Hop supplémentaire 9.6
Guide de l'API REST ExtraHop Trace

Pour plus de documentation, voir https://docs.extrahop.com.

Publié: 2024-04-10

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

Table des matières

Présentation de l'API REST ExtraHop 4
Exigences relatives à l'API ExtraHop 4

Accédez à l'API REST ExtraHop et authentifiez-vous 5
Niveaux de privilèges 5
Gérer l'accès aux clés d'API 8
Génération d'une clé d'API 8
Configurer le partage de ressources entre origines (CORS) 9

En savoir plus sur l'explorateur d'API REST 10
Ouvrez l'explorateur d'API REST 10
Afficher les informations sur les opérations 10
Identifier les objets sur le système ExtraHop 10

Ressources de l'API ExtraHop 13
Clé API 13
Appareil 13
Hop supplémentaire 14
Emplois 15
Licence 15
Configuration en cours 16
Pack de support 16
Utilisateur 16

Exemples d'API REST ExtraHop 18
Mettre à jour le firmware ExtraHop via l'API REST 18
Mettez à niveau le firmware ExtraHop via l'explorateur d'API REST 19
Téléchargez le microprogramme et mettez à niveau l'appliance 19
Surveillez la progression de la tâche de mise à niveau 19
Mettre à jour le firmware ExtraHop avec cURL 19
Récupérez et exécutez l'exemple de script Python 20
Mise à niveau des magasins de disques ExtraHop 21

Présentation de l'API REST ExtraHop

L'API REST ExtraHop vous permet d'automatiser les tâches d'administration et de configuration de votre système ExtraHop. Vous pouvez envoyer des requêtes à l'API ExtraHop via une interface REST (Representational State Transfer), accessible via des URI de ressources et des normes HTTP méthodes.

Lorsqu'une demande d'API REST est envoyée via HTTPS à un système ExtraHop, cette demande est authentifiée puis autorisée via une clé API. Après l'authentification, la demande est soumise au système ExtraHop et l'opération est terminée.

Vidéo: Consultez la formation associée : Présentation de l'API Rest

Chaque système ExtraHop donne accès à l'explorateur d'API ExtraHop REST intégré, qui vous permet de visualiser toutes les ressources, méthodes, propriétés et paramètres système disponibles. L'explorateur d'API REST vous permet également d'envoyer des appels d'API directement à votre système ExtraHop.

Note: Ce guide est destiné à un public ayant une connaissance de base du développement de logiciels et du système ExtraHop.

Exigences relatives à l'API ExtraHop

Avant de pouvoir commencer à écrire des scripts pour l'API REST ExtraHop ou à effectuer des opérations via l'explorateur d'API REST, vous devez satisfaire aux exigences suivantes :

- Votre système ExtraHop doit être configuré pour permettre la génération de clés d'API pour le type d'utilisateur que vous êtes (distant ou local).
- Vous devez générer une clé d'API valide.
- Vous devez avoir un compte utilisateur sur le système ExtraHop avec un compte utilisateur approprié privilèges défini pour le type de tâches que vous souhaitez effectuer.

Accédez à l'API REST ExtraHop et authentifiez-vous

Les utilisateurs de configuration et les utilisateurs dotés de privilèges d'administration du système et d'accès contrôlent si les utilisateurs peuvent générer des clés d'API. Par exemple, vous pouvez empêcher les utilisateurs distants de générer des clés ou vous pouvez désactiver complètement la génération de clés d'API. Lorsque cette fonctionnalité est activée, les clés d'API sont générées par les utilisateurs et ne peuvent être consultées que par l'utilisateur qui les a générées.

Note: Les administrateurs configurent les comptes utilisateurs et attribuent des privilèges, mais les utilisateurs génèrent ensuite leurs propres clés d'API. Les utilisateurs peuvent supprimer les clés d'API pour leur propre compte, et les utilisateurs disposant de privilèges d' administration du système et d'accès peuvent supprimer les clés d'API de n'importe quel utilisateur. Pour plus d'informations, voir Utilisateurs et groupes d'utilisateurs.

