upgrade in Frage kommen, zeigen einen Aufwärtspfeil in der Sensorversion Feld.



2. Markieren Sie das Kästchen neben jedem Sensor die Sie aktualisieren möchten.
3. In der Angaben zum Sensor Bereich, wählen Sie die Firmware-Version aus dem **Verfügbare Firmware** Dropdownliste.
   In der Dropdownliste werden nur Versionen angezeigt, die mit den ausgewählten Versionen kompatibel sind Sensoren.

   Nur die ausgewählten Sensoren für die ein Firmware-Upgrade verfügbar ist , finden Sie im Fühler Bereich „Details“.
4. Klicken Sie **Firmware installieren**.
   Wenn das Upgrade abgeschlossen ist, wird Sensorversion Das Feld wurde mit der neuen Firmware-Version aktualisiert.

Systemzeit

Auf der Seite Systemzeit werden die aktuellen Zeiteinstellungen angezeigt, die für Ihr ExtraHop-System konfiguriert sind. Zeigen Sie die aktuellen Systemzeiteinstellungen, die Standardanzeigezeit für Benutzer und Details für konfigurierte NTP-Server an.

Systemzeit ist die Uhrzeit und das Datum, die von Diensten verfolgt werden, die auf dem ExtraHop-System ausgeführt werden, um genaue Zeitberechnungen zu gewährleisten. Standardmäßig ist die Systemzeit auf dem Sensor oder der Konsole lokal konfiguriert. Für eine bessere Genauigkeit empfehlen wir, die Systemzeit über einen NTP-Zeitserver zu konfigurieren.

Bei der Datenerfassung muss die Systemzeit mit der Uhrzeit der angeschlossenen Sensoren übereinstimmen, um sicherzustellen , dass die Zeitstempel in geplanten Berichten, exportierten Dashboards und Diagrammmetriken korrekt und vollständig sind. Wenn Probleme mit der Zeitsynchronisierung auftreten, überprüfen Sie, ob die konfigurierte Systemzeit, externe Zeitserver oder NTP-Server korrekt sind. Setzen Sie die Systemzeit zurück oder NTP-Server synchronisieren bei Bedarf

Die folgende Tabelle enthält Details zur aktuellen Systemzeitkonfiguration. Klicken Sie **Zeit konfigurieren** zu Systemzeiteinstellungen konfigurieren.

Detail	Beschreibung
Zeitzone	Zeigt die aktuell gewählte Zeitzone an.
Systemzeit	Zeigt die aktuelle Systemzeit an.
Zeitserver	Zeigt eine kommagetrennte Liste der konfigurierten Zeitserver an.

Standardanzeigezeit für Benutzer

Im Abschnitt Standardanzeigezeit für Benutzer wird die Uhrzeit angezeigt, die allen Benutzern im ExtraHop-System angezeigt wird, es sei denn, ein Benutzer manuell ändert ihre angezeigte Zeitzone.

Um die Standardanzeigezeit zu ändern, wählen Sie eine der folgenden Optionen und klicken Sie dann auf **Änderungen speichern**:

- Uhrzeit des Browsers
- Systemzeit
- UTC

NTP-Status

Die NTP-Statustabelle zeigt die aktuelle Konfiguration und den Status aller NTP-Server an, die die Systemuhr synchron halten. Die folgende Tabelle enthält Details zu jedem konfigurierten NTP-Server. Klicken Sie **Jetzt synchronisieren** um die aktuelle Systemzeit mit einem Remote-Server zu synchronisieren.

Fernbedienung	Der Hostname oder die IP-Adresse des Remote-NTP-Servers, mit dem Sie die Synchronisierung konfiguriert haben.
st	Die Stratum-Ebene, 0 bis 16.
t	Die Art der Verbindung. Dieser Wert kann `u` für Unicast oder Manycast, `b` für Broadcast oder Multicast, `l` für lokale Referenzuhr, `s` für symmetrischen Peer, `A` für einen Manycast-Server `B` für einen Broadcast-Server, oder `M` für einen Multicast-Server.
wenn	Das letzte Mal, als der Server für diese Uhrzeit abgefragt wurde. Der Standardwert ist Sekunden, oder `m` wird minutenlang angezeigt, `h` stundenlang und `d` tagelang.
Umfrage	Wie oft der Server nach der Uhrzeit abgefragt wird, mindestens 16 Sekunden bis maximal 36 Stunden.
erreichen	Wert, der die Erfolgs- und Ausfallrate der Kommunikation mit dem Remoteserver Server. Erfolg bedeutet, dass das Bit gesetzt ist, Misserfolg bedeutet, dass das Bit nicht gesetzt ist. `377` ist der höchste Wert.
Verzögerung	Die Roundtrip-Zeit (RTT) der ExtraHop-Appliance, die mit dem Remote-Server kommuniziert, in Millisekunden.
Offset	Gibt an, wie weit die Uhr der ExtraHop-Appliance von der vom Server gemeldeten Uhrzeit entfernt ist. Der Wert kann positiv oder negativ sein und wird in Millisekunden angezeigt.
Jitter	Gibt den Unterschied zwischen zwei Stichproben in Millisekunden an.

Konfigurieren Sie die Systemzeit

Standardmäßig synchronisiert das ExtraHop-System die Systemzeit über die NTP-Server (*.extrahop.pool.ntp.org Netzwerk Time Protokoll). Wenn Ihre Netzwerkumgebung verhindert, dass das ExtraHop-System mit diesen Zeitservern kommuniziert, müssen Sie eine alternative Zeitserverquelle konfigurieren.

Bevor Sie beginnen

Wichtig: Konfigurieren Sie immer mehr als einen NTP-Server , um die Genauigkeit und Zuverlässigkeit der auf dem System gespeicherten Zeit zu erhöhen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken **Systemzeit**.

3. Klicken Sie **Zeit konfigurieren**.
4. Aus dem **Wählen Sie eine Zeitzone** Drop-down-Liste, wählen Sie Ihre Zeitzone aus.
5. Klicken Sie **Speichern und fortfahren**.
6. Auf dem Uhrzeit einrichten Seite, wählen Sie eine der folgenden Optionen:
   - Zeit manuell einstellen

     Hinweis Sie können die Zeit für Sensoren, die von einer Konsole oder RevealX 360 verwaltet werden, nicht manuell einstellen.
   - Zeit mit NTP-Server einstellen
7. Wählen Sie **Zeit mit NTP-Server einstellen** und klicken Sie dann **Wählen Sie**.

   Die ExtraHop-Zeitserver, `0.extrahop.pool.ntp.org`, `1.extrahop.pool.ntp.org`, `2.extrahop.pool.ntp.org`, und `3.extrahop.pool.ntp.org` erscheinen in den ersten vier Zeitserver standardmäßig Felder.
8. In der Zeitserver Felder, geben Sie die IP-Adresse oder den vollqualifizierten Domänenname (FQDN) für die Zeitserver ein.

   Sie können bis zu neun Zeitserver angeben.

   Hinweis Nachdem Sie den fünften Zeitserver hinzugefügt haben, klicken Sie auf **Server hinzufügen** um bis zu vier zusätzliche Timer-Serverfelder anzuzeigen.
9. Klicken Sie **Erledigt**.

Das NTP-Status In der Tabelle wird eine Liste von NTP-Servern angezeigt, die die Systemuhr synchron halten. Um die aktuelle Systemzeit auf einem Remoteserver zu synchronisieren, klicken Sie auf **Jetzt synchronisieren** knopf.

Herunterfahren oder Neustarten

Die Administrationseinstellungen bieten eine Schnittstelle zum Anhalten, Herunterfahren und Neustarten des ExtraHop-Systems und seiner Systemkomponenten. Für jede ExtraHop-Systemkomponente enthält die Tabelle einen Zeitstempel zur Anzeige der Startzeit.

- Starten Sie das System neu oder fahren Sie es herunter, um das ExtraHop-System anzuhalten oder herunterzufahren und neu zu starten.
- Starten Sie Bridge Status (nur Sensor) neu, um die ExtraHop Bridge-Komponente neu zu starten.
- Starten Sie Capture neu (nur Sensor), um die ExtraHop-Capture-Komponente neu zu starten.
- Starten Sie Portal Status neu, um das ExtraHop-Webportal neu zu starten.
- Starten Sie Scheduled Reports (nur Konsole) neu, um die ExtraHop-Komponente für geplante Berichte neu zu starten.

Sensormigration

Sie können Ihre gespeicherten Metriken, Anpassungen und Systemressourcen auf Ihren vorhandenen physischen ExtraHop migrieren Sensor zu einem neuen Sensor.

Hilfe auf dieser Seite

- Migrieren Sie einen ExtraHop-Sensor

Migrieren Sie einen ExtraHop-Sensor

Wenn Sie bereit sind, Ihr bestehendes zu aktualisieren Sensor, können Sie problemlos auf neue Hardware migrieren, ohne geschäftskritische Kennzahlen und zeitaufwändige Systemkonfigurationen zu verlieren.

Die folgenden Anpassungen und Ressourcen werden nicht gespeichert, wenn Sie ein Backup erstellen oder zu einem neuen Ziel migrieren.

- Lizenzinformationen für das System. Wenn Sie Einstellungen für ein neues Ziel wiederherstellen, müssen Sie das neue Ziel manuell lizenzieren.
- Präzise Paketerfassung. Sie können gespeicherte Paketerfassungen manuell herunterladen, indem Sie die Schritte unter Paketerfassungen anzeigen und herunterladen.
- Bei der Wiederherstellung einer virtuellen Konsole, die über eine getunnelte Verbindung von einem Sensor, der Tunnel muss nach Abschluss der Wiederherstellung und aller Anpassungen an der Konsole dafür neu eingerichtet werden Sensor muss manuell neu erstellt werden.
- Vom Benutzer hochgeladene TLS-Schlüssel für die Entschlüsselung des Datenverkehrs.
- Sichere Keystore-Daten, die Passwörter enthalten. Wenn Sie eine Sicherungsdatei auf demselben Ziel wiederherstellen, das das Backup erstellt hat, und der Keystore intakt ist, müssen Sie die Anmeldedaten nicht erneut eingeben. Wenn Sie jedoch eine Sicherungsdatei auf einem neuen Ziel wiederherstellen oder zu einem neuen Ziel migrieren, müssen Sie die folgenden Anmeldedaten erneut eingeben:
  - Alle SNMP-Community-Zeichenketten, die für die SNMP-Abfrage von Flow-Netzwerken bereitgestellt werden.
  - Jedes Bindkennwort, das für die Verbindung mit LDAP für Fernauthentifizierungszwecke bereitgestellt wird.
  - Jedes Passwort, das für die Verbindung zu einem SMTP-Server bereitgestellt wird, für den eine SMTP-Authentifizierung erforderlich ist.
  - Jedes Passwort, das für die Verbindung zu einem externen Datenspeicher angegeben wurde.
  - Jedes Passwort, das für den Zugriff auf externe Ressourcen über den konfigurierten globalen Proxy bereitgestellt wird.
  - Jedes Passwort, das für den Zugriff auf ExtraHop Cloud Services über den konfigurierten ExtraHop-Cloud-Proxy angegeben wurde.
  - Alle Authentifizierungsdaten oder Schlüssel, die zur Konfiguration von Open Data Stream-Zielen bereitgestellt werden.

Bevor du anfängst

Wichtig: Wenn der Quellsensor über einen externen Datenspeicher verfügt und der Datenspeicher auf einem SMB-Server konfiguriert ist, für den eine Passwortauthentifizierung erforderlich ist, wenden Sie sich an den ExtraHop-Support, um Sie bei der Migration zu unterstützen.

- Quelle und Ziel Sensoren muss dieselbe Firmware-Version ausführen.
- Migrieren Sie nur auf den gleichen Typ von Sensoren, wie RevealX Enterprise bis RevealX Enterprise. Wenn Sie zwischen Sensortypen (wie RevealX Enterprise zu RevealX 360) migrieren müssen, wenden Sie sich an Ihr ExtraHop-Vertriebsteam, um Unterstützung zu erhalten.
- Die Migration wird nur zwischen physischen Geräten unterstützt Sensoren. Virtuell Sensor Migrationen werden nicht unterstützt.
- Die Migration von einer früheren Serie zu einer neueren Serie wird nur unterstützt (Sie können beispielsweise nur eine EDA 6200 auf eine EDA 6300, EDA 9300 oder ähnliches migrieren.) Außerdem können Sie nur von einem kleineren Sensor auf einen größeren Sensor migrieren.

RevealX-Kompatibilitätsmatrix

Die unterstützten Migrationspfade sind in der folgenden Tabelle aufgeführt.

