ExtraHop 9.4
Leitfaden zur ExtraHop Trace REST API

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

Veröffentlicht: 2023-10-24

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 REST API

Die ExtraHop REST API ermöglicht es Ihnen, Administrations- und Konfigurationsaufgaben auf Ihrem ExtraHop-System zu automatisieren. Sie können Anfragen an die ExtraHop-API über eine REST-Schnittstelle (Representational State Transfer) senden, auf die über Ressourcen-URIs und Standard zugegriffen wird HTTP Methoden.

Wenn eine REST-API-Anfrage über HTTPS an ein ExtraHop-System gesendet wird, wird diese Anfrage authentifiziert und dann über einen API-Schlüssel autorisiert. Nach der Authentifizierung wird die Anfrage an das ExtraHop-System gesendet und der Vorgang abgeschlossen.

Jedes ExtraHop-System bietet Zugriff auf den integrierten ExtraHop REST API Explorer, mit dem Sie alle verfügbaren Systemressourcen, Methoden, Eigenschaften und Parameter anzeigen können. Mit dem REST API Explorer können Sie auch API-Aufrufe direkt an Ihr ExtraHop-System senden.

Hinweis: Dieser Leitfaden richtet sich an ein Publikum, das über Grundkenntnisse in der Softwareentwicklung und dem ExtraHop-System verfügt.

ExtraHop API-Anforderungen

Bevor Sie mit dem Schreiben von Skripten für die ExtraHop REST API oder dem Ausführen von Vorgängen über den REST API Explorer beginnen können, müssen Sie die folgenden Anforderungen erfüllen:

- Ihr ExtraHop-System muss konfiguriert, um die Generierung von API-Schlüsseln zu ermöglichen für den Benutzertyp, der Sie sind (remote oder lokal).
- Du musst Generieren Sie einen gültigen API-Schlüssel.
- Sie benötigen ein Benutzerkonto auf dem ExtraHop-System mit entsprechendem Privilegien für die Art der Aufgaben festlegen, die Sie ausführen möchten.

Greifen Sie auf die ExtraHop REST API zu und authentifizieren Sie sich bei ihr

Setup-Benutzer und Benutzer mit System- und Zugriffsadministrationsrechten steuern, ob Benutzer API-Schlüssel generieren können. Sie können beispielsweise verhindern, dass Remotebenutzer Schlüssel generieren, oder Sie können die API-Schlüsselgenerierung vollständig deaktivieren. Wenn diese Funktion aktiviert ist, werden API-Schlüssel von Benutzern generiert und können nur von dem Benutzer eingesehen werden, der den Schlüssel generiert hat.

Hinweis: Administratoren richten Benutzerkonten ein und weisen Berechtigungen zu, aber dann generieren Benutzer ihre eigenen API-Schlüssel. Benutzer können API-Schlüssel für ihr eigenes Konto löschen, und Benutzer mit System- und Zugriffsadministrationsrechten können API-Schlüssel für jeden Benutzer löschen. Weitere Informationen finden Sie unter Benutzer und Benutzergruppen.

Nachdem Sie einen API-Schlüssel generiert haben, müssen Sie den Schlüssel an Ihre Anforderungsheader anhängen. Das folgende Beispiel zeigt eine Anfrage, die Metadaten über die Firmware abruft, die auf dem ExtraHop-System läuft:

```
curl -i -X GET --header "Accept: application/json" \
--header "Authorization: ExtraHop apikey=2bc07e55971d4c9a88d0bb4d29ecbb29" \
"https://<hostname-or-IP-of-your-ExtraHop-system>/api/v1/extrahop"
```

Privilegienstufen

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

Sie können die Berechtigungsstufen für Benutzer über die `granted_roles` und `effective_roles` Eigenschaften. Die `granted_roles` Die Eigenschaft zeigt Ihnen, welche Berechtigungsstufen dem Benutzer explizit gewährt wurden. Die `effective_roles` Die Eigenschaft zeigt Ihnen alle Berechtigungsstufen für einen Benutzer, einschließlich derer, die Sie außerhalb der zugewiesenen Rolle erhalten haben, z. B. über eine Benutzergruppe.

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

- GET /users
- GET /users/ {Nutzername}

Die `granted_roles` und `effective_roles` Eigenschaften unterstützen die folgenden Berechtigungsstufen. Beachten Sie, dass die Art der Aufgaben für jedes ExtraHop-System je nach verfügbarem Ressourcen sind im REST API Explorer aufgeführt und hängen von den für das System aktivierten Modulen und den Zugriffsberechtigungen für Benutzermodule ab.