Après avoir généré une clé d'API, vous devez l'ajouter aux en-têtes de vos demandes. L' exemple suivant montre une demande qui récupère les métadonnées relatives au microprogramme exécuté sur le système ExtraHop :

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

Niveaux de privilèges

Les niveaux de privilèges utilisateur déterminent les tâches système et d'administration ExtraHop que l'utilisateur peut effectuer via l'API REST ExtraHop.

Vous pouvez consulter les niveaux de privilèges des utilisateurs via `granted_roles` et `effective_roles` propriétés. Le `granted_roles` La propriété vous indique quels niveaux de privilèges sont explicitement accordés à l'utilisateur. Le `effective_roles` La propriété affiche tous les niveaux de privilèges d'un utilisateur, y compris ceux reçus en dehors du rôle accordé, par exemple via un groupe d'utilisateurs.

Le `granted_roles` et `effective_roles` les propriétés sont renvoyées par les opérations suivantes :

- GET /utilisateurs
- GET /users/ {nom d'utilisateur}

Le `granted_roles` et `effective_roles` les propriétés prennent en charge les niveaux de privilèges suivants. Notez que le type de tâches pour chaque système ExtraHop varie en fonction de la disponibilité ressources répertoriés dans l'explorateur d'API REST et dépendent des modules activés sur le système et des privilèges d'accès aux modules utilisateur.

Niveau de privilège	Actions autorisées
« système » : « complet »	• Activez ou désactivez la génération de clés API pour le système ExtraHop. • Générez une clé API. • Consultez les quatre derniers chiffres et la description de chaque clé API du système. • Supprimez les clés d'API de n'importe quel utilisateur. • Afficher et modifier le partage de ressources entre origines. • Effectuez toutes les tâches d'administration disponibles via l'API REST.

Niveau de privilège	Actions autorisées
	• Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « complet »	• Générez votre propre clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez n'importe quelle tâche système ExtraHop disponible via l'API REST.
« write » : « limité »	• Générez une clé API. • Afficher ou supprimer leur propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« write » : « personnel »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez toutes les opérations GET via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « complet »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST. • Effectuez des requêtes métriques et d'enregistrement.
« metrics » : « restreint »	• Générez une clé API. • Consultez ou supprimez votre propre clé API. • Modifiez votre propre mot de passe, mais vous ne pouvez pas effectuer d'autres tâches d'administration via l'API REST.
« ndr » : « complet »	• Afficher les détections de sécurité • Afficher et créer des enquêtes Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« ndr » : « aucun »	• Pas d'accès au contenu du module NDR

Niveau de privilège	Actions autorisées
	Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « complet »	• Afficher les détections de performances • Afficher et créer des tableaux de bord • Afficher et créer des alertes Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« npm » : « aucun »	• Aucun accès au contenu du module NPM Il s'agit d'un privilège d'accès au module qui peut être accordé à un utilisateur en plus de l'un des niveaux de privilège d'accès au système suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « pleins »	• Consultez et téléchargez des paquets via `GET /packets/search` et `POST /packets/search` opérations. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« paquets » : « full_with_keys »	• Consultez et téléchargez les paquets et les clés de session via `GET /packets/search` et `POST /packets/search` opérations.

Niveau de privilège	Actions autorisées
	Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »
« packets » : « slices_only »	• Consultez et téléchargez les 64 premiers octets de paquets via `GET /packets/search` et `POST /packets/search` opérations. Il s'agit d'un privilège supplémentaire qui peut être accordé à un utilisateur disposant de l'un des niveaux de privilège suivants : • « write » : « complet » • « write » : « limité » • « write » : « personnel » • « écrire » : nul • « metrics » : « complet » • « metrics » : « restreint »

Gérer l'accès aux clés d'API

Les utilisateurs disposant de privilèges d'administration du système et des accès peuvent configurer s'ils peuvent générer des clés d'API pour le système ExtraHop. Vous pouvez autoriser uniquement les utilisateurs locaux à générer des clés, ou vous pouvez également désactiver complètement la génération de clés d'API.