Quelle	Ziel							
	SEIT 1200	SEIT 6200	AB 820	SEIT 8320	SEIT 9200	SEIT 9300	VON 10200	VON 10300
SEIT 1200	JA	JA	JA	JA	JA	JA	JA	JA

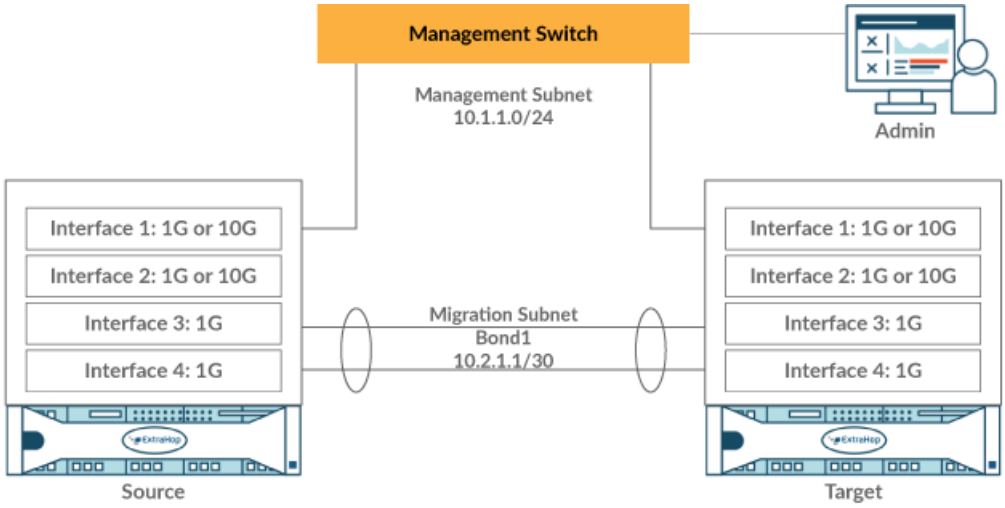
Quelle	Ziel							
SEIT 6200	NEIN	JA*	JA	JA	JA	JA	JA	JA
AB 8200	NEIN	NEIN	JA*	JA*	JA*	JA	JA	JA
SEIT 8320	NEIN	NEIN	NEIN	JA	NEIN	JA	NEIN	JA
SEIT 9200	NEIN	NEIN	NEIN	NEIN	JA*	JA	JA	JA
SEIT 9300	NEIN	NEIN	NEIN	NEIN	NEIN	JA	NEIN	JA
VON 10200	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA*	JA
VON 10300	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	NEIN	JA

*Die Migration wird nur unterstützt, wenn Quelle und Ziel Sensor wurden im Mai 2019 oder später hergestellt. Wenden Sie sich an den ExtraHop Support, um die Kompatibilität zu überprüfen.

Für Informationen über die frühere Performance Edition wenden Sie sich bitte an Ihren ExtraHop-Vertreter, um Hilfe zu erhalten.

Bereite die Quelle- und Zielsensoren vor

1. Folgen Sie den Anweisungen in der Bereitstellungsanleitung für Ihr Sensormodell, um den Zielsensor einzusetzen.
2. Registrieren der Zielsensor.
3. Stellen Sie sicher, dass das Ziel und die Quelle Sensor verwenden exakt dieselbe Firmware-Version. Sie können die aktuelle und frühere Firmware von der herunterladen ExtraHop Kundenportal.
4. Wählen Sie eine der folgenden Netzwerkmethoden, um zum Ziel zu migrieren Sensor.
   - (Empfohlen) Um die Migration so schnell wie möglich abzuschließen, verbinden Sie die Sensoren direkt mit 10G-Managementschnittstellen.
   - Erstellen Sie eine Bond-Schnittstelle (optional) der verfügbaren 1G-Managementschnittstellen. Verbinden Sie mit den entsprechenden Netzwerkkabeln den oder die verfügbaren Anschlüsse des Quellsensors direkt mit ähnlichen Anschlüssen am Zielsensor. Die folgende Abbildung zeigt eine Beispielkonfiguration mit gebundenen 1G-Schnittstellen.



Wichtig: Stellen Sie sicher, dass Ihre IP-Adresse und Subnetzkonfiguration auf beiden Sensoren den Verwaltungsdatenverkehr an Ihre Verwaltungs-Workstation und den Migrationsverkehr an den Direktlink weiterleiten.

- Migrieren Sie den Sensor über Ihr bestehendes Netzwerk. Die Quelle- und Zielsensoren müssen in der Lage sein, über Ihr Netzwerk miteinander zu kommunizieren. Beachten Sie , dass die Migration bei dieser Konfiguration erheblich länger dauern kann.

Erstellen Sie eine Bond-Schnittstelle (optional)
Folgen Sie den nachstehenden Anweisungen, um 1G-Schnittstellen zu verbinden. Durch das Erstellen einer Bond-Schnittstelle wird die Zeit reduziert, die benötigt wird, um die Migration über 1G-Schnittstellen abzuschließen.

Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

1. In der Netzwerkeinstellungen Abschnitt über die Quelle Sensor, klicken **Konnektivität**.
2. In der Einstellungen für die Bond-Schnittstelle Abschnitt, klicken **Bond-Schnittstelle erstellen**.
3. In der Mitglieder Abschnitt, wählen Sie die Mitglieder der Bond-Schnittstelle je nach Sensor Typ.

   Schließen Sie die aktuelle Verwaltungsschnittstelle, in der Regel Schnittstelle 1 oder Schnittstelle 3, nicht in die Bond-Schnittstelle ein.
4. Aus dem **Einstellungen übernehmen von** Wählen Sie in der Dropdownliste eines der Mitglieder der neuen Bond-Schnittstelle aus.
5. Für Art der Anleihe, wählen **Statisch**.
6. Aus dem **Hash-Richtlinie** Wählen Sie in der Dropdownliste eine der folgenden Optionen aus:
   - **Schicht 3+4** Richtlinie, die die Verteilung des Datenverkehrs auf die Schnittstellen gleichmäßiger verteilt. Diese Richtlinie entspricht jedoch nicht vollständig den 802.3ad-Standards.
   - **Ebene 2+3** Richtlinie, die den Datenverkehr weniger gleichmäßig verteilt und den 802.3ad-Standards entspricht.
7. Klicken Sie **Erstellen**.
8. Auf dem Konnektivität Seite, in der Bond-Schnittstellen Abschnitt, klicken **Bond-Schnittstelle 1**.
9. Aus dem **Schnittstellen-Modus** Dropdownliste, wählen **Verwaltung**.
10. Geben Sie die IPv4-Adresse, die Netzwerkmaske und das Gateway für Ihr Migrationsnetzwerk Netzwerk.
11. Klicken Sie **Speichern**.
12. Wiederholen Sie diesen Vorgang am Ziel Sensor.

Starten Sie die Migration
Der Abschluss der Migration kann mehrere Stunden dauern. Während dieser Zeit weder die Quelle noch das Ziel Sensor kann Daten sammeln. Der Migrationsvorgang kann nicht unterbrochen oder abgebrochen werden.

1. Loggen Sie sich in die Administrationseinstellungen der Quelle ein Sensor.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. Notieren Sie sich die IP-Adresse der Verwaltungsschnittstelle, der DNS-Server und aller statischen Routen. Sie werden diese Einstellungen auf dem Ziel konfigurieren, nachdem die Migration abgeschlossen ist.
4. In der Appliance-Einstellungen Abschnitt, klicken Sie **Appliance-Migration**.
5. In der Ziel-Appliance Geben Sie in dieses Feld die IP-Adresse der Schnittstelle ein, die Sie für die Migration auf dem Ziel konfiguriert haben.
6. In der Benutzerkennwort einrichten Feld, geben Sie das Passwort des Setup-Benutzers auf dem Ziel ein.

   Das Standardkennwort ist die Systemseriennummer des Zielsensors.
7. Klicken Sie **Weiter**.
8. Vergewissern Sie sich auf der Seite „Fingerabdruck bestätigen“, dass der auf dieser Seite angezeigte Fingerabdruck genau mit dem Fingerabdruck übereinstimmt, der auf der Seite „Fingerabdruck“ in den Verwaltungseinstellungen des Ziels angezeigt wird.

   Wenn die Fingerabdrücke nicht übereinstimmen, stellen Sie sicher, dass Sie den richtigen Hostnamen oder die richtige IP-Adresse des Ziels angegeben haben, das Sie in Schritt 5 eingegeben haben.
9. Klicken Sie **Migration starten**.
   Warten Sie, bis die Erfolgsmeldung der Migration angezeigt wird. Dies kann mehrere Stunden dauern. Während der Migration ist das ExtraHop-System auf dem Ziel nicht zugänglich. Wenn Sie versehentlich die Seite mit dem Migrationsstatus der Appliance auf der Quelle schließen, können Sie zu `https://<source hostname>/admin/appliance_migration_status/` um die Migration weiter zu überwachen.

   Wenn die Migration aus irgendeinem Grund fehlschlägt, starten Sie die Migration neu. Wenn die Migration weiterhin fehlschlägt, wenden Sie sich an den ExtraHop-Support, um Unterstützung zu erhalten.

   Hinweis: Das Ziel wird nach Abschluss der Migration automatisch neu gestartet.
10. Klicken Sie **Herunterfahren** um die Quelle auszuschalten.

    Wichtig: Um Sensor-ID-Konflikte zu vermeiden, schalten Sie den Quellsensor nicht ein, solange er mit demselben Netzwerk verbunden ist, in dem sich der Zielsensor befindet, es sei denn, Sie setzen den Sensor über das ExtraHop Rescue Media zurück.

Konfigurieren Sie den Zielsensor
Wenn Sensor Das Netzwerk wird nicht über DHCP konfiguriert. Stellen Sie sicher, dass die Konnektivitätseinstellungen aktualisiert werden, einschließlich aller zugewiesenen IP-Adressen, DNS-Server und statischen Routen. Verbindungen zu ExtraHop Konsolen, Recordstores und Packetstores in der Quelle Sensor werden automatisch auf dem Ziel eingerichtet Sensor wenn die Netzwerkeinstellungen konfiguriert sind.

1. Loggen Sie sich in die Administrationseinstellungen auf dem Ziel ein Sensor.
2. In der Netzwerkeinstellungen Abschnitt, klicken **Konnektivität**.
3. In der Schnittstellen Abschnitt, klicken Sie auf die Verwaltungsschnittstelle (normalerweise Schnittstelle 1 oder Schnittstelle 3, abhängig von Sensor Modell).
4. Geben Sie im Feld IPv4-Adresse die IP-Adresse der Quelle ein Sensor.
5. Konfigurieren Sie alle statischen Routen, die auf der Quelle konfiguriert wurden Sensor:

a) Klicken Sie **Routen bearbeiten**.
b) Fügen Sie alle erforderlichen Routeninformationen hinzu.
c) Klicken Sie **Speichern**.

6. Klicken Sie **Speichern**.

Nächste Schritte
Wenn Sie Schnittstelleneinstellungen ändern mussten, um die Migration mit gebündelten Schnittstellen durchzuführen, stellen Sie sicher, dass die Schnittstellenmodi erwartungsgemäß konfiguriert sind.

Stellen Sie alle zusätzlichen Einstellungen wieder her, die werden nicht automatisch wiederhergestellt.

Lizenz

Auf der Seite Lizenzverwaltung können Sie Lizenzen für Ihr ExtraHop-System einsehen und verwalten. Sie benötigen eine aktive Lizenz, um auf das ExtraHop-System zugreifen zu können, und Ihr System muss in der Lage sein, eine Verbindung zum ExtraHop-Lizenzserver herzustellen, um regelmäßige Updates und Check-ins über Ihren Lizenzstatus zu erhalten.

Weitere Informationen zu ExtraHop-Lizenzen finden Sie in der Häufig gestellte Fragen zur Lizenz.

Registrieren Sie Ihr ExtraHop-System

Diese Anleitung enthält Anweisungen zum Anwenden eines neuen Produktschlüssels und zur Aktivierung all Ihrer gekauften Module. Sie müssen über Rechte auf dem ExtraHop-System verfügen, um auf die Administrationseinstellungen zugreifen zu können.

Registrieren Sie das Gerät

Bevor Sie beginnen

Hinweis: Wenn Sie einen Sensor oder eine Konsole registrieren, können Sie optional den Produktschlüssel eingeben, nachdem Sie die EULA akzeptiert und sich beim ExtraHop-System angemeldet haben (`https://<extrahop_ip_address>/`).

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Lesen Sie die Lizenzvereinbarung und wählen Sie Ich stimme zu, und klicken Sie dann auf **Einreichen**.
3. Geben Sie auf dem Anmeldebildschirm Folgendes ein `Einrichten` für den Nutzernamen.
4. Wählen Sie für das Passwort eine der folgenden Optionen aus:
   - Geben Sie bei 1U- und 2U-Geräten die Seriennummer ein, die auf dem Etikett auf der Rückseite des Geräts aufgedruckt ist. Die Seriennummer finden Sie auch auf dem LCD-Display an der Vorderseite des Geräts in der `Info` Abschnitt.
   - Geben Sie für den EDA 1100 die im Feld angezeigte Seriennummer ein `Appliance info` Abschnitt des LCD-Menüs. Die Seriennummer ist auch auf der Unterseite des Geräts aufgedruckt.
   - Geben Sie für den EDA 1200 die Seriennummer ein, die auf der Rückseite des Geräts aufgedruckt ist.
   - Geben Sie für eine virtuelle Appliance in AWS die Instanz-ID ein. Dabei handelt es sich um die Zeichenfolge, die auf i- folgt (aber nicht auf i- selbst).
   - Geben Sie für eine virtuelle Appliance in GCP die Instanz-ID ein.
   - Geben Sie für alle anderen virtuellen Appliances Folgendes ein `Standard`.
5. klicken **Einloggen**.
6. In der Appliance-Einstellungen Abschnitt, klicken Sie **Lizenz**.
7. klicken **Lizenz verwalten**.
8. Wenn Sie einen Produktschlüssel haben, klicken Sie auf **Registriere dich** und geben Sie Ihren Produktschlüssel in das Feld ein.