Privilegienstufe	Zulässige Aktionen
„system“: „voll“	• Aktivieren oder deaktivieren Sie 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.

Privilegienstufe	Zulässige Aktionen
	• 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. • 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.
„metrics“: „vollständig“	• 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 eine Modulzugriffsberechtigung, die einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„ndr“: „keine“	• Kein Zugriff auf Inhalte des NDR-Moduls

Privilegienstufe	Zulässige Aktionen
	Dies ist eine Modulzugriffsberechtigung, die einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„npm“: „voll“	• Leistungserkennungen anzeigen • Dashboards anzeigen und erstellen • Benachrichtigungen anzeigen und erstellen Dies ist eine Modulzugriffsberechtigung, die einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„npm“: „keine“	• Kein Zugriff auf den Inhalt des NPM-Moduls Dies ist eine Modulzugriffsberechtigung, die einem Benutzer zusätzlich zu einer der folgenden Systemzugriffsberechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„Pakete“: „voll“	• Pakete anzeigen und herunterladen über `GET/packetcaptures/{id}` Betrieb. Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„Pakete“: „full_with_keys“	• Pakete anzeigen und herunterladen über `GET/packetcaptures/{id}` Betrieb.

Privilegienstufe	Zulässige Aktionen
	Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“
„packages“: „slices_only“	• Sehen Sie sich die ersten 64 Byte von Paketen an und laden Sie sie herunter über `GET/packetcaptures/{id}` Betrieb. Dies ist eine Zusatzberechtigung, die einem Benutzer mit einer der folgenden Berechtigungsstufen gewährt werden kann: • „write“: „voll“ • „write“: „begrenzt“ • „write“: „persönlich“ • „schreiben“: null • „metrics“: „vollständig“ • „metrics“: „eingeschränkt“

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**.

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 Zugriffs-Einstellungen Abschnitt, klicken **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 Abschnitt API-Schlüssel 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.

Konfiguration von Cross-Origin Resource Sharing (CORS)

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

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

1. In der **Auf Einstellungen zugreifen** Abschnitt, klicken **API-Zugriff**.
2. 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 den genauen Domänenname. Sie können keinen Pfad anhängen, Sie können jedoch eine Portnummer angeben.
   - Um den Zugriff von einer beliebigen URL aus zu ermöglichen, wählen Sie API-Anfragen von beliebigem Ursprung zulassen Checkbox.

     Hinweis: Das Zulassen des REST-API-Zugriffs von einem beliebigen Ursprung aus ist weniger sicher als die Bereitstellung einer Liste mit expliziten Ursprüngen.
3. klicken **Einstellungen speichern** und dann klicken **Erledigt**.

Erfahren Sie mehr über den REST API Explorer

Der REST API Explorer ist ein webbasiertes Tool, mit dem Sie detaillierte Informationen zu den ExtraHop REST API-Ressourcen, Methoden, Parametern, Eigenschaften und Fehlercodes anzeigen können. Codebeispiele sind in Python, cURL und Ruby für jede Ressource verfügbar. Sie können Operationen auch direkt über das Tool ausführen.

Öffnen Sie den REST API Explorer

Sie können den REST API Explorer in den Administrationseinstellungen oder über die folgende URL öffnen:

```
https://<extrahop-hostname-or-ip-address>/api/v1/explore/
```

1. Loggen Sie sich in die Administrationseinstellungen des ExtraHop-Systems ein über `https://<extrahop-hostname-or-IP-address>/admin`.
2. Klicken Sie im Bereich Zugriffseinstellungen auf **API-Zugriff**.
3. Auf dem API-Zugriff Seite, klick **REST-API-Explorer**.

   Der REST API Explorer wird in Ihrem Browser geöffnet.

Betriebsinformationen anzeigen

Im REST API Explorer können Sie auf einen beliebigen Vorgang klicken, um die Konfigurationsinformationen für die Ressource anzuzeigen.

Die folgende Tabelle enthält Informationen zu den Abschnitten, die für Ressourcen im REST API Explorer verfügbar sind. Die Verfügbarkeit von Abschnitten variiert je nach HTTP-Methode. Nicht bei allen Methoden sind alle Abschnitte in der Tabelle aufgeführt.