Les utilisateurs doivent générer une clé d'API avant de pouvoir effectuer des opérations via l'API REST ExtraHop. Les clés ne peuvent être consultées que par l'utilisateur qui les a générées ou par les administrateurs système dotés de privilèges illimités. Une fois qu'un utilisateur a généré une clé d'API, il doit l'ajouter à ses en-têtes de demande.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez **Accès à l'API**.
3. Dans le Gérer l'accès aux API section, sélectionnez l'une des options suivantes :
   - **Autoriser tous les utilisateurs à générer une clé d'API**: Les utilisateurs locaux et distants peuvent générer des clés d'API.
   - **Seuls les utilisateurs locaux peuvent générer une clé d'API**: Les utilisateurs distants ne peuvent pas générer de clés d'API.
   - **Aucun utilisateur ne peut générer de clé d'API**: aucune clé d'API ne peut être générée par aucun utilisateur.
4. Cliquez **Enregistrer les paramètres**.

Génération d'une clé d'API

Vous devez générer une clé d'API avant de pouvoir effectuer des opérations via l' API REST ExtraHop. Les clés ne peuvent être consultées que par l'utilisateur qui les a générées ou par les utilisateurs disposant de

privilèges d'administration du système et d'accès. Après avoir généré une clé d'API, ajoutez-la à vos en-têtes de demande ou à l'explorateur d'API REST ExtraHop.

Avant de commencer
Assurez-vous que le système ExtraHop est configuré pour permettre la génération de clés d'API.

1. Dans le Paramètres d'accès section, cliquez **Accès à l'API**.
2. Dans le Générer une clé d'API section, tapez une description pour la nouvelle clé, puis cliquez sur **Générer**.
3. Faites défiler la page jusqu'à la section Clés d'API et copiez la clé d'API correspondant à votre description.

Vous pouvez coller la clé dans l'explorateur d'API REST ou l'ajouter à un en-tête de demande.

Configurer le partage de ressources entre origines (CORS)

Partage de ressources entre origines (CORS) vous permet d'accéder à l'API REST ExtraHop au-delà des limites du domaine et à partir de pages Web spécifiées sans que la demande passe par un serveur proxy.

Vous pouvez configurer une ou plusieurs origines autorisées ou autoriser l'accès à l'API REST ExtraHop depuis n'importe quelle origine. Seuls les utilisateurs disposant de privilèges d'administration du système et de l'accès peuvent consulter et modifier les paramètres CORS.

1. Dans le **Paramètres d'accès** section, cliquez sur **Accès à l'API**.
2. Dans le Paramètres CORS section, spécifiez l'une des configurations d'accès suivantes.
   - Pour ajouter une URL spécifique, saisissez une URL d'origine dans la zone de texte, puis cliquez sur l'icône plus (+) ou appuyez sur ENTER.

     L'URL doit inclure un schéma, tel que HTTP ou HTTPS, et le nom de domaine exact. Vous ne pouvez pas ajouter de chemin, mais vous pouvez fournir un numéro de port.
   - Pour autoriser l'accès depuis n'importe quelle URL, sélectionnez Autoriser les requêtes d'API depuis n'importe quelle origine case à cocher.

     Note: Autoriser l'accès à l'API REST depuis n'importe quelle origine est moins sûr que de fournir une liste d' origines explicites.
3. Cliquez **Enregistrer les paramètres** puis cliquez sur **Terminé**.

En savoir plus sur l'explorateur d'API REST

L'explorateur d'API REST est un outil Web qui vous permet d'afficher des informations détaillées sur les ressources, les méthodes, les paramètres, les propriétés et les codes d'erreur de l'API REST ExtraHop. Des exemples de code sont disponibles en Python, cURL et Ruby pour chaque ressource. Vous pouvez également effectuer des opérations directement via l'outil.

Ouvrez l'explorateur d'API REST

Vous pouvez ouvrir l'explorateur d'API REST depuis les paramètres d'administration ou via l'URL suivante :

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

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Accès à l'API**.
3. Sur le Accès à l'API page, cliquez **Explorateur d'API REST**.