Hinweis: Wenn Sie eine Lizenzdatei vom ExtraHop Support erhalten haben, klicken Sie auf **Lizenz verwalten**, klicken **Aktualisieren**, fügen Sie dann den Inhalt der Datei in das Lizenz eingeben Feld. Klicken Sie **Aktualisieren**.

9. klicken **Registriere dich**.

Nächste Schritte
Haben Sie weitere Fragen zur Lizenzierung von Werken von ExtraHop? Sehen Sie die Häufig gestellte Fragen zur Lizenz.

Problembehandlung bei der Lizenzserverkonnektivität

Für ExtraHop-Systeme, die für die Verbindung mit ExtraHop Cloud Services lizenziert und konfiguriert sind, erfolgt die Registrierung und Überprüfung über eine HTTPS-Anfrage an ExtraHop Cloud Services.

Wenn Ihr ExtraHop-System nicht für ExtraHop Cloud Services lizenziert ist oder noch nicht lizenziert ist, versucht das System, das System über eine DNS-TXT-Anfrage für zu registrieren `regions.hopcloud.extrahop.com` und eine HTTPS-Anfrage an alle ExtraHop Cloud Services-Regionen. Schlägt diese Anfrage fehl, versucht das System, über den DNS-Serverport 53 eine Verbindung zum ExtraHop-Lizenzserver herzustellen. Das folgende Verfahren ist hilfreich, um zu überprüfen, ob das ExtraHop-System über DNS mit dem Lizenzserver kommunizieren kann.

Öffnen Sie eine Terminalanwendung auf Ihrem Windows-, Linux- oder macOS-Client, der sich im selben Netzwerk wie Ihr ExtraHop-System befindet, und führen Sie den folgenden Befehl aus:

```
nslookup -type=NS d.extrahop.com
```

Wenn die Namensauflösung erfolgreich ist, wird eine Ausgabe ähnlich der folgenden angezeigt:

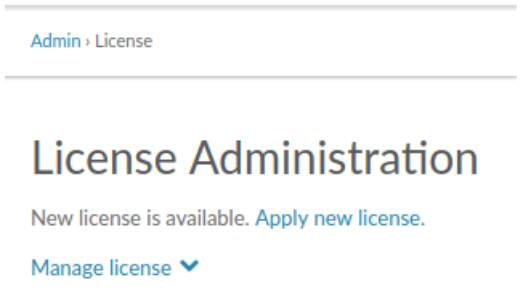
```
Non-authoritative answer:
d.extrahop.com  nameserver = ns0.use.d.extrahop.com.
d.extrahop.com  nameserver = ns0.usw.d.extrahop.com.
```

Wenn die Namensauflösung nicht erfolgreich ist, stellen Sie sicher, dass Ihr DNS-Server richtig konfiguriert ist, um nach dem `extrahop.com` Domäne.

Eine aktualisierte Lizenz anwenden

Wenn Sie ein neues Protokollmodul, einen neuen Dienst oder eine neue Funktion erwerben, ist die aktualisierte Lizenz automatisch im ExtraHop-System verfügbar. Sie müssen die aktualisierte Lizenz jedoch über die Verwaltungseinstellungen auf das System anwenden, damit die neuen Änderungen wirksam werden.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken **Lizenz**.
   Es wird eine Meldung über die Verfügbarkeit Ihrer neuen Lizenz angezeigt.



3. Klicken Sie **Neue Lizenz beantragen**.

Der Aufnahmevorgang wird neu gestartet, was einige Minuten dauern kann.

Hinweis: Wenn Ihre Lizenz nicht automatisch aktualisiert wird, Problembehandlung bei der Lizenzserverkonnektivität oder wenden Sie sich an den ExtraHop Support.

Eine Lizenz aktualisieren

Wenn ExtraHop Support Ihnen eine Lizenzdatei zur Verfügung stellt, können Sie diese Datei auf Ihrem Gerät installieren, um die Lizenz zu aktualisieren.

Hinweis: Wenn Sie den Produktschlüssel für Ihr Gerät aktualisieren möchten, müssen Sie registrieren Sie Ihr ExtraHop-System.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken Sie **Lizenz**.
3. Klicken Sie Lizenz verwalten.
4. Klicken Sie **Aktualisieren**.
5. In der Lizenz eingeben Textfeld, geben Sie die Lizenzinformationen für das Modul ein.

   Fügen Sie den Lizenztext ein, den Sie vom ExtraHop Support erhalten haben. Stellen Sie sicher, dass Sie den gesamten Text angeben, einschließlich der `BEGIN` und `END` Zeilen, wie im folgenden Beispiel gezeigt:

   ```
   -----BEGIN EXTRAHOP LICENSE-----
   serial=ABC123D;
   dossier=1234567890abcdef1234567890abcdef;
   mod_cifs=1;
   mod_nfs=1;
   mod_amf=0;
   live_capture=1;
   capture_upload=1;
   ...
   ssl_decryption=0;
   +++;
   ABCabcDE/FGHIjklm12nopqrstuvwXYZAB12345678abcde901abCD;
   12ABCDEFG1HIJklmnOP+1aA=;
   =abcd;
   -----END EXTRAHOP LICENSE-----
   ```
6. Klicken Sie **Aktualisieren**.

Festplatten

Die Seite Festplatten zeigt eine Übersicht der Laufwerke auf dem ExtraHop-System und listet deren Status auf. Anhand dieser Informationen können Sie feststellen, ob Laufwerke installiert oder ausgetauscht werden müssen. Automatische Systemzustandsprüfungen und E-Mail-Benachrichtigungen (falls aktiviert) können rechtzeitig über eine Festplatte informieren, die sich in einem heruntergefahrenen Zustand befindet. Bei Systemzustandsprüfungen werden Festplattenfehler oben auf der Seite „Einstellungen“ angezeigt.

Selbstverschlüsselnde Festplatten (SEDs)

Für Sensoren, die selbstverschlüsselnde Festplatten (SEDs) enthalten, ist der `Hardware Disk Encryption` Status kann gesetzt werden auf `Disabled` oder `Enabled`. Dieser Status wurde auf gesetzt `Unsupported` für Sensoren, die keine SEDs enthalten.

Diese Sensoren unterstützen SEDs:

- SEIT 9300

- VON 10300
- Intrusion Detection System 980

Hinweise zur Konfiguration von SEDs finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

ÜBERFALL

Hilfe beim Austauschen einer RAID 0-Festplatte oder beim Installieren eines SSD-Laufwerks finden Sie in den folgenden Anweisungen. Die RAID 0-Anweisungen gelten für die folgenden Festplattentypen:

- Datenspeicher
- Paketerfassung
- Firmware

Versuchen Sie nicht, das Laufwerk in Steckplatz 0 zu installieren oder auszutauschen, es sei denn, Sie werden vom ExtraHop-Support dazu aufgefordert.

Hinweis Stellen Sie sicher, dass Ihr Gerät über einen RAID-Controller verfügt, bevor Sie das folgende Verfahren ausführen. Wenn Sie unsicher sind, wenden Sie sich an ExtraHop-Unterstützung. Eine dauerhaft beschädigte Festplatte kann mit diesem Verfahren möglicherweise nicht ausgetauscht werden.

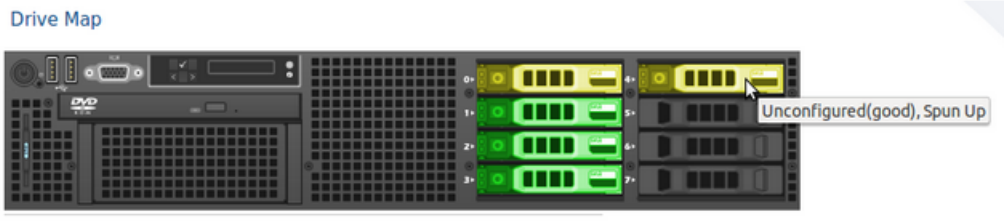
Ersetzen Sie eine RAID 0-Festplatte

1. Notieren Sie in der E-Mail-Benachrichtigung zum Systemstatus, auf welchem Computer die problematische Festplatte installiert ist.
2. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
3. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
4. Unter dem Abschnitt für den Festplattentyp (z. B. **Datenspeicher**), suchen Sie die problematische Festplatte und notieren Sie sich die Steckplatznummer.

   Klicken Sie **Details zur RAID-Festplatte** um mehr Details anzuzeigen.

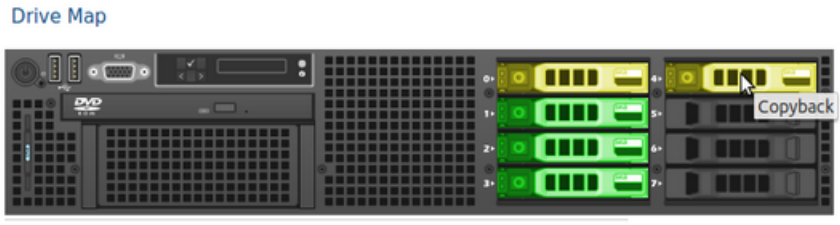
   Wichtig: Bewahren Sie die ausgefallene Festplatte auf, bis die Daten erfolgreich auf die neue Festplatte kopiert wurden.
5. Legen Sie eine identische Festplatte in einen verfügbaren Steckplatz ein.

   Das System erkennt die neue Festplatte und fügt eine neue Zeile (Disk Error Action) mit einem Link zum Ersetzen der defekten Festplatte hinzu.
6. Überprüfen Sie die neuen Festplatteninformationen:
   - Unter **Unbenutzte Festplatten** Stellen Sie auf der Seite Festplattendetails sicher, dass die neue Festplatte dieselbe Größe, Geschwindigkeit und denselben Typ hat wie die Festplatte, die ausgetauscht wird.
   - Fahren Sie mit der Maus über die alten und neuen Festplatten in der Drive Map. Die neue Festplatte zeigt die Meldung an"`Unconfigured(good), Spun Up`."



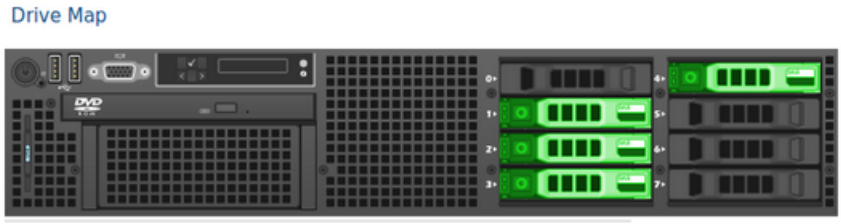
7. Klicken Sie unter dem Abschnitt für den Festplattentyp auf **Durch Diskette im Steckplatz #n ersetzen** in der Aktion „Festplattenfehler" Reihe.

Die Daten beginnen zu kopieren. In der Zeile Copy Status wird der Fortschritt angezeigt. Wenn Sie in der Drive Map mit der Maus über die Festplatte fahren, wird der Status angezeigt.



8. Stellen Sie nach Abschluss des Kopiervorgangs sicher, dass der Kopiervorgang erfolgreich war:
   - **Einstellungen** Auf der Schaltfläche und auf der Einstellungsseite werden keine Fehlermeldungen mehr angezeigt.
   - Auf der Festplattenseite wird die alte Festplatte im Abschnitt Unbenutzter Datenträger angezeigt
9. Entfernen Sie die alte Festplatte.

   Die Drive Map zeigt die neue Festplatte jetzt grün an.

