

Aktualisieren Sie die ExtraHop-Firmware über die REST-API

Veröffentlicht: 2024-11-03

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.	<ul style="list-style-type: none"> • Befehlsgerät • Geräte entdecken • Alle Explore-Appliances (Managerknoten, dann Datenknoten)
Entdecken Sie Geräte	siehe ExtraHop-Plattenspeicher aktualisieren .	<ul style="list-style-type: none"> • Appliances verfolgen
Appliances verfolgen	Keine	

Aktualisieren Sie die ExtraHop-Firmware über den REST API Explorer

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 `ebdbbc9e-7113-448c-ab9b-cc0ec2307702`

```
/api/v1/jobs/ebdbbc9e-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 `ebdbbc9e-7113-448c-ab9b-cc0ec2307702`:

```
< Location: /api/v1/jobs/ebdbbc9e-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 RevealX 360-REST-API kompatibel ist. Um dieses Skript mit RevealX 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 TLS-Zertifikatsüberprüfung fehlgeschlagen ist, stellen Sie sicher, dass **Ihrem Sensor oder Ihrer Konsole wurde ein vertrauenswürdigen 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}'
```