   L'explorateur d'API REST s'ouvre dans votre navigateur.

Afficher les informations sur les opérations

Dans l'explorateur d'API REST, vous pouvez cliquer sur n'importe quelle opération pour afficher les informations de configuration de la ressource.

Le tableau suivant fournit des informations sur les sections disponibles pour les ressources dans l'explorateur d' API REST. La disponibilité des sections varie selon la méthode HTTP. Toutes les méthodes ne comportent pas toutes les sections répertoriées dans le tableau.

Rubrique	Descriptif
Paramètres du corps	Fournit tous les champs du corps de la demande et les valeurs prises en charge pour chaque champ.
Paramètres	Fournit des informations sur les paramètres de requête disponibles.
Réponses	Fournit des informations sur les possibilités HTTP codes d'état de la ressource. Si vous cliquez **Envoyer une demande**, cette section inclut également la réponse du serveur ainsi que les syntaxes cURL, Python et Ruby requises pour envoyer la demande spécifiée. **Conseil** Cliquez **Modèle** pour afficher les descriptions des champs renvoyés dans une réponse.

Identifier les objets sur le système ExtraHop

Les objets du système ExtraHop peuvent être identifiés par n'importe quelle valeur unique, telle que l' adresse IP, l'adresse MAC, le nom ou l'identifiant du système. Toutefois, pour effectuer des opérations d'API sur un objet spécifique, vous devez localiser l'ID de l'objet. Vous pouvez facilement localiser l'ID de l'objet à l'aide des méthodes suivantes dans l'explorateur d'API REST.

- L'identifiant de l'objet est fourni dans les en-têtes renvoyés par une requête POST. Par exemple, si vous envoyez une requête POST pour créer une page, les en-têtes de réponse affichent une URL de localisation.

  La demande suivante a renvoyé l'emplacement de la balise nouvellement créée sous la forme `/api/v1/tags/1` et l'identifiant du tag sous la forme `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"
}
```

- L'ID d'objet est fourni pour tous les objets renvoyés par une requête GET. Par exemple, si vous exécutez une requête GET sur tous les appareils, le corps de la réponse contient des informations pour chaque équipement, y compris l'identifiant.

  Le corps de réponse suivant affiche une entrée pour un seul équipement, avec un ID de 10212 :