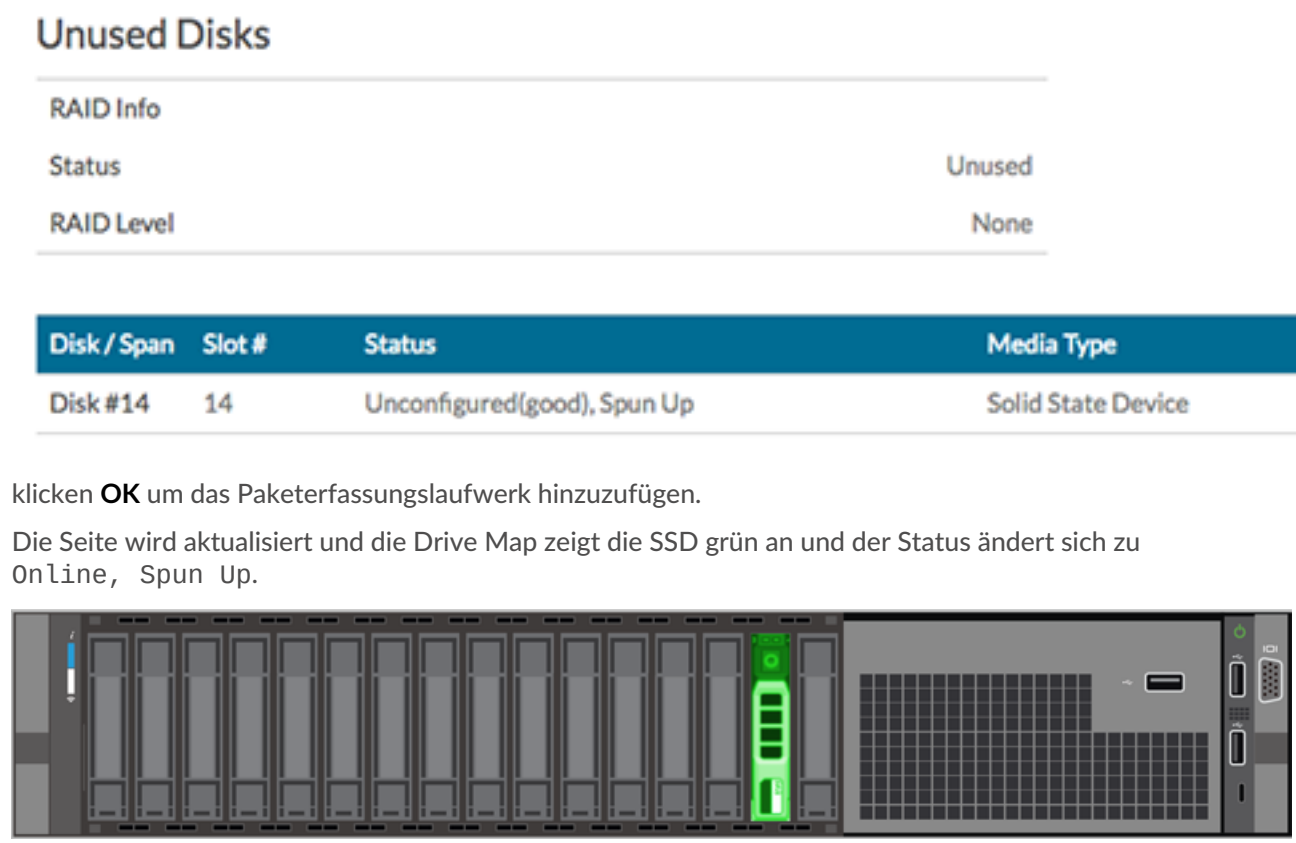


Installieren Sie eine neue Paketerfassungsdiskette

1. In der Einstellungen der Appliance Abschnitt, klicken **Festplatten**.
   Wenn in der Laufwerksübersicht der Steckplatz, in dem die SSD installiert ist, rot angezeigt wird, müssen Sie die SSD austauschen.
2. Stecken Sie das SSD-Laufwerk in den Steckplatz, in dem die vorherige SSD installiert war, und warten Sie, bis die LED am Laufwerk grün leuchtet.
3. Aktualisieren Sie in den Administrationseinstellungen den Browser.

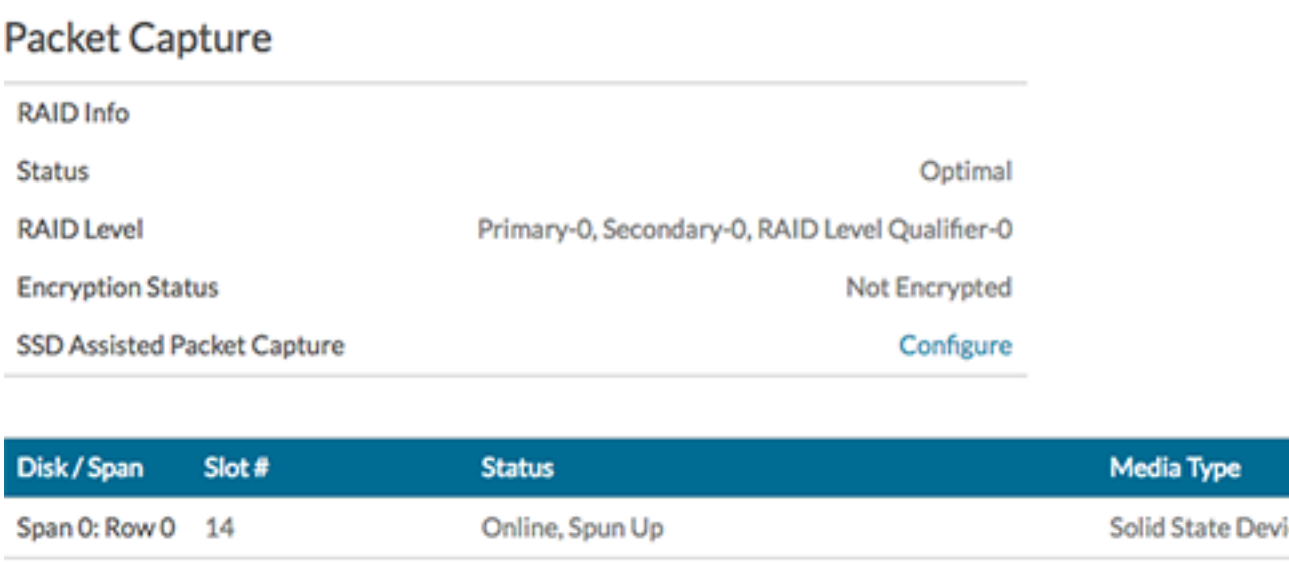
   In der Laufwerksübersicht wird der SSD-Steckplatz gelb angezeigt, da das Laufwerk nicht konfiguriert ist.

4. Neben SSD-gestützte Paketerfassung, klicken **Aktivieren**.



5. klicken **OK** um das Paketerfassungslaufwerk hinzuzufügen.

   Die Seite wird aktualisiert und die Drive Map zeigt die SSD grün an und der Status ändert sich zu `Online, Spun Up`.



Hinweis: Wenn das SSD-Laufwerk entfernt und wieder eingesetzt wird, können Sie es erneut aktivieren. Dieser Vorgang erfordert eine Neuformatierung der Festplatte, wodurch alle Daten gelöscht werden.

Spitzname der Konsole

Standardmäßig ist Ihr ExtraHop Konsole wird auf angeschlossenen Sensoren anhand seines Hostnamens identifiziert. Sie können jedoch optional einen benutzerdefinierten Namen konfigurieren, um Ihre Konsole.

Wählen Sie aus den folgenden Optionen, um den Anzeigenamen zu konfigurieren:

- Wählen **Benutzerdefinierten Spitznamen anzeigen** und geben Sie den Namen in das Feld ein, das Sie für diese Konsole anzeigen möchten.
- Wählen **Hostnamen anzeigen** um den für diese Konsole konfigurierten Hostnamen anzuzeigen.

Meldung auf dem Anmeldebildschirm

PCAP konfigurieren

Mit der Paketerfassung können Sie Datenpakete aus Ihrem Netzwerkverkehr sammeln, speichern und abrufen. Sie können eine Paketerfassungsdatei zur Analyse in einem Drittanbieter-Tool wie Wireshark herunterladen. Pakete können überprüft werden, um Netzwerkprobleme zu diagnostizieren und zu lösen und um sicherzustellen , dass die Sicherheitsrichtlinien eingehalten werden.

Durch Hinzufügen einer Paketerfassungsdiskette zum ExtraHop Sensor, können Sie die an Ihr ExtraHop-System gesendeten Rohdaten speichern. Diese Festplatte kann zu Ihrer virtuellen Festplatte hinzugefügt werden Sensor oder eine SSD, die in Ihrem physischen Gerät installiert ist Sensor.

Diese Anweisungen gelten nur für ExtraHop-Systeme, die über eine Precision Paket Capture Disk verfügen. Informationen zum Speichern von Paketen auf einer ExtraHop PacketStore-Appliance finden Sie in der Anleitungen zur Bereitstellung von Packetstore.

Wichtig: Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

Päckchen schneiden

Standardmäßig speichert der Packetstore ganze Pakete. Wenn Pakete noch nicht in Scheiben geschnitten sind, können Sie den Sensor so konfigurieren, dass er Pakete speichert, die auf eine feste Anzahl von Byte aufgeteilt sind, um den Datenschutz und das Lookback zu verbessern.

Weitere Informationen zur Konfiguration dieser Funktion in Ihrer laufenden Konfigurationsdatei erhalten Sie vom ExtraHop-Support.

PCAP aktivieren

Ihr ExtraHop-System muss für die PCAP lizenziert und mit einer dedizierten Speicherplatte konfiguriert sein. Körperlich Sensoren benötigen eine SSD-Speicherfestplatte und virtuelle Sensoren benötigen eine Festplatte, die auf Ihrem Hypervisor konfiguriert ist.

Bevor Sie beginnen
Stellen Sie sicher, dass Ihr ExtraHop-System für Packet Capture lizenziert ist, indem Sie sich in den Administrationseinstellungen anmelden und auf **Lizenz**. Die Paketerfassung ist unter Funktionen aufgeführt und **Aktiviert** sollte erscheinen.

Wichtig: Der Erfassungsvorgang wird neu gestartet, wenn Sie die Paketerfassungsdiskette aktivieren.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Appliance-Einstellungen Abschnitt, klicken **Festplatten**.
3. Abhängig von deinem Sensor Typ- und Menüoptionen, konfigurieren Sie die folgenden Einstellungen.
   - Für physische Sensoren klicken Sie auf **Aktiviere** neben SSD Assisted Packet Capture, und klicken Sie dann auf **OK**.
   - Stellen Sie für virtuelle Sensoren sicher, dass `running` wird in der Spalte Status angezeigt und die Festplattengröße, die Sie für die PCAP konfiguriert haben, wird in der Spalte Größe angezeigt. Klicken Sie **Aktiviere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette, und klicken Sie dann auf **OK**.

Nächste Schritte

Ihre Paketerfassungsdiskette ist jetzt aktiviert und bereit, Pakete zu speichern. Klicken Sie **Konfiguriere** wenn Sie die Festplatte verschlüsseln oder konfigurieren möchten weltweite oder Präzisionspaket erfasst.

Verschlüsseln Sie die Paketerfassungsdiskette

Paketerfassungsfestplatten können mit einer 256-Bit-AES-Verschlüsselung gesichert werden.

Hier sind einige wichtige Überlegungen, bevor Sie eine Paketerfassungsdiskette verschlüsseln:

- Sie können eine Paketerfassungsdiskette nicht entschlüsseln, nachdem sie verschlüsselt wurde. Sie können die Verschlüsselung löschen, aber die Festplatte ist formatiert und alle Daten werden gelöscht.
- Sie können eine verschlüsselte Festplatte sperren, um jeglichen Lese- oder Schreibzugriff auf gespeicherte Paketerfassungsdateien zu verhindern. Wenn das ExtraHop-System neu gestartet wird, werden verschlüsselte Festplatten automatisch gesperrt und bleiben gesperrt, bis sie mit der Passphrase entsperrt werden. Unverschlüsselte Festplatten können nicht gesperrt werden.
- Sie können eine verschlüsselte Festplatte neu formatieren, aber alle Daten werden dauerhaft gelöscht. Sie können eine gesperrte Festplatte neu formatieren, ohne die Festplatte zuerst zu entsperren.
- Sie können eine sichere Löschung (oder Systemlöschung) aller Systemdaten durchführen. Anweisungen finden Sie in der Medienleitfaden für ExtraHop Rescue.

Warnung: Wenn Sie eine Paketerfassungsdiskette verschlüsseln, werden alle auf der Festplatte gespeicherten Pakete gelöscht.

Wichtig: Systeme mit selbstverschlüsselnden Festplatten (SEDs) können nicht für die Softwareverschlüsselung bei Paketerfassungen konfiguriert werden. Informationen zur Aktivierung der Sicherheit auf diesen Systemen finden Sie unter Konfigurieren Sie selbstverschlüsselnde Festplatten (SEDs).

1. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Sensortyp eine der folgenden Optionen aus.
   - Für virtuelle Sensoren klicken Sie auf **Konfiguriere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette.
   - Für physische Sensoren klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.
3. Klicken Sie **Festplatte verschlüsseln**.
4. Geben Sie einen Festplattenverschlüsselungsschlüssel aus einer der folgenden Optionen an:
   - Geben Sie eine Passphrase in die Felder Passphrase und Bestätigen ein.
   - Klicken Sie **Wählen Sie Datei** und wählen Sie eine Verschlüsselungsschlüsseldatei aus.
5. Klicken Sie **Verschlüsseln**.

Nächste Schritte
Sie können den Festplattenverschlüsselungsschlüssel ändern, indem Sie zur Seite Festplatten zurückkehren und auf **Konfiguriere** und dann **Festplattenverschlüsselungsschlüssel ändern**.

Formatieren Sie die Paketerfassungsdiskette

Sie können eine verschlüsselte Paketerfassungsdiskette so formatieren, dass alle Paketerfassungen dauerhaft entfernt werden. Beim Formatieren einer verschlüsselten Festplatte wird die Verschlüsselung aufgehoben. Wenn Sie eine unverschlüsselte Paketerfassungsdiskette formatieren möchten, müssen Sie die Festplatte entfernen und die Festplatte dann erneut aktivieren.

Warnung: Diese Aktion kann nicht rückgängig gemacht werden.

1. In der Appliance-Einstellungen Abschnitt, klicken Sie **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.

- Für virtuelle Sensoren klicken Sie auf **Konfiguriere** in der Aktionen Spalte der Zeile für die Paketerfassungsdiskette.
- Für physische Sensoren klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.

3. Klicken Sie **Festplattenverschlüsselung löschen**.
4. Klicken Sie **Format**.

Entfernen Sie die Paketerfassungsdiskette

Wenn Sie eine Paketerfassungsdiskette austauschen möchten, müssen Sie die Festplatte zuerst aus dem System entfernen. Wenn eine Paketerfassungsdiskette aus dem System entfernt wird, werden alle Daten auf der Festplatte dauerhaft gelöscht.

Zum Entfernen des Datenträgers muss eine Formatoption ausgewählt werden. Bei physischen Geräten können Sie die Festplatte nach Abschluss dieses Vorgangs sicher aus der Appliance entfernen.