Abschnitt	Beschreibung
Körperparameter	Stellt alle Felder für den Anforderungstext und unterstützte Werte für jedes Feld bereit.
Parameter	Stellt Informationen zu den verfügbaren Abfrageparametern bereit.
Antworten	Informiert über die möglichen HTTP Statuscodes für die Ressource. Wenn du klickst **Anfrage senden**, dieser Abschnitt enthält auch die Antwort des Server und die cURL-, Python- und Ruby-Syntax, die zum Senden der angegebenen Anfrage erforderlich ist. **Hinweis:** Klicken **Modell** um Beschreibungen der Felder anzuzeigen, die in einer Antwort zurückgegeben wurden.

Identifizieren Sie Objekte auf dem ExtraHop-System

Objekte auf dem ExtraHop-System können durch jeden eindeutigen Wert identifiziert werden, z. B. durch die IP-Adresse , die MAC-Adresse, den Namen oder die System-ID. Um API-Operationen für ein bestimmtes Objekt auszuführen, müssen Sie jedoch die Objekt-ID suchen. Sie können die Objekt-ID mit den folgenden Methoden im REST API Explorer leicht finden.

- Die Objekt-ID wird in den Headern bereitgestellt, die von einer POST-Anforderung zurückgegeben werden. Wenn Sie beispielsweise eine POST-Anfrage senden, um eine Seite zu erstellen, zeigen die Antwortheader eine Standort-URL an.

  Die folgende Anfrage gab den Speicherort für das neu erstellte Tag als zurück `/api/v1/tags/1` und die ID für das Tag als `1`.

  ```
  {
   "date": "Tue, 09 Nov 2021 18:21:00 GMT ",
   "via": "1.1 localhost",
   "server": "Apache",
   "content-type": "text/plain; charset=utf-8",
   "location": "/api/v1/tags/1",
   "cache-control": "private, max-age=0",
   "connection": "Keep-Alive",
   "keep-alive": "timeout=90, max=100",
   "content-length": "0"
  }
  ```

- Die Objekt-ID wird für alle Objekte bereitgestellt, die von einer GET-Anfrage zurückgegeben werden. Wenn Sie beispielsweise eine GET-Anfrage auf allen Geräten ausführen, enthält der Antworttext Informationen für jedes Gerät, einschließlich der ID.

  Der folgende Antworttext zeigt einen Eintrag für ein einzelnes Gerät mit der ID 10212 an:

  ```
  {
   "mod_time": 1448474346504,
   "node_id": null,
   "id": 10212,
   "extrahop_id": "test0001",
   "description": null,
   "user_mod_time": 1448474253809,
   "discover_time": 1448474250000,
   "vlanid": 0,
   "parent_id": 9352,
   "macaddr": "00:05:G3:FF:FC:28",
   "vendor": "Cisco",
   "is_l3": true,
   "ipaddr4": "10.10.10.5",
   "ipaddr6": null,
   "device_class": "node",
   "default_name": "Cisco5",
   "custom_name": null,
   "cdp_name": "",
   "dhcp_name": "",
   "netbios_name": "",
   "dns_name": "",
   "custom_type": "",
   "analysis_level": 1
  },
  ```

- Die Objekt-ID ist in der URL für die meisten Objekte angegeben. Klicken Sie beispielsweise im ExtraHop-System auf **Vermögenswerte**, und dann **Geräte**. Wählen Sie ein beliebiges Gerät aus und sehen Sie sich die URL an. Im folgenden Beispiel zeigt die URL für die Geräteseite Oid=10180.

  ```
  https://10.10.10.205/extrahop/#/Devices?details=true&device
  Oid=10180&from=6&interval_type=HR&until=0&view=l2stats
  ```

  Um spezifische Anfragen für dieses Gerät auszuführen, fügen Sie 10180 zur id Feld im REST API Explorer oder für den Body-Parameter in Ihrer Anfrage.

Die URL für Dashboards zeigt einen Short_Code an, der hinter /Dashboard erscheint. Wenn Sie den short_code zum REST API Explorer oder zu Ihrer Anfrage hinzufügen, müssen Sie dem Shortcode eine Tilde voranstellen.

Im folgenden Beispiel ist kmc9Y der short_code. Um Anfragen für dieses Dashboard auszuführen, fügen Sie `~kmC9Y` als Wert für das Feld short_code.

```
https://10.10.10.205/extrahop/#/Dashboard/kmC9Y/?from=6&interval_
type=HR&until=0
```

Sie finden den short_code und die Dashboard-ID auch in den Dashboard-Eigenschaften für jedes Dashboard, auf das Sie über das Befehlsmenü zugreifen können ⋮. Für einige API-Operationen, wie DELETE, ist die Dashboard-ID erforderlich.