```
{
 "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
},
```

- L'ID de l'objet est fourni dans l'URL de la plupart des objets. Par exemple, dans le système ExtraHop, cliquez sur **Actifs**, puis **Appareils**. Sélectionnez n'importe quel équipement et consultez l'URL. Dans l'exemple suivant, l'URL de la page de l'équipement indique Oid=10180.

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

  Pour effectuer des demandes spécifiques pour cet équipement, ajoutez 10180 au identifiant champ dans l'explorateur d'API REST ou dans le paramètre body de votre demande.

L'URL pour tableaux de bord affiche un short_code, qui apparaît après /Dashboard. Lorsque vous ajoutez le short_code à l'explorateur d'API REST ou à votre demande, vous devez ajouter un tilde au code court.

Dans l'exemple suivant, KMC9y est le short_code. Pour effectuer des demandes pour ce tableau de bord, ajoutez `~kmC9Y` comme valeur du champ short_code.

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

Vous pouvez également trouver le short_code et l'ID du tableau de bord dans les propriétés du tableau de bord de tout tableau de bord, accessibles depuis le menu de commande ⋮. Certaines opérations d'API, telles que DELETE, nécessitent l'ID du tableau de bord.

Ressources de l'API ExtraHop

Vous pouvez effectuer des opérations sur les ressources suivantes via l'API REST ExtraHop. Vous pouvez également consulter des informations plus détaillées sur ces ressources, telles que disponibles HTTP méthodes, paramètres de requête et propriétés d'objet dans l'explorateur d'API REST.

Clé API

Une clé d'API permet à un utilisateur d'effectuer des opérations via l'API REST ExtraHop.

Vous pouvez générer la clé d'API initiale pour le compte utilisateur configuré via l'API REST. Toutes les autres clés d' API sont générées via la page Accès aux API dans les paramètres d'administration.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
OBTENEZ /apikeys	Récupérez toutes les clés d'API.
POST/apikeys	Créez la clé d'API initiale pour le compte utilisateur configuré.
OBTENEZ /apikeys/ {keyid}	Récupérez les informations relatives à une clé d'API spécifique.

Appareil

Le système ExtraHop consiste en un réseau d'appareils ExtraHop connectés, tels que capteurs, consoles, des magasins de disques et des magasins de paquets qui exécutent des tâches telles que la surveillance du trafic, l' analyse des données, le stockage des données et l'identification des détections.

Vous pouvez récupérer des informations et établir des connexions pour les appareils ExtraHop locaux et distants.

Note: Vous ne pouvez établir une connexion qu'entre des appliances ExtraHop similaires, telles que Reveal (x) Enterprise ou Performance.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
GET /appareils	Récupérez tous les appareils ExtraHop distants connectés à l'appareil local.
POST /appareils	Établissez une nouvelle connexion à une appliance ExtraHop distante.
SUPPRIMER /appliances/ {id}	Déconnectez un appareil ExtraHop spécifique de ce console.
OBTENEZ /appliances/ {id}	Récupérez une appliance ExtraHop distante spécifique connectée à l'appliance locale (valable uniquement sur les consoles).
GET /appliances/ {id} /services cloud	Récupérez l'état des services cloud ExtraHop sur cette appliance (valable uniquement sur les consoles).

Fonctionnement	Descriptif
OBTENEZ /appliances/ {id} /productkey	Récupérez la clé de produit pour une appliance spécifiée (valable uniquement sur les consoles).
GET /appareils/ {ids_id} /association	Récupérez l'ID du réseau danalyse de paquets auquel le capteur IDS est joint.
POST /appareils/ {ids_id} /association	Associez une sonde IDS à une sonde réseau danalyse de paquets.
GET /appareils/firmware/next	Récupérez les versions du microprogramme vers lesquelles les systèmes ExtraHop distants peuvent être mis à niveau (valable uniquement sur les consoles).
POST /appareils/firmware/mise à niveau	Mettez à jour le microprogramme sur les systèmes ExtraHop distants connectés au système local. Les images du firmware sont téléchargées depuis ExtraHop Cloud Services (uniquement valables sur les consoles).
`GET /appliances/{ids_id}/association`	Récupérez l'ID du réseau danalyse de paquets auquel le capteur IDS est joint (valide uniquement sur les consoles).
`POST /appliances/{ids_id}/association`	Associez une sonde IDS à une sonde réseau danalyse de paquets (valable uniquement sur les consoles).

Hop supplémentaire

Cette ressource fournit des métadonnées sur le système ExtraHop.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