1. In der Appliance-Einstellungen Abschnitt, klicken **Festplatten**.
2. Wählen Sie auf der Seite Festplatten je nach Appliance-Plattform eine der folgenden Optionen aus.
   - Für virtuelle Appliances klicken Sie auf **Konfiguriere** neben Triggered Packet Capture.
   - Für physische Geräte klicken Sie auf **Konfiguriere** neben SSD Assisted Packet Capture.
3. Klicken Sie **Festplatte entfernen**.
4. Wählen Sie eine der folgenden Formatoptionen aus:
   - **Schnelles Format**
   - **Sicheres Löschen**
5. Klicken Sie **entfernen**.

Konfigurieren Sie eine globale PCAP

Eine globale PCAP erfasst jedes Paket, das an das ExtraHop-System gesendet wird, für die Dauer, die den Kriterien entspricht.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Paketerfassung Abschnitt, klicken **Globale Paketerfassung**.

   Bei der Konfiguration der PCAP müssen Sie nur die gewünschten Kriterien für die Paketerfassung angeben.
3. In der Name Feld, geben Sie einen Namen ein, um die Paketerfassung zu identifizieren.
4. In der Max. Pakete Feld, geben Sie die maximale Anzahl der zu erfassenden Pakete ein.
5. In der Max. Byte Feld, geben Sie die maximale Anzahl der zu erfassenden Byte ein.
6. In der Max. Dauer (Millisekunden) Feld, geben Sie die maximale Dauer der PCAP in Millisekunden ein.

   ExtraHop empfiehlt den Standardwert 1000 (1 Sekunde). Der Maximalwert beträgt bis zu 60000 Millisekunden (1 Minute).
7. In der Schnappschuss Feld, geben Sie die maximale Anzahl der pro Frame kopierten Byte ein.

   Der Standardwert ist 96 Byte, aber Sie können diesen Wert auf eine Zahl zwischen 1 und 65535 setzen.
8. Klicken Sie **Starten**.

   Hinweis: Notieren Sie sich den Zeitpunkt, zu dem Sie mit der Erfassung beginnen, um das Auffinden der Pakete zu erleichtern.
9. Klicken Sie **Stopp** um die Paketerfassung zu stoppen, bevor eine der Höchstgrenzen erreicht wird.

Laden Sie Ihre PCAP herunter.

- Klicken Sie auf RevealX Enterprise-Systemen auf **Pakete** aus dem Hauptmenü und dann auf **PCAP herunterladen**.

  Um das Auffinden Ihrer PCAP zu erleichtern, klicken und ziehen Sie auf die Zeitleiste der Paketabfrage, um den Zeitraum auszuwählen, in dem Sie die PCAP gestartet haben.
- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen, klicken **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Paketerfassung.

Konfigurieren Sie eine präzise PCAP

Für präzise Paketerfassungen sind ExtraHop-Trigger erforderlich, mit denen Sie nur die Pakete erfassen können, die Ihren Spezifikationen entsprechen. Trigger sind hochgradig anpassbarer benutzerdefinierter Code, der bei definierten Systemereignissen ausgeführt wird.

Bevor Sie beginnen
Die Paketerfassung muss auf Ihrem ExtraHop-System lizenziert und aktiviert sein.

Es wird empfohlen, dass Sie sich mit dem Schreiben von Triggern vertraut machen, bevor Sie eine präzise PCAP konfigurieren. Hier sind einige Ressourcen, die Ihnen helfen, mehr über ExtraHop Triggers zu erfahren:

- Triggerkonzepte
- Einen Auslöser erstellen
- Trigger-API-Referenz
- Gehen Sie durch: Initiieren Sie präzise Paketerfassungen, um Bedingungen ohne Fenster zu analysieren

Im folgenden Beispiel erfasst der Auslöser einen HTTP-Flow mit dem Namen `HTTP host <hostname>` und stoppt die Erfassung, nachdem maximal 10 Pakete gesammelt wurden.

1. Klicken Sie auf das Symbol Systemeinstellungen und klicken Sie dann **Trigger**.
2. klicken **Erstellen**.
3. Geben Sie einen Namen für den Auslöser ein und wählen Sie die Ereignisse HTTP_REQUEST und HTTP_RESPONSE aus.
4. Geben Sie den folgenden Triggercode in den rechten Bereich ein oder fügen Sie ihn ein.

```
Flow.captureStart("HTTP host " + HTTP.host, {maxPackets: 10});
```

5. Weisen Sie den Auslöser einem Gerät oder einer Gruppe von Geräten zu.

   Warnung: Das Ausführen von Triggern auf unnötigen Geräten und Netzwerken erschöpft die Systemressourcen. Minimieren Sie die Auswirkungen auf die Leistung, indem Sie einen Auslöser nur den spezifischen Quellen zuweisen, aus denen Sie Daten erheben müssen.
6. Wählen **Auslöser aktivieren**.
7. Klicken Sie **Speichern**.

Nächste Schritte
Laden Sie die Paketerfassungsdatei herunter.

- Klicken Sie auf RevealX Enterprise-Systemen auf **Rekorde** aus dem oberen Menü. Wählen **Paketerfassung** aus dem Typ des Datensatzes Dropdownliste. Nachdem die mit Ihrer PCAP verknüpften Datensätze angezeigt werden, klicken Sie auf das Symbol Pakete, und klicken Sie dann auf **PCAP herunterladen**.
- Klicken Sie auf ExtraHop Performance-Systemen auf das Symbol Systemeinstellungen, klicken **Die gesamte Verwaltung**, und klicken Sie dann auf **Paketerfassungen anzeigen und herunterladen** im Abschnitt Paketerfassung.

Paketerfassungen anzeigen und herunterladen

Wenn Sie Paketerfassungen auf einer virtuellen Festplatte oder auf einer SSD-Festplatte in Ihrem gespeichert haben Sensor, Sie können diese Dateien auf der Seite „Paketerfassung anzeigen“ in den Administrationseinstellungen verwalten. Sehen Sie sich für RevealX-Systeme und ExtraHop-Paketstores die Seite Pakete an.

Der Abschnitt Paketerfassungen anzeigen und herunterladen wird nur auf ExtraHop Performance-Systemen angezeigt. Auf RevealX-Systemen werden Precision-Paketerfassungsdateien gefunden, indem Datensätze nach dem Datensatztyp für die PCAP durchsucht werden.

- klicken **Einstellungen für die PCAP konfigurieren** um gespeicherte Paketerfassungen nach der angegebenen Dauer (in Minuten) automatisch zu löschen.
- Sehen Sie sich Statistiken über Ihre Paketerfassungsdiskette an.
- Geben Sie Kriterien zum Filtern von Paketerfassungen an und begrenzen Sie die Anzahl der in der Paketerfassungsliste angezeigten Dateien.
- Wählen Sie eine Datei aus der Paketerfassungsliste aus und laden Sie die Datei dann herunter oder löschen Sie sie.

  Hinweis Sie können keine einzelnen Paketerfassungsdateien von RevealX-Systemen löschen.

Plattenladen

Sie können vom ExtraHop-System geschriebene Datensätze auf Transaktionsebene an einen unterstützten Recordstore senden und diese Datensätze dann von der Datensatzseite oder der REST-API auf Ihrer Konsole abfragen und Sensoren.

Erfahre mehr über ExtraHop Records

- Konzepte aufzeichnen

Datensätze von ExtraHop an Google BigQuery senden

Sie können Ihr ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Google BigQuery-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen. Datensätze in BigQuery-Datensatzspeichern laufen nach 90 Tagen ab.

Bevor Sie beginnen

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen die BigQuery-Projekt-ID
- Sie benötigen die Anmeldeinformationsdatei (JSON) von Ihrem BigQuery-Dienstkonto. Für das Dienstkonto sind die Rollen BigQuery Data Editor, BigQuery Data Viewer und BigQuery User erforderlich.
- Für den Zugriff auf den cloudbasierten Recordstore, der in RevealX Standard Investigation enthalten ist, benötigen Sie Sensoren muss in der Lage sein, auf ausgehendes TCP 443 (HTTPS) auf diese vollständig qualifizierten Domainnamen zuzugreifen:
  - `bigquery.googleapis.com`
  - `bigquerystorage.googleapis.com`
  - `oauth2.googleapis.com`
  - `www.googleapis.com`
  - `www.mtls.googleapis.com`
  - `iamcredentials.googleapis.com`

  Sie können auch die öffentlichen Leitlinien von Google zu folgenden Themen lesen Berechnung möglicher IP-Adressbereiche für googleapis.com.
- Wenn Sie die BigQuery-Recordstore-Einstellungen mit der Google Cloud-Workload-Identitätsverbundauthentifizierung konfigurieren möchten, benötigen Sie die Konfigurationsdatei aus Ihrem Workload-Identitätspool.

  Hinweis: Der Workload-Identitätsanbieter muss so eingerichtet sein, dass er als Antwort auf eine Anfrage mit Client-Anmeldeinformationen ein vollständig gültiges OIDC-ID-Token bereitstellt. Weitere Informationen zum Workload-Identitätsverbund finden Sie unter https://cloud.google.com/iam/docs/workload-identity-federation.

BigQuery als Recordstore aktivieren

Führen Sie diesen Vorgang an allen angeschlossenen ExtraHop-Sensoren und der Konsole durch.

Hinweis: Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem ExtraHop-Recordstore werden automatisch zu BigQuery umgeleitet. Es ist keine weitere Konfiguration erforderlich.

Wichtig: Wenn Ihr ExtraHop-System eine Konsole enthält, konfigurieren Sie alle Appliances mit denselben Recordstore-Einstellungen oder übertragen Sie die Verwaltung, um die Einstellungen von der Konsole aus zu verwalten.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Plattenladen**.
3. Wählen **BigQuery als Recordstore aktivieren**.

   Wichtig: Wenn Sie von einem verbundenen ExtraHop-Recordstore zu BigQuery migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
4. In der Projekt-ID Feld, geben Sie die ID für Ihr BigQuery-Projekt ein.

   Sie finden die Projekt-ID in der BigQuery API-Konsole.
5. In der JSON-Anmeldeinformationsdatei Feld, klicken **Wählen Sie Datei** und wählen Sie eine der folgenden Dateien aus:

   - Die Anmeldeinformationsdatei, die von Ihrem gespeichert wurde BigQuery-Dienstkonto.

     Informationen zum Erstellen eines Dienstkontos und zum Generieren eines Dienstkontoschlüssels finden Sie in der Google Cloud-Dokumentation.

     Wichtig: Erstellen Sie Ihr Dienstkonto mit den folgenden BigQuery-Rollen:

     - BigQuery-Dateneditor
     - BigQuery-Datenviewer
     - BigQuery-Benutzer
   - Die Konfigurationsdatei aus Ihrem Workload-Identitätspool.
6. Optional: Wenn Sie im vorherigen Schritt die Konfigurationsdatei aus Ihrem Workload-Identitätspool ausgewählt haben, wählen Sie **Authentifizieren Sie sich über den lokalen Identitätsanbieter für Workload Identity Federation** und geben Sie die Anmeldedaten Ihres Identitätsanbieters in die folgenden Felder ein:

   - **Token-URL**
   - **Kunden-ID**
   - **Geheimer Kunde**
7. Klicken Sie **Verbindung testen** um zu überprüfen, ob Ihr Sensor mit dem BigQuery-Server kommunizieren kann.
8. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde**.

Wichtig: Ändern oder löschen Sie die Tabelle in BigQuery, in der die Datensätze gespeichert sind, nicht. Durch das Löschen der Tabelle werden alle gespeicherten Datensätze gelöscht.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.

2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.

Datensätze von ExtraHop an Splunk senden

Sie können das ExtraHop-System so konfigurieren, dass Datensätze auf Transaktionsebene zur Langzeitspeicherung an einen Splunk-Server gesendet werden, und diese Datensätze dann vom ExtraHop-System und der ExtraHop-REST-API abfragen.

Hier sind einige Überlegungen zum Senden von Datensätzen von ExtraHop an Splunk:

- Alle Trigger, die für das Senden von Datensätzen konfiguriert sind `commitRecord` zu einem Recordstore werden automatisch zum Splunk-Server umgeleitet. Es ist keine weitere Konfiguration erforderlich.
- Wenn Sie von einem verbundenen ExtraHop-Recordstore zu Splunk migrieren, können Sie nicht mehr auf die im Recordstore gespeicherten Datensätze zugreifen.
- Wenn Sie ExtraHop-Daten wie Metriken und Erkennungen in einer Splunk-Oberfläche anzeigen und analysieren möchten, konfigurieren Sie eine Splunk oder Splunk SOAR Integration.

Splunk als Recordstore aktivieren

Führen Sie dieses Verfahren auf allen angeschlossenen ExtraHop-Systemen durch.

Wichtig: Wenn Ihr ExtraHop-System eine Konsole oder RevealX 360 enthält, konfigurieren Sie alle Sensoren mit denselben Recordstore-Einstellungen oder Übertragungsmanagement, um die Einstellungen von der Konsole oder RevealX 360 aus zu verwalten.