ExtraHop API-Ressourcen

Sie können über die ExtraHop REST API Operationen für die folgenden Ressourcen ausführen. Sie können auch detailliertere Informationen zu diesen Ressourcen einsehen, z. B. verfügbare HTTP Methoden, Abfrageparameter und Objekteigenschaften im REST API Explorer.

API-Schlüssel

Ein API-Schlüssel ermöglicht es einem Benutzer, Operationen über die ExtraHop REST API durchzuführen.

Sie können den ersten API-Schlüssel für das Setup-Benutzerkonto über die REST-API generieren. Alle anderen API-Schlüssel werden über die API-Zugriffsseite in den Administrationseinstellungen generiert.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
HOLEN SIE SICH /apikeys	Ruft alle API-Schlüssel ab.
POST /apikeys	Erstellen Sie den ersten API-Schlüssel für das Setup-Benutzerkonto.
GET /apikeys/ {keyid}	Rufen Sie Informationen zu einem bestimmten API-Schlüssel ab.

Gerät

Das ExtraHop-System besteht aus einem Netzwerk verbundener ExtraHop-Geräte, wie Sensoren, Konsolen, Datensatzspeicher und Paketspeicher, die Aufgaben wie die Überwachung des Datenverkehrs, die Analyse von Daten, die Speicherung von Daten und die Identifizierung von Erkennungen ausführen.

Sie können Informationen abrufen und Verbindungen für lokale und entfernte ExtraHop-Appliances herstellen.

Hinweis: Sie können nur eine Verbindung zwischen ähnlichen ExtraHop-Appliances wie Reveal (x) Enterprise oder Performance herstellen.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
GET /geräte	Rufen Sie alle Remote-ExtraHop-Geräte ab, die mit der lokalen Appliance verbunden sind.
POST /Geräte	Stellen Sie eine neue Verbindung zu einer externen ExtraHop-Appliance her.
/appliances/ {id} LÖSCHEN	Trennen Sie eine bestimmte ExtraHop-Appliance von dieser Konsole.
GET /appliances/ {id}	Rufen Sie eine bestimmte Remote-ExtraHop-Appliance ab, die mit der lokalen Appliance verbunden ist (nur auf Konsolen gültig).
GET /appliances/ {id} /cloudservices	Rufen Sie den Status der ExtraHop Cloud Services auf dieser Appliance ab (nur gültig auf Konsolen).

Betrieb	Beschreibung
GET /appliances/ {id} /productkey	Rufen Sie den Produktschlüssel für eine angegebene Appliance ab (nur auf Konsolen gültig).
GET /appliances/ {ids_id} /association	Ruft die ID des Paketsensor ab, mit dem der IDS-Sensor verbunden ist.
POST /appliances/ {ids_id} /association	Verbinden Sie einen IDS-Sensor mit einem Paketsensor.
GET /appliances/firmware/next	Rufen Sie Firmware-Versionen ab, auf die externe ExtraHop-Systeme aktualisiert werden können (nur auf Konsolen gültig).
POST /Geräte/Firmware/Upgrade	Aktualisieren Sie die Firmware auf externen ExtraHop-Systemen, die mit dem lokalen System verbunden sind. Firmware-Images werden von ExtraHop Cloud Services heruntergeladen (nur auf Konsolen gültig).
`GET /appliances/{ids_id}/association`	Ruft die ID des Paketsensor ab, mit dem der IDS-Sensor verbunden ist (nur auf Konsolen gültig).
`POST /appliances/{ids_id}/association`	Verbindet einen IDS-Sensor mit einem Paketsensor (nur auf Konsolen gültig).