OBTIENDREZ /extrahop	Récupérez les métadonnées relatives au microprogramme exécuté sur le système ExtraHop.
GET /extrahop/édition	Récupérez l'édition du système ExtraHop.
POST/extrahop/firmware	Téléchargez une nouvelle image du firmware sur le système ExtraHop. Pour plus d' informations, voir Mettre à jour le firmware ExtraHop via l'API REST.
POST/extrahop/firmware/téléchargement/URL	Téléchargez une nouvelle image du firmware sur le système ExtraHop à partir d'une URL.
POST /extrahop/firmware/dernier/mise à niveau	Mettez à niveau le système ExtraHop vers la dernière image du firmware téléchargée.
OBTENEZ /extrahop/idrac	Récupérez l'adresse IP iDRAC du système ExtraHop.
GET/extrahop/platform	Récupérez le nom de plateforme du système ExtraHop.
GET /extrahop/process	Récupérez une liste des processus exécutés sur le système ExtraHop.

Fonctionnement	Descriptif
POST /extrahop/processes/ {process} /restart	Redémarrez un processus en cours d'exécution sur le système ExtraHop.
OBTENEZ /extrahop/services	Récupérez les paramètres de tous les services.
PATCH /extrahop/services	Mettez à jour les paramètres des services.
POST /extrahop/restart	Redémarrez le système ExtraHop.
PUBLIEZ /extrahop/sslcert	Régénérez le certificat SSL sur le système ExtraHop. Pour plus d' informations, voir Créez un certificat SSL fiable via l'API REST
PUT /extrahop/sslcert	Remplacez le certificat SSL sur le système ExtraHop.
POST /extrahop/sslcert/signingrequest	Créez une demande de signature de certificat SSL. Pour plus d'informations, voir Créez un certificat SSL fiable via l'API REST.
RECEVEZ /extrahop/billetterie	Récupérez le statut de l'intégration de la billetterie.
PATCH /extrahop/billetterie	Activez ou désactivez l'intégration de la billetterie.
OBTENEZ /extrahop/version	Récupérez la version du firmware exécuté sur le système ExtraHop.

Les informations d'implémentation et les instructions pour chaque opération sont documentées dans l'explorateur d'API REST. Vous pouvez cliquer sur n'importe quelle opération dans l'explorateur d'API REST pour afficher les informations d' implémentation telles que les paramètres, la classe de réponse et les messages, ainsi que le modèle et le schéma JSON.

Emplois

Vous pouvez suivre la progression de certaines tâches d'administration lancées via l' API REST. Si une requête REST crée une tâche, l'ID de la tâche est renvoyé dans le `location` en-tête de la réponse. Les opérations suivantes créent des emplois :

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

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
OBTENIR /jobs	Récupérez le statut de toutes les tâches.
GET /jobs/ {id}	Récupérez le statut d'une tâche spécifique.

Licence

Cette ressource vous permet de récupérer et de définir des clés de produit ou de récupérer et de définir une licence.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
GET /licence	Récupérez la licence appliquée à ce système ExtraHop.

Fonctionnement	Descriptif
PUT/licence	Appliquez et enregistrez une nouvelle licence sur le système ExtraHop.
OBTENIR /license/clé de produit	Récupérez la clé de produit de ce système ExtraHop.
PUT/licence/clé de produit	Appliquez la clé de produit spécifiée au système ExtraHop et enregistrez la licence.

Configuration en cours

Le fichier de configuration en cours est un document JSON qui contient des informations de configuration système de base pour le système ExtraHop.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
OBTENEZ /runningconfig	Récupérez le fichier de configuration en cours d'exécution.
PUT/runningconfig	Remplacez le fichier de configuration en cours d'exécution. Les modifications du fichier de configuration ne sont pas enregistrées automatiquement.
POST/runningconfig/save	Enregistrez les modifications actuelles dans le fichier de configuration en cours d'exécution.
OBTENEZ /runningconfig/saved	Récupérez le fichier de configuration en cours d'exécution enregistré.

Pack de support

Un pack de support est un fichier contenant les ajustements de configuration fournis par ExtraHop Support.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
GET/supportpacks	Récupérez les métadonnées de tous les packs de support.
POST/Supportpacks	Téléchargez et exécutez un pack de support.
POST /supportpacks/execute	Exécutez un nouveau pack de support.
GET /supportpacks/queue/ {id}	Vérifiez l'état d'un pack de support en cours d'exécution.
GET /supportpacks/ {nom de fichier}	Téléchargez un pack de support existant par nom de fichier.

Utilisateur