Bevor Sie beginnen

- Auf jeder Konsole und allen angeschlossenen Sensoren muss dieselbe ExtraHop-Firmware-Version ausgeführt werden.
- Sie benötigen Version 7.0.3 oder höher von Splunk Enterprise und ein Benutzerkonto mit Administratorrechte.
- Sie müssen den Splunk HTTP Event Collector konfigurieren, bevor Ihr Splunk-Server ExtraHop-Datensätze empfangen kann. Sehen Sie die Splunk HTTP-Event-Collector Dokumentation für Anweisungen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Wählen **Splunk als Recordstore aktivieren**.
4. In der Aufnahmeziel aufzeichnen Abschnitt, füllen Sie die folgenden Felder aus:

   • **Splunk Ingest Host:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **Port für HTTP-Event-Collector:** Der Port, über den der HTTP Event Collector Datensätze senden soll.

   • **HTTP-Event-Collector-Token:** Das Authentifizierungstoken, das Sie erstellt in Splunk für den HTTP Event Collector.
5. In der Ziel der Datensatzabfrage Abschnitt, füllen Sie die folgenden Felder aus:

   • **Splunk-Abfragehost:** Der Hostname oder die IP-Adresse Ihres Splunk-Servers.

   • **REST-API-Port:** Der Port, über den Datensatzabfragen gesendet werden sollen.

• **Methode der Authentifizierung:** Die Authentifizierungsmethode, die von Ihrer Splunk-Version abhängt.

Für Splunk-Versionen nach 7.3.0 wählen Sie **Authentifizieren Sie sich mit einem Token**, und fügen Sie dann Ihr Splunk-Authentifizierungstoken ein. Anweisungen zum Erstellen eines Authentifizierungstokens finden Sie in der Splunk-Dokumentation.

Für Splunk-Versionen vor 7.3.0 wählen Sie **Authentifizieren Sie sich mit Benutzername und Passwort**, und geben Sie dann Ihre Splunk-Anmeldeinformationen Anmeldedaten.

6. Löschen Sie das **Zertifikatsüberprüfung erforderlich** Kontrollkästchen, wenn für Ihre Verbindung kein gültiges TLS-Zertifikat erforderlich ist.

   Hinweis: Sichere Verbindungen zum Splunk-Server können verifiziert werden durch vertrauenswürdige Zertifikate die Sie in das ExtraHop-System hochladen.

7. In der Name des Indexes Feld, geben Sie den Namen des Splunk-Indexes ein , in dem Sie Datensätze speichern möchten.

   Der Standardindex auf Splunk heißt `main`Wir empfehlen jedoch, dass Sie einen separaten Index für Ihre ExtraHop-Datensätze erstellen und den Namen dieses Indexes eingeben. Anweisungen zum Erstellen eines Indexes finden Sie in der Splunk-Dokumentation.

8. (ExtraHop Sensor (nur) Klicken **Verbindung testen** um zu überprüfen , ob das ExtraHop-System Ihren Splunk-Server erreichen kann.

9. Klicken Sie **Speichern**.

Nachdem Ihre Konfiguration abgeschlossen ist, können Sie im ExtraHop-System nach gespeicherten Datensätzen abfragen, indem Sie auf **Rekorde** aus dem oberen Menü.

Recordstore-Einstellungen übertragen

Wenn du einen ExtraHop hast Konsole Wenn Sie an Ihre ExtraHop-Sensoren angeschlossen sind, können Sie die Recordstore-Einstellungen auf dem Sensor konfigurieren und verwalten oder die Verwaltung der Einstellungen an den Konsole. Durch die Übertragung und Verwaltung der Recordstore-Einstellungen auf der Konsole können Sie die Recordstore-Einstellungen für mehrere Sensoren auf dem neuesten Stand halten.

Die Recordstore-Einstellungen werden für verbundene Recordstores von Drittanbietern konfiguriert und gelten nicht für den ExtraHop-Recordstore.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken **Plattenladen**.
3. Aus dem **Recordstore-Einstellungen** Dropdownliste, wählen Sie die Konsole aus und klicken Sie dann auf **Inhaberschaft übertragen**.

   Wenn Sie sich später dazu entschließen, die Einstellungen auf der Sensor, wählen **dieser Sensor** aus der Dropdownliste Recordstore-Einstellungen und klicken Sie dann auf **Inhaberschaft übertragen**.

ExtraHop-Befehlseinstellungen

Das ExtraHop-Befehlseinstellungen Ein Abschnitt auf dem ExtraHop-Sensor ermöglicht es Ihnen, einen Paketsensor mit einer ExtraHop-Konsole zu verbinden. Abhängig von Ihrer Netzwerkkonfiguration können Sie eine Verbindung vom Sensor (getunnelte Verbindung) oder von der Konsole (direkte Verbindung) herstellen.

- Wir empfehlen Ihnen, sich in den Administrationseinstellungen auf Ihrem Konsole und stellen Sie eine direkte Verbindung zum Sensor her. Direkte Verbindungen werden hergestellt von Konsole über HTTPS auf Port 443 und benötigen keinen speziellen Zugriff. Anweisungen dazu finden Sie unter Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden.
- Wenn dein Sensor befindet sich hinter einer Firewall, daraus können Sie eine SSH-Tunnelverbindung herstellen Sensor zu deinem Konsole. Anweisungen dazu finden Sie unter Stellen Sie von einem Sensor aus eine Verbindung zu einer Konsole her.

Token generieren

Sie müssen ein Token auf einem generieren Sensor bevor Sie eine Verbindung zu einem herstellen können Konsole. Das Token gewährleistet eine sichere Verbindung und macht den Verbindungsprozess weniger anfällig für Machine-in-the-Middle-Angriffe (MITM).

klicken **Token generieren** und dann vervollständigen Sie die Konfiguration auf Ihrer Konsole.

Stellen Sie von einem Sensor aus eine Verbindung zu einer Konsole her

Du kannst den ExtraHop verbinden Sensor zum Konsole durch einen SSH-Tunnel.

Wir empfehlen Ihnen, immer Sensoren direkt anschließen über die Konsole; in Netzwerkumgebungen, in denen eine direkte Verbindung von der Konsole aus aufgrund von Firewalls oder anderen Netzwerkeinschränkungen nicht möglich ist, kann jedoch eine getunnelte Verbindung erforderlich sein. Nachdem Sie die Sensoren angeschlossen haben, können Sie die Sensoreigenschaften anzeigen und bearbeiten, einen Spitznamen zuweisen, die Firmware aktualisieren, den Lizenzstatus überprüfen und ein Diagnose-Supportpaket erstellen.

Bevor Sie beginnen

- Sie können nur eine Verbindung herstellen zu einem Sensor die für dieselbe Systemedition lizenziert ist wie die Konsole. Zum Beispiel ein Konsole auf RevealX Enterprise kann nur eine Verbindung herstellen zu Sensoren auf RevealX Enterprise.

1. Loggen Sie sich in die Administrationseinstellungen auf der Sensor.
2. In der ExtraHop Konsoleneinstellungen Abschnitt, klicken **Konsolen verbinden**.
3. Klicken Sie **Konsole verbinden**.
4. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse der Konsole ein.

   Hinweis Sie können keine verknüpfungslokale IPv6-Adresse angeben.
5. In der Passwort einrichten Feld, geben Sie das Passwort für den Setup-Benutzer auf der Konsole ein.
6. In der Spitzname des Sensors (optional) Feld, geben Sie einen benutzerfreundlichen Namen für den Sensor ein, der auf dem Verbundene Geräte verwalten Seite.

   Wenn kein benutzerfreundlicher Name konfiguriert ist, wird stattdessen der Hostname für den Sensor angezeigt.
7. Wählen Sie die **Konfiguration zurücksetzen** Kontrollkästchen, um vorhandene Sensoranpassungen wie Gerätegruppen, Alarme und Auslöser vom Sensor zu entfernen.

Gesammelte Messwerte wie Aufnahmen und Geräte werden nicht entfernt.

8. Klicken Sie **Verbinde**.

Eine ExtraHop-Konsole mit einem ExtraHop-Sensor verbinden

Du kannst mehrere ExtraHop verwalten Sensoren von einem Konsole. Nachdem Sie das angeschlossen haben Sensoren, können Sie das ansehen und bearbeiten Sensor Eigenschaften, weisen Sie einen Spitznamen zu, aktualisieren Sie die Firmware, überprüfen Sie den Lizenzstatus und erstellen Sie ein Diagnose-Support-Paket.

Das Konsole stellt über HTTPS auf Port 443 eine direkte Verbindung zum Sensor her. Wenn es aufgrund von Firewalleinschränkungen in Ihrer Netzwerkumgebung nicht möglich ist, eine direkte Verbindung herzustellen, können Sie eine Verbindung zum Konsole durch eine getunnelte Verbindung vom ExtraHop-Sensor.

Video: Sehen Sie sich die entsprechende Schulung an: Eine Appliance mit einer RevealX Enterprise Console (ECA) verbinden

Bevor Sie beginnen
Sie können nur eine Verbindung herstellen zu einem Sensor die für dieselbe Systemedition lizenziert ist wie die Konsole. Zum Beispiel ein Konsole auf RevealX Enterprise kann nur eine Verbindung herstellen zu Sensoren auf RevealX Enterprise.

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.

Generieren Sie ein Token auf dem Sensor

Generieren Sie ein Token auf dem Sensor, bevor Sie mit dem Verbindungsvorgang auf der Konsole beginnen.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der ExtraHop-Befehlseinstellungen Abschnitt, klicken **Token generieren**.
3. klicken **Token generieren**.
4. Kopieren Sie das Token und fahren Sie mit dem nächsten Verfahren fort.

Verbinden Sie die Konsole und die Sensoren

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Verwaltung verbundener Appliances Abschnitt, klicken **Sensoren verwalten**.
3. klicken **ExtraHop-Sensor**.
4. klicken **Sensor anschließen**.
5. In der Gastgeber Feld, geben Sie den Hostnamen oder die IP-Adresse des Sensor.
6. Klicken Sie **Verbinde**.
7. In der Token von ExtraHop Sensor Feld, geben Sie das Token ein oder fügen Sie es ein, das Sie auf dem Sensor generiert haben.
8. Geben Sie im Feld Sensor-Nickname (empfohlen) einen benutzerfreundlichen Namen für das ExtraHop-System ein.

   Wenn kein Spitzname eingegeben wird, wird das System durch den Hostnamen identifiziert.
9. Optional: Wählen **Konfiguration zurücksetzen** um bestehende Systemanpassungen wie Gerätegruppen, Alarme und Trigger aus dem ExtraHop-System zu entfernen.

   Gesammelte Messwerte wie Aufnahmen und Geräte werden nicht entfernt.

10. Klicken Sie **Verbinde**.

Paketsensoren verwalten

Von der ExtraHop-Konsole aus können Sie die angeschlossenen Sensoren anzeigen und einige Verwaltungsaufgaben verwalten.

Markieren Sie das Kontrollkästchen für einen oder mehrere angeschlossene Sensoren. Wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Lizenz überprüfen** um eine Verbindung zum ExtraHop-Lizenzierungsserver herzustellen und den neuesten Status für die ausgewählten Sensoren abzurufen. Wenn Ihre Command-Appliance nicht auf Daten von einem angeschlossenen Sensor zugreifen kann, ist die Lizenz möglicherweise ungültig.
- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Klicken Sie **Standard-Support-Skript ausführen** um Informationen über die ausgewählten Sensoren zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Klicken Sie **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Firmware aktualisieren** um den ausgewählten Sensor zu aktualisieren. Sie können eine URL zur Firmware auf dem Kundenportal Website oder laden Sie die Firmware-Datei von Ihrem Computer hoch. Bei beiden Optionen empfehlen wir dringend, die Firmware zu lesen Versionshinweise und die Anleitung zum Firmware-Upgrade.
- Klicken Sie **Deaktiviert** oder **Aktiviere** um die Verbindung zwischen Sensoren und Konsolen vorübergehend zu ändern. Wenn diese Verbindung deaktiviert ist, zeigt die Command-Appliance den Sensor nicht an und kann nicht auf die Sensordaten zugreifen.
- Klicken Sie **Gerät entfernen** um ausgewählte Sensoren dauerhaft abzuschalten.

ExtraHop Recordstore-Einstellungen

Dieser Abschnitt enthält die folgenden Konfigurationseinstellungen für den ExtraHop Recordstore.