ExtraHop

Diese Ressource enthält Metadaten über das ExtraHop-System.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
HOLEN SIE SICH /extrahop	Rufen Sie Metadaten über die Firmware ab, die auf dem ExtraHop-System ausgeführt wird.
HOLEN SIE SICH /extrahop/edition	Rufen Sie die Edition des ExtraHop-Systems ab.
BEITRAG /extrahop/firmware	Laden Sie ein neues Firmware-Image auf das ExtraHop-System hoch. Weitere Informationen finden Sie unter Aktualisieren Sie die ExtraHop-Firmware über die REST-API.
BEITRAG /extrahop/firmware/download/url	Laden Sie ein neues Firmware-Image von einer URL auf das ExtraHop-System herunter.
POST /extrahop/firmware/neuest/upgrade	Aktualisieren Sie das ExtraHop-System auf das zuletzt hochgeladene Firmware-Image.
HOLEN SIE SICH /extrahop/idrac	Rufen Sie die iDRAC-IP-Adresse des ExtraHop-Systems ab.
GET /extrahop/platform	Rufen Sie den Plattformnamen des ExtraHop-Systems ab.
GET /extrahop/Prozesse	Rufen Sie eine Liste der Prozesse ab, die auf dem ExtraHop-System ausgeführt werden.
POST /extrahop/processes/ {process} /restart	Starten Sie einen Prozess neu, der auf dem ExtraHop-System läuft.

Betrieb	Beschreibung
GET /extrahop/services	Rufen Sie die Einstellungen für alle Dienste ab.
PATCH /extrahop/services	Aktualisieren Sie die Einstellungen für Dienste.
POST /extrahop/restart	Starten Sie das ExtraHop-System neu.
BEITRAG /extrahop/sslcert	Generieren Sie das SSL-Zertifikat auf dem ExtraHop-System neu. Weitere Informationen finden Sie unter Erstellen Sie ein vertrauenswürdiges SSL-Zertifikat über die REST-API
GIB /extrahop/sslcert ein	Ersetzen Sie das SSL-Zertifikat auf dem ExtraHop-System.
POST /extrahop/sslcert/signingrequest	Erstellen Sie eine Anfrage zum Signieren eines SSL-Zertifikats. Weitere Informationen finden Sie unter Erstellen Sie ein vertrauenswürdiges SSL-Zertifikat über die REST-API.
HOLEN SIE SICH /extrahop/ticketing	Rufen Sie den Status der Ticketing-Integration ab.
PATCH /extrahop/Ticketverkauf	Aktivieren oder deaktivieren Sie die Ticketintegration.
Holen Sie sich /extrahop/version	Rufen Sie die Version der Firmware ab, die auf dem ExtraHop-System ausgeführt wird.

Implementierungsinformationen und Anweisungen für jeden Vorgang sind im REST API Explorer dokumentiert. Sie können im REST API Explorer auf eine beliebige Operation klicken, um Implementierungsinformationen wie Parameter, Antwortklasse und Nachrichten sowie JSON-Modell und -Schema anzuzeigen.

Jobs

Sie können den Fortschritt einiger Verwaltungsaufgaben überwachen, die über die REST-API gestartet wurden. Wenn eine REST-Anfrage einen Job erstellt, wird die Job-ID zurückgegeben in `location` Header der Antwort. Die folgenden Operationen schaffen Arbeitsplätze:

- `POST /extrahop/firmware/latest/upgrade`
- `POST /extrahop/sslcert`

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
GET /jobs	Ruft den Status aller Jobs ab.
GET /jobs/ {id}	Rufen Sie den Status eines bestimmten Jobs ab.

Lizenz

Diese Ressource ermöglicht es Ihnen, Produktschlüssel abzurufen und festzulegen oder eine Lizenz abzurufen und festzulegen.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
GET /license	Rufen Sie die Lizenz ab, die auf dieses ExtraHop-System angewendet wurde.
PUT /Lizenz	Beantragen und registrieren Sie eine neue Lizenz für das ExtraHop-System.
HOLEN SIE SICH /license/productkey	Rufen Sie den Produktschlüssel für dieses ExtraHop-System ab.
PUT /license/productkey	Wenden Sie den angegebenen Produktschlüssel auf das ExtraHop-System an und registrieren Sie die Lizenz.

Konfiguration ausführen

Die laufende Konfigurationsdatei ist ein JSON-Dokument, das wichtige Systemkonfigurationsinformationen für das ExtraHop-System enthält.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
Holen Sie sich /runningconfig	Ruft die aktuell laufende Konfigurationsdatei ab.
PUT /runningconfig	Ersetzt die aktuell laufende Konfigurationsdatei. Änderungen an der Konfigurationsdatei werden nicht automatisch gespeichert.
POST/runningconfig/save	Speichert die aktuellen Änderungen in der laufenden Konfigurationsdatei.
GET /runningconfig/saved	Rufen Sie die gespeicherte laufende Konfigurationsdatei ab.

