Aktualisieren Sie die ExtraHop-Firmware über die REST-API mit ExtraHop Cloud Services

Veröffentlicht: 2024-07-02

Sie können Upgrades der Firmware auf Ihren Appliances über die ExtraHop REST API automatisieren. Sie können auch verfügbare Firmware-Versionen anzeigen und Firmware über die ExtraHop Cloud Services direkt auf Ihr Gerät herunterladen.

Hinweis Bevor Sie die Schritte in diesem Handbuch ausführen können, muss die Appliance mit den ExtraHop Cloud Services verbunden sein. Informationen zum Upgrade ohne ExtraHop Cloud Services finden Sie unter Aktualisieren Sie die ExtraHop-Firmware über die REST-API.

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 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

Verfügbare Firmware-Versionen anzeigen

1. Navigieren Sie in einem Browser zum REST API Explorer.

   Die URL ist der Hostname oder die IP-Adresse Ihres Sensor oder Konsole, gefolgt von `/api/v1/explore/`. Wenn Ihr Hostname beispielsweise seattle-eda ist, lautet die URL `https://seattle-eda/api/v1/explore/`.
2. klicken **API-Schlüssel eingeben** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. klicken **Autorisieren** und dann klicken **Schliessen**.

4. klicken **ExtraHop**.
5. klicken **HOLEN SIE SICH /extrahop/firmware/next**.
6. klicken **Probiere es aus**.
7. klicken **Anfrage senden**.

   Sehen Sie sich im Abschnitt Antworttext die Versionen für jede Freigabe an und notieren Sie sich die Version, auf die Sie aktualisieren möchten.

   Hinweis: Für Sensoren enthält die Liste nur Firmware-Versionen, die mit der Version kompatibel sind, die auf der angeschlossenen Konsole ausgeführt wird.

Laden Sie die Firmware herunter und aktualisieren Sie die Appliance

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

   • **Ausführung:** Die Firmware-Version, auf die Sie aktualisieren möchten.

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

   Das folgende Textfeld aktualisiert die Appliance auf Firmware-Version 8.7.1.1282:

   ```
   {
       "upgrade": true,
       "version": "8.7.1.1282"
   }
   ```

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-cc1ec2407702`:

   ```
   /api/v1/jobs/ebbdbc9e-7113-448c-ab9b-cc1ec2407702
   ```

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.

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 und API-Schlüssel aus einer CSV-Datei liest.

Hinweis: Das Skript deaktiviert die Aufnahme von Datensatz für ExtraHop-Plattenspeicher nicht automatisch. Sie müssen die Aufnahme von Datensatz manuell deaktivieren, bevor Sie das Skript für ExtraHop-Recordstores ausführen.

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.

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

   Sie müssen eines der folgenden Argumente angeben:

   --neuester Hotfix

   Führt ein Upgrade des Systems auf den neuesten Hotfix der Freigabe durch, die derzeit auf dem ExraHop-System installiert ist. Wenn auf dem System beispielsweise Version 8.7.1 ausgeführt wird und die Versionen 8.7.2, 8.7.3, 8.8.0 und 8.8.1 verfügbar sind, wird das System auf 8.7.3 aktualisiert.

   --neuestes Freigabe

   Führt ein Upgrade des Systems auf die neueste Version der neuesten Freigabe durch, auf die das System aktualisiert werden kann. Wenn auf dem System beispielsweise Version 8.7.1 ausgeführt wird und die Versionen 8.7.2, 8.7.3, 8.8.0 und 8.8.1 verfügbar sind, wird das System auf 8.8.1 aktualisiert.

   --version {str}

   Führt ein Upgrade des Systems auf die angegebene Version durch.

   Die folgenden Argumente sind optional:

   --kraft

   Fordert vor dem Upgrade nicht zur Bestätigung auf.

   --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 Appliances beispielsweise auf den neuesten Hotfix der aktuell installierten Freigabe aktualisiert:

   ```
   python3 upgrade_system_cloud.py --latest-hotfix
   ```

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

   Das System zeigt eine Ausgabe an, die dem folgenden Text ähnelt:

   ```
   The following systems will be upgraded:
       extrahop.example.com: 8.7.5.2941
       extrahop.example2.com: 8.7.5.2941
   Do you want to continue?
   y/n
   ```

   Um das System zu aktualisieren, geben Sie y und drücken Sie dann die EINGABETASTE.

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}"
```