- Automatische Flow-Aufzeichnungen konfigurieren (Nur Sensoren)
- Stellen Sie eine Verbindung zu einem ExtraHop-Plattenladen her
- Verwalte einen ExtraHop-Plattenladen (Nur Konsole)

Verbinden Sie den EXA 5200 mit dem ExtraHop-System

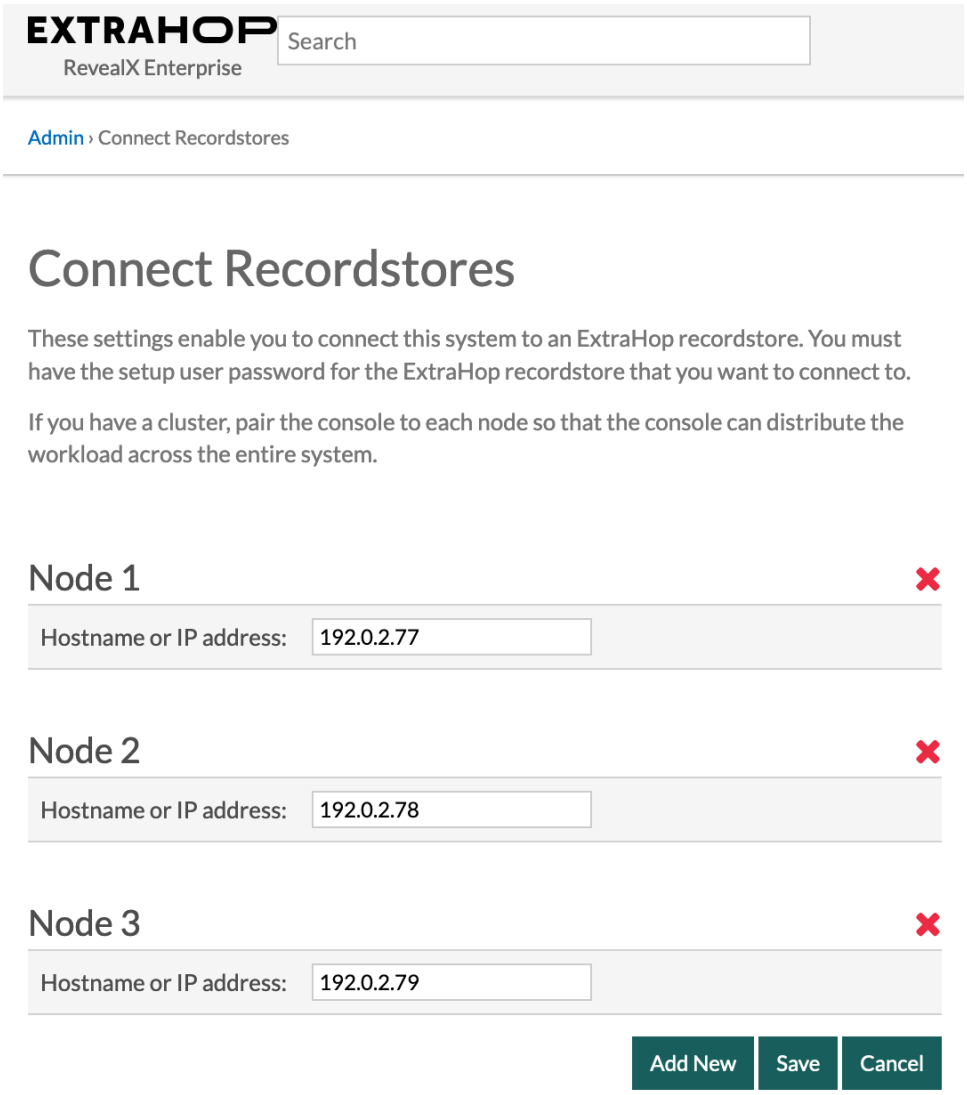
Nachdem Sie einen EXA 5200-Recordstore bereitgestellt haben, müssen Sie eine Verbindung von allen ExtraHop aus herstellen Sensoren und die Konsole zu den Recordstore-Knoten, bevor Sie nach gespeicherten Datensätzen abfragen können.

Wichtig: Wenn Ihr Recordstore-Cluster konfiguriert ist mit Knoten nur für Manager, Sie müssen nur die Sensoren und die Konsole mit den reinen Datenknoten im Recordstore-Cluster verbinden. Stellen Sie keine Verbindung zu den Knoten nur für Manager her, da Knoten nur für Manager keine Datensätze empfangen.

1. Loggen Sie sich in die Administrationseinstellungen auf der Konsole oder Sensor.

   Hinweis: Wenn die Recordstore-Verbindungen von einer Konsole aus verwaltet werden, müssen Sie dieses Verfahren von der Konsole aus und nicht von jedem Sensor aus ausführen.
2. In der ExtraHop Recordstore-Einstellungen Abschnitt, klicken **Synchronisiere Recordstores**.
3. Klicken Sie **Neues hinzufügen**.
4. In der Knoten 1 Feld, geben Sie den Hostnamen oder die IP-Adresse eines beliebigen Recordstore im Recordstore-Cluster ein.

   Hinweis: Wenn der Cluster auch Knoten nur für Manager enthält, fügen Sie nur die Knoten hinzu, die nur Daten enthalten.
5. Klicken Sie für jeden weiteren Recordstore-Knoten im Cluster auf **Neues hinzufügen** und geben Sie den individuellen Hostnamen oder die IP-Adresse in das entsprechende Feld ein Knoten Feld.



6. Klicken Sie **Speichern**.
7. Vergewissern Sie sich, dass der Fingerabdruck auf dieser Seite mit dem Fingerabdruck von Knoten 1 des Cluster übereinstimmt.
8. In der Recordstore-Setup-Passwort Feld, geben Sie das Passwort für Node 1 ein `setup` Benutzerkonto.
9. Klicken Sie **Verbinden**.
10. Wenn die Cluster-Einstellungen gespeichert sind, klicken Sie auf **Erledigt**.

Nächste Schritte
Wenn die Recordstore-Einstellungen von Sensoren und nicht von einer angeschlossenen Konsole verwaltet werden, wiederholen Sie diesen Vorgang auf der Konsole.

Trennen Sie den Recordstore

Um die Aufnahme von Datensätzen in den Recordstore zu stoppen, trennen Sie alle Recordstore-Knoten vom ExtraHop Konsole und Sensoren.

Hinweis: Wenn Recordstore-Verbindungen von einer Konsole verwaltet werden, können Sie dieses Verfahren nur auf der Konsole 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 Recordstores**.
3. Klicken Sie auf das rote **X** neben jedem Knoten im Recordstore-Cluster.

4. Klicken Sie **Speichern**.

Verbinden Sie den EXA 5300 mit dem ExtraHop-System

Nachdem Sie einen EXA 5300-Recordstore bereitgestellt haben, müssen Sie eine Verbindung von allen ExtraHop aus herstellen Sensoren und die Konsole zu den Recordstore-Knoten, bevor Sie nach gespeicherten Datensätzen abfragen können.

Hier sind einige wichtige Überlegungen zu Recordstore-Verbindungen:

- Sie können Sensoren nicht an mehr als einen EXA 5300 anschließen, aber Sie können mehrere EXA 5300 an eine einzige Konsole anschließen.
- Wenn ein Sensor oder eine Konsole an einen EXA 5200 oder EXA 5100v angeschlossen ist, müssen Sie die Verbindung zum EXA 5200 oder EXA 5100v trennen , bevor Sie eine Verbindung zu einem EXA 5300 herstellen können.

Recordstore-Partitionen

Der EXA 5300 organisiert Daten nach Tabellenpartitionen. Das Recordstore-Status Seite enthält eine Zusammenfassung der Partition Abschnitt, der alle Partitionen auflistet, einschließlich der Daten für eine bestimmte Tabelle für ein ausgewähltes Datum.

Ältere Datensätze werden automatisch gelöscht, wenn die Festplatte voll ist. Sie können Partitionen jedoch bei Bedarf auch manuell aus dem System löschen. Auf dem Recordstore-Status Seite, wählen Sie eine oder mehrere Partitionen aus und klicken Sie auf **Ausgewähltes löschen**. Wenn Sie eine Partition löschen, werden bei der Suche nach Datensätzen keine Datensätze aus dieser Partition für dieses Datum zurückgegeben. Das Löschen von Partitionen wird im Audit-Log aufgezeichnet.

Generieren Sie ein Token auf dem EXA 5300

Der EXA 5300 Recordstore stellt eine Verbindung zu einem ExtraHop her Konsole mit tokenbasierter Authentifizierung.

Generieren Sie ein Token im EXA 5300-Recordstore, bevor Sie den Verbindungsvorgang auf dem beginnen Konsole.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Verwaltung verbundener Appliances Abschnitt, unter Recordstore-Einstellungen, klicken Sie **Token generieren**.
3. Klicken Sie **Token generieren**.
4. Kopieren Sie das Token und fahren Sie mit dem nächsten Verfahren fort.

Den EXA 5300 an eine Konsole oder einen Sensor anschließen

Verbinden Sie den EXA 5300 Recordstore mit einem ExtraHop Konsole oder Sensor.

Wichtig: EXA 5300 Recordstore-Verbindungen können nicht von einer Konsole aus verwaltet werden, daher müssen Sie dieses Verfahren sowohl von der Konsole als auch vom Sensor aus ausführen.

1. Loggen Sie sich in die Administrationseinstellungen auf der Konsole oder Sensor durch `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Recordstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Recordstores**.
3. Klicken Sie **Neues hinzufügen**.
4. In der Knoten 1 Feld, geben Sie den Hostnamen oder die IP-Adresse eines beliebigen Recordstore im Recordstore-Cluster ein.
5. Klicken Sie **Speichern**.
6. In der Token von ExtraHop Recordstore Geben Sie in dieses Feld das Token ein, das Sie auf dem EXA 5300 generiert haben, oder fügen Sie es ein.
7. Klicken Sie **Verbinden**.
8. Wenn die Recordstore-Einstellungen gespeichert sind, klicken Sie auf **Erledigt**.

Datensatzaufnahme in einem Recordstore konfigurieren

Konfigurieren Sie die Einstellungen für die Aufnahme von Datensätzen in einem ExtraHop-Recordstore. Die Aufnahme von Datensätzen muss nur aktiviert werden, wenn Sie diese Einstellungen zuvor deaktiviert haben.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Die Einstellung für die Aufnahme von Datensätzen verwalten:
   - Für den EXA 5200, in der Recordstore-Einstellungen Abschnitt, klicken Sie **Cluster-Datenmanagement**.
   - Für den EXA 5300, in der Recordstore-Einstellungen Abschnitt, klicken Sie **Verwaltung der Daten**.
3. In der Aufnahme aufzeichnen Abschnitt, klicken Sie **Record Ingest aktivieren**.
4. Klicken Sie **Speichern**.

Trennen Sie den Recordstore

Um die Aufnahme von Datensätzen in den Recordstore zu stoppen, trennen Sie alle Recordstore-Knoten vom ExtraHop Konsole und Sensoren.

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 Recordstores**.
3. Klicken Sie auf das rote **X** neben jedem Knoten im Recordstore-Cluster.

4. Klicken Sie **Speichern**.

Plattenläden verwalten

Von der ExtraHop-Konsole aus können Sie verbundene Recordstores anzeigen und einige administrative Aufgaben verwalten.

Sehen Sie sich Informationen über verbundene Recordstores als einzelne Appliances oder als Teil eines Cluster an.

- Klicken Sie **Recordstore-Cluster** im Feld Name, um die Cluster-Eigenschaften zu öffnen. Sie können einen benutzerdefinierten Spitznamen für den Recordstore hinzufügen und die Cluster-ID anzeigen.
- Klicken Sie auf einen beliebigen Knotennamen, um die Knoteneigenschaften zu öffnen. Durch Anklicken **Admin-UI öffnen**, können Sie auf die Administrationseinstellungen für den jeweiligen Recordstore zugreifen.
- Zeigen Sie das Datum und die Uhrzeit an, zu denen die Appliance zu dieser Konsole hinzugefügt wurde.
- Sehen Sie sich den Lizenzstatus für Ihre Appliances an.
- Sehen Sie sich die Liste der Aktionen an, die Sie auf dieser Appliance ausführen können.
- In der Spalte Job können Sie den Status aller laufenden Support-Skripts einsehen.

Wählen Sie den Recordstore-Cluster oder einen einzelnen Knoten im Cluster aus, indem Sie auf einen leeren Bereich in der Tabelle klicken, und wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Wählen **Standard-Support-Skript ausführen** um Informationen über den ausgewählten Recordstore zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Wählen **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Cluster entfernen** um den ausgewählten Recordstore dauerhaft zu trennen. Diese Option verhindert nur, dass Sie die Verwaltungsaufgaben auf dieser Seite von der Konsole aus ausführen. Der Recordstore bleibt mit Ihrem Paketsensor verbunden und sammelt weiterhin Datensätze.

Flow-Aufzeichnungen sammeln

Sie können automatisch alle Datenflussdatensätze erfassen und speichern, bei denen es sich um Kommunikation auf Netzwerkebene zwischen zwei Geräten über ein IP-Protokoll handelt. Wenn Sie diese Einstellung aktivieren, aber keine IP-Adressen oder Portbereiche hinzufügen, werden alle erkannten Flussdatensätze erfasst. Die Konfiguration von Flow-Datensätzen für die automatische Erfassung ist ziemlich einfach und kann eine gute Möglichkeit sein, die Konnektivität zu Ihrem Recordstore zu testen.

Bevor Sie beginnen
Sie müssen Zugriff auf ein ExtraHop-System haben mit System- und Zugriffsadministrationsrechte.

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Rekorde Abschnitt, klicken Sie **Automatische Flussaufzeichnungen**.
3. Wählen Sie die **Aktiviert** Ankreuzfeld.
4. In der Intervall veröffentlichen Feld, geben Sie eine Zahl zwischen 60 und 21600 ein.

   Dieser Wert bestimmt, wie oft Datensätze aus einem aktiven Fluss an den Recordstore gesendet werden. Der Standardwert ist 1800 Sekunden.
5. In der IP Adresse Feld, geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich im IPv4-, IPv6- oder CIDR-Format ein.
6. Klicken Sie auf das grüne Plus (**+**) Symbol.

   Sie können einen Eintrag entfernen, indem Sie auf das rote Löschen klicken (**X**) Symbol.
7. In der Portbereiche Feld, geben Sie einen einzelnen Port oder Portbereich ein, und klicken Sie dann auf das grüne Plus (**+**) Symbol.
8. Klicken Sie **Speichern**.