Unterstützungspaket

Ein Support Pack ist eine Datei, die vom ExtraHop Support bereitgestellte Konfigurationsanpassungen enthält.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
HOLEN SIE SICH /supportpacks	Rufen Sie Metadaten zu allen Support Packs ab.
POST /supportpacks	Laden Sie ein Support Pack hoch und führen Sie es aus.
POST /supportpacks/execute	Führen Sie ein neues Support Pack aus.
GET /supportpacks/queue/ {id}	Überprüfen Sie den Status eines laufenden, laufenden Support Packs.
GET /supportpacks/ {Dateiname}	Laden Sie ein vorhandenes Support Pack anhand des Dateinamens herunter.

Nutzer

Mit der Benutzerressource können Sie die Liste der Benutzer, die Zugriff auf das ExtraHop-System haben, und die Berechtigungsstufen für diese Benutzer erstellen und verwalten.

In der folgenden Tabelle sind alle Operationen aufgeführt, die Sie mit dieser Ressource ausführen können:

Betrieb	Beschreibung
GET /users	Ruft alle Benutzer ab.
POST /Benutzer	Erstellen Sie einen neuen Benutzer.
LÖSCHE /users/ {username}	Löscht einen bestimmten Benutzer.
GET /users/ {Nutzername}	Rufen Sie einen bestimmten Benutzer ab.
PATCH /users/ {Nutzername}	Aktualisieren Sie die Einstellungen für einen bestimmten Benutzer.
GET /users/ {username} /apikeys	Ruft alle API-Schlüssel für einen bestimmten Benutzer ab.
GET /users/ {username} /apikeys/ {keyid}	Rufen Sie Informationen über einen bestimmten API-Schlüssel und Benutzer ab.

ExtraHop REST-API-Beispiele

Die folgenden Beispiele zeigen gängige REST-API-Operationen.

- Ändern Sie einen Dashboard-Besitzer über die REST-API
- Extrahieren Sie die Geräteliste über die REST-API
- Erstellen und Zuweisen eines Geräte-Tags über die REST-API
- Abfragen von Metriken zu einem bestimmten Gerät über die REST-API
- Ein Objekt über die REST-API erstellen, abrufen und löschen
- Das Datensatzprotokoll abfragen

Aktualisieren Sie die ExtraHop-Firmware über die REST-API

Sie können Upgrades der Firmware auf Ihren ExtraHop-Appliances über die ExtraHop REST API automatisieren. Dieses Handbuch enthält Anweisungen zum Upgrade über den REST API Explorer, einen cURL-Befehl und ein Python-Skript.

Hinweis: Wenn Ihr Gerät mit ExtraHop Cloud Services verbunden ist, können Sie den Upgrade-Prozess vereinfachen, indem Sie sich die verfügbaren Firmware-Versionen ansehen und Firmware direkt von ExtraHop Cloud Services auf das System herunterladen. Weitere Informationen finden Sie unter Aktualisieren Sie die ExtraHop-Firmware über die REST-API mit ExtraHop Cloud Services.

Der Firmware-Upgrade-Prozess ist zwar bei allen ExtraHop-Appliances ähnlich, bei einigen Appliances sind jedoch zusätzliche Überlegungen oder Schritte erforderlich, die Sie berücksichtigen müssen, bevor Sie die Firmware in Ihrer Umgebung installieren. Wenn Sie Hilfe bei Ihrem Upgrade benötigen, wenden Sie sich an den ExtraHop-Support.

Alle Geräte müssen die folgenden Anforderungen erfüllen:

- Die Firmware-Version muss mit Ihrem Gerätemodell kompatibel sein.
- Die Firmware-Version auf Ihrem Gerät muss von der Upgrade-Version unterstützt werden.
- Auf Befehlsgeräten muss eine Firmware ausgeführt werden, die größer oder gleich der Firmware der angeschlossenen Geräte ist.
- Auf Discover-Appliances muss eine Firmware ausgeführt werden, die größer oder gleich der Firmware der verbundenen Explore and Trace-Appliances ist.

Wenn Ihr Einsatz nur eine umfasst Sensor, weiter zum API-Explorer, cURL oder Python Upgrade-Anweisungen.

Wenn Ihre Bereitstellung zusätzliche Appliance-Typen umfasst, müssen Sie die folgenden Abhängigkeiten berücksichtigen, bevor Sie mit den Upgrade-Anweisungen fortfahren.