La ressource utilisateur vous permet de créer et de gérer la liste des utilisateurs ayant accès au système ExtraHop et les niveaux de privilège de ces utilisateurs.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur cette ressource :

Fonctionnement	Descriptif
GET /utilisateurs	Récupérez tous les utilisateurs.
POST/utilisateurs	Créez un nouvel utilisateur.
SUPPRIMER /users/ {nom d'utilisateur}	Supprimez un utilisateur spécifique.
GET /users/ {nom d'utilisateur}	Récupérez un utilisateur spécifique.
PATCH /users/ {nom d'utilisateur}	Mettez à jour les paramètres d'un utilisateur spécifique.
GET /users/ {nom d'utilisateur} /apikeys	Récupérez toutes les clés d'API pour un utilisateur spécifique.
GET /users/ {nom d'utilisateur} /apikeys/ {keyid}	Récupérez des informations sur une clé d'API et un utilisateur spécifiques.

Exemples d'API REST ExtraHop

Les exemples suivants illustrent les opérations courantes de l'API REST.

- Modifier le propriétaire d'un tableau de bord via l'API REST
- Extrayez la liste des équipements via l'API REST
- Création et attribution d'une étiquette d'équipement via l'API REST
- Requête de métriques relatives à un équipement spécifique via l'API REST
- Création, récupération et suppression d'un objet via l'API REST
- Interroger le journal des enregistrements

Mettre à jour le firmware ExtraHop via l'API REST

Vous pouvez automatiser les mises à niveau du micrologiciel de vos appareils ExtraHop via l'API REST ExtraHop. Ce guide fournit des instructions pour effectuer une mise à niveau via l' explorateur d'API REST, une commande cURL et un script Python.

Note: Si votre appareil est connecté à ExtraHop Cloud Services, vous pouvez simplifier le processus de mise à niveau en consultant les versions de firmware disponibles et en téléchargeant le firmware directement sur le système depuis ExtraHop Cloud Services. Pour plus d'informations, voir Mettez à niveau le firmware ExtraHop via l'API REST avec ExtraHop Cloud Services.

Bien que le processus de mise à niveau du microprogramme soit similaire sur tous les appareils ExtraHop, certains appareils comportent des considérations ou étapes supplémentaires que vous devez prendre en compte avant d'installer le microprogramme dans votre environnement. Si vous avez besoin d' aide pour votre mise à niveau, contactez le support ExtraHop.

Tous les appareils doivent répondre aux exigences suivantes :

- La version du microprogramme doit être compatible avec le modèle de votre appareil.
- La version du microprogramme de votre appliance doit être prise en charge par la version de mise à niveau.
- Les appareils de commande doivent exécuter un microprogramme supérieur ou égal à celui des appareils connectés.
- Les appliances Discover doivent exécuter un microprogramme supérieur ou égal à celui des appliances Explore and Trace connectées.

Si votre déploiement inclut uniquement un sonde, passez au Explorateur d'API, cURL ou Python instructions de mise à niveau.

Si votre déploiement inclut des types d'appareils supplémentaires, vous devez résoudre les dépendances suivantes avant de suivre les instructions de mise à niveau.

Si votre déploiement inclut...	Tâches préalables à la mise	Ordre de mise à niveau
Appareils de commande	Réservez une fenêtre de maintenance d'une heure pour les appareils Command gérant 50 000 appareils ou plus.	• Appareil de commande • Découvrez les appareils • Toutes les appliances Explore (nœuds de gestion, puis nœuds de données) • Appareils Trace
Découvrez les appareils	Voir Mise à niveau des magasins de disques ExtraHop.	
Appareils Trace	Aucune	

Mettez à niveau le firmware ExtraHop via l'explorateur d'API REST

Téléchargez le microprogramme et mettez à niveau l'appliance

1. Cliquez **POST/extrahop/firmware/téléchargement/url**.
2. Cliquez **Essayez-le**.
3. Dans le champ body, spécifiez les champs suivants :

   • **URL_du microprogramme:** URL à partir de laquelle le fichier .tar du microprogramme peut être téléchargé.

   • **mettre à niveau:** Indique s'il convient de mettre à niveau l'appliance une fois le téléchargement du microprogramme terminé. Définissez ce champ sur `true`.

   Le champ body doit ressembler à l'exemple de texte suivant :

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

4. Cliquez **Envoyer une demande**.

   Dans les en-têtes de réponse, notez la valeur située après la dernière barre oblique `location` en-tête. Vous aurez besoin de cette valeur pour suivre la progression de la tâche de mise à niveau. Par exemple, l'ID de tâche dans l'exemple suivant est `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`

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