   Flow-Datensätze, die Ihre Kriterien erfüllen, werden jetzt automatisch an Ihren konfigurierten Recordstore gesendet. Warten Sie ein paar Minuten, bis die Aufzeichnungen gesammelt sind.

9. Klicken Sie im ExtraHop-System auf **Rekorde** aus dem Hauptmenü, und klicken Sie dann auf **Aufzeichnungen ansehen** um eine Abfrage zu starten.

   Wenn Sie keine Aufzeichnungen sehen, warten Sie ein paar Minuten und versuchen Sie es erneut. Wenn nach fünf Minuten keine Aufzeichnungen angezeigt werden, überprüfen Sie Ihre Konfiguration oder wenden Sie sich an ExtraHop-Unterstützung.

Status des ExtraHop Recordstore

Wenn Sie einen ExtraHop-Plattenladen Recordstore Ihrem verbunden haben Sensor oder Konsole, können Sie auf Informationen über den Recordstore zugreifen.

Die Tabelle auf dieser Seite enthält die folgenden Informationen zu allen verbundenen Datensatzspeichern.

Aktivität seit

Zeigt die Zeitstempel als die Plattensammlung begann. Dieser Wert wird automatisch alle 24 Stunden zurückgesetzt.

Datensatz gesendet

Zeigt die Anzahl der Datensätze an, die von einem an den Recordstore gesendet wurden Sensor.

I/O-Fehler

Zeigt die Anzahl der generierten Fehler an.

Warteschlange voll (Datensätze gelöscht)

Zeigt die Anzahl der gelöschten Datensätze an, wenn Datensätze schneller erstellt werden, als sie an den Recordstore gesendet werden können.

ExtraHop Packetstore-Einstellungen

ExtraHop Packetstores sammeln und speichern kontinuierlich unformatierte Paketdaten von Ihrem Sensoren. Verbinde den Sensor zum Packetstore, um mit dem Speichern von Paketen zu beginnen.

Sensoren und Konsole mit dem Packetstore verbinden

Bevor Sie Pakete abfragen können, müssen Sie die Konsole und alle Sensoren zum Packetstore.

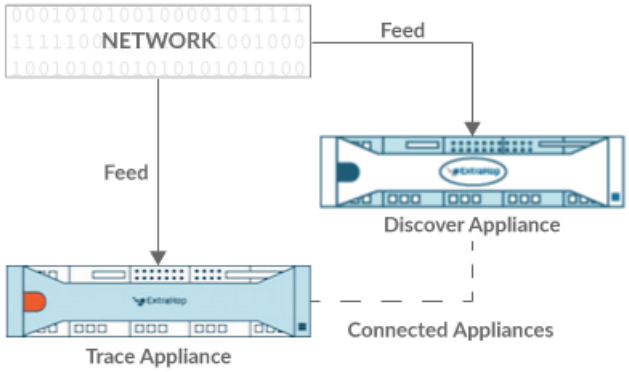


Abbildung 1: An einen Sensor angeschlossen

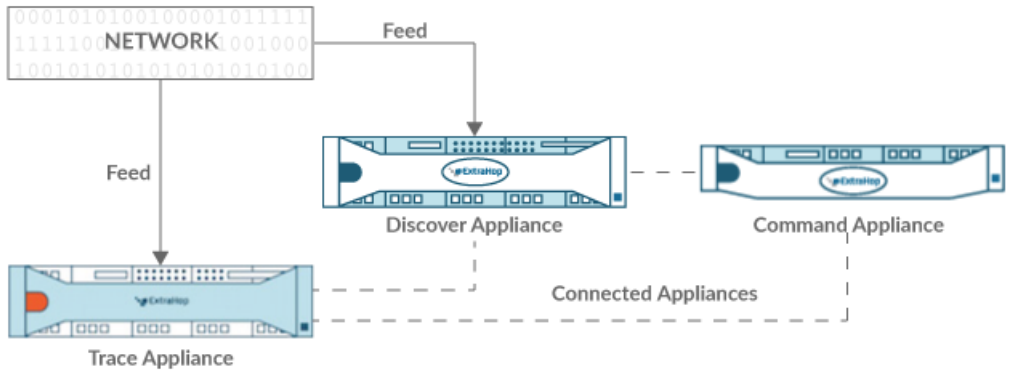


Abbildung 2: Mit Sensor und Konsole verbunden

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. In der Packetstore-Einstellungen Abschnitt, klicken Sie **Synchronisiere Packetstores**.
3. In der Hostname des Paketspeichers Feld, geben Sie den Hostnamen oder die IP-Adresse des Packetstore ein.
4. Klicken Sie **Paar**.
5. Beachten Sie die Informationen in der Fingerabdruck Feld, und überprüfen Sie dann, ob der auf dieser Seite aufgeführte Fingerabdruck mit dem Packetstore-Fingerabdruck auf der Seite Fingerprint in den Administrationseinstellungen des Packetstore übereinstimmt.
6. In der Packetstore-Setup-Passwort Feld, geben Sie das Passwort des Packetstore ein `setup` Nutzer.
7. Klicken Sie **Verbinden**.
8. Um weitere Paketspeicher zu verbinden, wiederholen Sie die Schritte 2 bis 7.

Hinweis Sie können einen Sensor an zwanzig oder weniger Packetstores anschließen, und Sie können eine Konsole an fünfzig oder weniger Packetstores anschließen.

9. Wenn du eine hast Konsole, melden Sie sich in den Administrationseinstellungen auf der Konsole und wiederholen Sie die Schritte 3 bis 7 für alle Packetstores.

Paketspeicher verwalten

Von der ExtraHop-Konsole aus können Sie verbundene Paketspeicher anzeigen und einige Verwaltungsaufgaben verwalten.

Zeigt Informationen über verbundene Packetstores an.

- Klicken Sie **Packetstore-Cluster** im Feld Name, um die Cluster-Eigenschaften zu öffnen. Sie können einen benutzerdefinierten Spitznamen für den Packetstore hinzufügen und die Cluster-ID anzeigen.
- Klicken Sie auf ein beliebiges Gerät, um die Eigenschaften anzuzeigen. Durch Anklicken **Admin-UI öffnen**, können Sie auf die Administrationseinstellungen für den jeweiligen Packetstore zugreifen.
- Zeigen Sie das Datum und die Uhrzeit an, zu denen die Appliance zu dieser Command-Appliance hinzugefügt wurde.
- Sehen Sie sich den Lizenzstatus für Ihre Appliances an.
- Sehen Sie sich die Liste der Aktionen an, die Sie auf dieser Appliance ausführen können.
- In der Spalte Job können Sie den Status aller laufenden Support-Skripts einsehen.

Wählen Sie einen Packetstore aus. Wählen Sie dann eine der folgenden Verwaltungsaufgaben aus.

- Klicken Sie **Unterstützungsskript ausführen** und wählen Sie dann aus den folgenden Optionen:
  - Klicken Sie **Standard-Support-Skript ausführen** um Informationen über den ausgewählten Packetstore zu sammeln. Sie können diese Diagnosedatei zur Analyse an den ExtraHop Support senden.
  - Klicken Sie **Benutzerdefiniertes Support-Skript ausführen** um eine Datei vom ExtraHop Support hochzuladen, die kleine Systemänderungen oder -verbesserungen enthält.
- Klicken Sie **Firmware aktualisieren** um den ausgewählten Packetstore zu aktualisieren. Sie können eine URL zur Firmware auf dem Kundenportal Website oder laden Sie die Firmware-Datei von Ihrem Computer hoch. Bei beiden Optionen empfehlen wir Ihnen dringend, die Firmware zu lesen Versionshinweise und die Anleitung zum Firmware-Upgrade.
- Klicken Sie **Gerät entfernen** um den ausgewählten Packetstore dauerhaft zu trennen. Diese Option verhindert nur, dass Sie die Verwaltungsaufgaben auf dieser Seite von der Konsole aus ausführen. Der Packetstore bleibt mit Ihrem Paketsensor verbunden und sammelt weiterhin Pakete.

Anlage

Allgemeine Akronyme

Die folgenden gängigen Akronyme für Computer- und Netzwerkprotokolle werden in diesem Handbuch verwendet.

Akronym	Vollständiger Name
AAA	Authentifizierung, Autorisierung und Abrechnung
AMF	Format der Aktionsnachricht
CIFS	Gemeinsames Internet-Dateisystem
CLI	Befehlszeilenschnittstelle
CPU	Zentrale Verarbeitungseinheit
DB	Datenbank
DHCP	Dynamisches Host-Konfigurationsprotokoll
DNS	Domainnamensystem
ERSPAN	Gekapselter Remote-Switching-Port-Analysator
FIX	Austausch von Finanzinformationen
FTP	FTP
HTTP	Hypertext-Übertragungsprotokoll
IBMMQ	Nachrichtenorientierte IBM Middleware
ICA	Unabhängige Computerarchitektur
IP	Internet-Protokoll
iSCSI	Internetschnittstelle für kleine Computersysteme
L2	Ebene 2
L3	Schicht 3
L7	Schicht 7
LDAP	Leichtes Verzeichniszugriffsprotokoll
MAC	Medienzugriffskontrolle
MIB	Informationsbasis für das Management
NFS	NFS
NVRAM	Nichtflüchtiger Direktzugriffsspeicher
RADIUS	Benutzerdienst für Fernauthentifizierung mit Einwahl
RPC	Prozeduraufruf per Fernzugriff
RPCAP	Paketerfassung aus der Ferne
RSS	Größe des Resident-Sets

Akronym	Vollständiger Name
SMPP	Kurznachricht Peer-to-Peer-Protokoll
SMTP	Einfaches Nachrichtenübertragungsprotokoll
SNMP	Einfaches Netzwerkmanagement-Protokoll
SPAN	Analysator für geschaltete Anschlüsse
SSD	Solid-State-Laufwerk
SSH	Sichere Shell
SSL	Sichere Socket-Schicht
TACACS+	Zutrittskontrollsystem für Terminalzugriffssteuerungen Plus
TCP	TCP
TLS	Sicherheit auf Transportebene
UI	Benutzerschnittstelle
VLAN	VLAN
VM	Virtuelle Maschine

Cisco NetFlow-Geräte konfigurieren

Im Folgenden finden Sie Beispiele für die grundlegende Cisco-Router-Konfiguration für NetFlow. NetFlow wird pro Schnittstelle konfiguriert. Wenn NetFlow auf der Schnittstelle konfiguriert ist, IP-Paket Fluss Informationen werden auf den ExtraHop-Sensor exportiert.

Wichtig: NetFlow nutzt den SNMP ifIndex-Wert, um Eingangs- und Ausgangsschnittstelleninformationen in Flow-Datensätzen darzustellen. Um die Konsistenz der Schnittstellenberichte zu gewährleisten, aktivieren Sie die SNMP ifIndex-Persistenz auf Geräten, die NetFlow an den Sensor senden. Weitere Informationen zur Aktivierung der SNMP ifIndex-Persistenz auf Ihren Netzwerkgeräten finden Sie in der Konfigurationsanleitung des Geräteherstellers.

Weitere Informationen zur Konfiguration von NetFlow auf Cisco Switches finden Sie in der Dokumentation zu Ihrem Cisco Router oder auf der Cisco-Website unter www.cisco.com.

Konfigurieren Sie einen Exporter auf dem Cisco Nexus Switch

Definieren Sie einen Flow-Exporter, indem Sie das Exportformat angeben, Protokollund Ziel.

Melden Sie sich bei der Switch-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus:

a) Rufen Sie den globalen Konfigurationsmodus auf:

```
config t
```

b) Erstellen Sie einen Flow-Exporter und wechseln Sie in den Flow-Exporter-Konfigurationsmodus.

```
flow exporter <name>
```

Zum Beispiel:

```
flow exporter Netflow-Exporter-1
```

c) (Optional) Geben Sie eine Beschreibung ein:

```
description <string>
```

Zum Beispiel:

```
description Production-Netflow-Exporter
```

d) Legen Sie die IPv4- oder IPv6-Zieladresse für den Exporter fest.

```
destination <eda_mgmt_ip_address>
```

Zum Beispiel:

```
destination 192.168.11.2
```

e) Geben Sie die Schnittstelle an, die benötigt wird, um das zu erreichen NetFlow Collector am konfigurierten Ziel.

```
source <interface_type> <number>
```

Zum Beispiel:

```
source ethernet 2/2
```

f) Geben Sie die NetFlow-Exportversion an:

```
version 9
```

Konfiguration von Cisco Switches über Cisco IOS CLI

1. Melden Sie sich bei der Cisco IOS-Befehlszeilenschnittstelle an und führen Sie die folgenden Befehle aus.
2. Rufen Sie den globalen Konfigurationsmodus auf:

```
config t
```

3. Geben Sie die Schnittstelle an und wechseln Sie in den Schnittstellenkonfigurationsmodus.
   - Cisco Router der Serie 7500:

```
interface <type> <slot>/<port-adapter>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1/0
```

   - Cisco Router der Serie 7200:

```
interface <type> <slot>/<port>
```

Zum Beispiel:

```
interface fastethernet 0/1
```

4. NetFlow aktivieren:

```
ip route-cache flow
```

5. NetFlow-Statistiken exportieren:

```
ip flow-export <ip-address> <udp-port> version 5
```

Wo *<ip-address>* ist die Management + Flow Target-Schnittstelle auf dem ExtraHop-System und *<udp-port>* ist die konfigurierte Collector-UDP-Portnummer.