Wenn Ihr Einsatz beinhaltet...	Aufgaben vor dem Upgrade	Bestellung aktualisieren
Befehlsgeräte	Reservieren Sie ein Wartungsfenster von einer Stunde für Command-Appliances, die 50.000 Geräte oder mehr verwalten.	• Befehlsgerät • Geräte entdecken • Alle Explore-Appliances (Managerknoten, dann Datenknoten) • Appliances verfolgen
Entdecken Sie Geräte	siehe ExtraHop-Plattenspeicher aktualisieren.	
Appliances verfolgen	Keine	

Aktualisieren Sie die ExtraHop-Firmware über den REST API Explorer

Wichtig: Der REST-API-Explorer ist auf Reveal (x) 360 nicht verfügbar.

Laden Sie die Firmware herunter und aktualisieren Sie die Appliance

1. klicken **BEITRAG /extrahop/firmware/download/url**.
2. klicken **Probiere es aus**.
3. Geben Sie im Feld die folgenden Felder an:

   • **Firmware-URL:** Die URL, von der die Firmware-.tar-Datei heruntergeladen werden kann.

   • **aufrüsten:** Gibt an, ob die Appliance nach Abschluss des Firmware-Downloads aktualisiert werden soll. Setze dieses Feld auf `true`.

   Das Textfeld sollte dem folgenden Beispieltext ähneln:

   ```
   {
     "upgrade": true,
     "firmware_url": "https://example.extrahop.com/eda/8.7.1.tar"
   }
   ```

4. klicken **Anfrage senden**.

   Notieren Sie sich in den Antwort-Headern den Wert nach dem letzten Schrägstrich in der `location` Kopfzeile. Sie benötigen diesen Wert, um den Fortschritt des Upgrade-Jobs zu überwachen. Die Job-ID im folgenden Beispiel lautet beispielsweise `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`

   ```
   /api/v1/jobs/ebbdbc9e-7113-448c-ab9b-cc0ec2307702
   ```

Überwachen Sie den Fortschritt des Upgrade-Jobs

1. klicken **Jobs**.
2. klicken **GET /jobs/ {id}**.
3. Geben Sie im Feld id den Wert ein, den Sie aus dem `location` Kopfzeile in der vorherigen Aufgabe.
4. klicken **Anfrage senden**.
5. Sehen Sie sich im Antworttext Informationen zum Job an.

   Die `status` Feld ist `DONE` wenn der Job abgeschlossen ist.

Aktualisieren Sie die ExtraHop-Firmware mit cURL

Sie können die Firmware auf einer Appliance mit dem cURL-Befehl aktualisieren.

Bevor Sie beginnen

- Das cURL-Tool muss auf Ihrem Computer installiert sein.
- Die.tar-Datei der Systemfirmware muss auf Ihren Computer heruntergeladen werden.

1. Öffnen Sie eine Terminalanwendung.
2. Laden Sie die Firmware herunter und aktualisieren Sie die Appliance.

   Führen Sie den folgenden Befehl aus, wobei `YOUR_KEY` ist der API-Schlüssel für Ihr Benutzerkonto, `HOSTNAME` ist der Hostname Ihrer ExtraHop-Appliance und `FIRMWARE_URL` ist die URL, von der die Firmware-.tar-Datei heruntergeladen werden kann:

   ```
   curl -v -X POST https://HOSTNAME/api/v1/extrahop/firmware/download/url -H
    "Authorization: ExtraHop apikey=YOUR_KEY" -H "Content-Type: application/
   json" -d "{ \"upgrade\": true, \"firmware_url\": \"FIRMWARE_URL\"}"
   ```

Notieren Sie sich in der Befehlsausgabe die Job-ID im Location-Header. Die Job-ID im folgenden Beispiel lautet beispielsweise `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`:

```
< Location: /api/v1/jobs/ebbdbc9e-7113-448c-ab9b-cc0ec2307702
```

3. Überwachen Sie den Fortschritt des Upgrade-Jobs.

   Führen Sie den folgenden Befehl aus, wobei `YOUR_KEY` ist der API-Schlüssel für Ihr Benutzerkonto `HOSTNAME` ist der Hostname Ihrer Appliance und `JOB_ID` ist die ID, die Sie im vorherigen Schritt aufgezeichnet haben:

   ```
   curl -v -X GET https://HOSTNAME/api/v1/jobs/JOB_ID -H "Authorization:
    ExtraHop apikey=API_KEY"
   ```

   Der Befehl zeigt ein Objekt an, das Informationen über den Upgrade-Job enthält. Das Upgrade ist abgeschlossen, wenn `status` Feld ist `DONE`. Wenn das Upgrade nicht abgeschlossen ist, warten Sie einige Minuten und führen Sie den Befehl erneut aus.

Rufen Sie das Python-Beispielskript ab und führen Sie es aus

Das ExtraHop GitHub-Repository enthält ein Python-Skript, das mehrere Appliances aktualisiert, indem es URLs, API-Schlüssel und Firmware-Dateipfade aus einer CSV-Datei liest.

Wichtig: Das Beispiel-Python-Skript authentifiziert sich beim Sensor oder der Konsole über einen API-Schlüssel, der nicht mit der Reveal (x) 360-REST-API kompatibel ist. Um dieses Skript mit Reveal (x) 360 auszuführen, müssen Sie das Skript so ändern, dass es sich mit API-Token authentifiziert. Sehen Sie die py_rx360_auth.py Skript im ExtraHop GitHub-Repository für ein Beispiel für die Authentifizierung mit API-Token.

Hinweis: Das Skript deaktiviert die Aufnahme von Datensatz für ExtraHop-Plattenspeicher nicht automatisch. Du musst Datensatz manuell deaktivieren bevor Sie das Skript für einen ExtraHop-Recordstore ausführen.

1. Gehe zum GitHub-Repository mit ExtraHop-Codebeispielen und laden Sie den Inhalt des Verzeichnisses upgrade_system auf Ihren lokalen Computer herunter.
2. Öffnen Sie in einem Texteditor `systems.csv` archivieren und ersetzen Sie die Beispielwerte durch die Hostnamen und API-Schlüssel Ihrer Appliances.
3. Führen Sie den `upgrade_system_url.py` skript.

   Die folgenden Argumente sind optional:

   --max-threads {int}

   Gibt die maximale Anzahl gleichzeitiger Threads an. Der Standardwert ist 2.

   --warte {float}

   Gibt an, wie viele Minuten gewartet werden soll, bevor der Status eines Upgrade-Jobs überprüft wird. Der Standardwert ist 0,5.

   Mit dem folgenden Befehl werden beispielsweise maximal 3 Appliances gleichzeitig aktualisiert:

   ```
   python3 upgrade_system_url.py --max-threads 3
   ```

   Hinweis: Wenn das Skript eine Fehlermeldung zurückgibt, dass die Überprüfung des SSL-Zertifikats 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)
   ```

ExtraHop-Plattenspeicher aktualisieren

Aufgaben vor dem Upgrade

Bevor Sie einen ExtraHop-Recordstore aktualisieren, müssen Sie die Aufnahme von Datensätzen stoppen. Sie können die Aufnahme von Datensatz für alle Knoten in einem Cluster von einem einzelnen Knoten aus stoppen.

Hinweis: Die Botschaft `Could not determine ingest status on some nodes` und `Error` wird möglicherweise auf der Seite Cluster-Datenverwaltung in den Verwaltungseinstellungen der aktualisierten Knoten angezeigt, bis alle Knoten im Cluster aktualisiert sind. Diese Fehler werden erwartet und können ignoriert werden.

1. Öffnen Sie eine Terminal-Anwendung.
2. Führen Sie den folgenden Befehl aus, wobei `YOUR_KEY` ist die API für Ihr Benutzerkonto und `HOSTNAME` ist der Hostname Ihres ExtraHop-Recordstores:

```
curl -X PATCH "https://HOST/api/v1/extrahop/cluster" -H "accept:
 application/json" -H "Authorization: ExtraHop apikey=YOUR_KEY" -H
 "Content-Type: application/json" -d "{ \"ingest_enabled\": false}"
```

Aufgaben nach dem Upgrade

Nachdem Sie alle Knoten im Recordstore-Cluster aktualisiert haben, aktivieren Sie die Datensatzaufnahme.

1. Öffnen Sie eine Terminal-Anwendung.
2. Führen Sie den folgenden Befehl aus, wobei `YOUR_KEY` ist die API für Ihr Benutzerkonto und `HOSTNAME` ist der Hostname Ihres ExtraHop-Recordstores:

```
curl -X PATCH "https://HOST/api/v1/extrahop/cluster" -H "accept:
 application/json" -H "Authorization: ExtraHop apikey=YOUR_KEY" -H
 "Content-Type: application/json" -d "{ \"ingest_enabled\": true}"
```