Surveillez la progression de la tâche de mise à niveau

1. Cliquez **Emplois**.
2. Cliquez **GET /jobs/ {id}**.
3. Dans le champ id, saisissez la valeur que vous avez copiée depuis `location` en-tête de la tâche précédente.
4. Cliquez **Envoyer une demande**.
5. Dans le corps de la réponse, consultez les informations relatives à la tâche.

   Le `status` le champ est `DONE` lorsque le travail est terminé.

Mettre à jour le firmware ExtraHop avec cURL

Vous pouvez mettre à jour le microprogramme d'une appliance à l'aide de la commande cURL.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- Le fichier .tar du microprogramme du système doit être téléchargé sur votre machine.

1. Ouvrez une application de terminal.
2. Téléchargez le microprogramme et mettez à niveau l'appliance.

   Exécutez la commande suivante, où `YOUR_KEY` est la clé API de votre compte utilisateur, `HOSTNAME` est le nom d'hôte de votre appliance ExtraHop, et `FIRMWARE_URL` est l'URL à partir de laquelle le fichier .tar du microprogramme peut être téléchargé :

   ```
   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\"}"
   ```

Dans la sortie de commande, notez l'ID de la tâche dans l'en-tête Location. Par exemple, l'ID de tâche dans l'exemple suivant est `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`:

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

3. Surveillez la progression de la tâche de mise à niveau.

   Exécutez la commande suivante, où `YOUR_KEY` est la clé API de votre compte utilisateur `HOSTNAME` est le nom d'hôte de votre appliance, et `JOB_ID` est l'identifiant que vous avez enregistré à l' étape précédente :

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

   La commande affiche un objet contenant des informations sur la tâche de mise à niveau. La mise à niveau est terminée lorsque le `status` le champ est `DONE`. Si la mise à niveau n'est pas terminée, attendez quelques minutes et réexécutez la commande.

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub d'ExtraHop contient un exemple de script Python qui met à niveau plusieurs appareils en lisant les URL, les clés d'API et les chemins de fichiers du microprogramme à partir d'un fichier CSV.

Important: L'exemple de script python s'authentifie auprès de la sonde ou de la console via une clé API, qui n'est pas compatible avec l' API REST Reveal (x) 360. Pour exécuter ce script avec Reveal (x) 360, vous devez modifier le script pour vous authentifier à l'aide de jetons d'API. Consultez les py_rx360_auth.py script dans le référentiel GitHub d'ExtraHop pour un exemple d'authentification à l'aide de jetons d'API.

Note: Le script ne désactive pas automatiquement l'ingestion d'enregistrements pour les magasins de disques ExtraHop. Vous devez désactiver manuellement l' ingestion d'enregistrements avant d'exécuter le script pour un magasin de disques ExtraHop.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le contenu du répertoire upgrade_system sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `systems.csv` archivez et remplacez les valeurs d' exemple par les noms d'hôte et les clés d'API de vos appliances.
3. Exécutez le `upgrade_system_url.py` script.

   Les arguments suivants sont facultatifs :

   --max-threads {int}

   Spécifie le nombre maximum de threads simultanés. La valeur par défaut est 2.

   --wait {float}

   Spécifie le nombre de minutes à attendre avant de vérifier la progression d'une tâche de mise à niveau. La valeur par défaut est 0,5.

   Par exemple, la commande suivante met à niveau un maximum de 3 appliances à la fois :

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

   Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat SSL a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter le `verify=False` option permettant de contourner la vérification des certificats. Cependant, cette méthode n'est pas sûre et n'est pas recommandée. Le code suivant envoie une requête HTTP GET sans vérification du certificat :

   ```
   requests.get(url, headers=headers, verify=False)
   ```

Mise à niveau des magasins de disques ExtraHop

Tâches préalables à la mise

Avant de mettre à niveau un espace de stockage des enregistrements ExtraHop, vous devez arrêter l'ingestion d'enregistrements. Vous pouvez arrêter l' acquisition d'enregistrements pour tous les nœuds d'un cluster à partir d'un seul nœud.

Note: Le message `Could not determine ingest status on some nodes` et `Error` peut apparaître sur la page Gestion des données du cluster dans les paramètres d'administration des nœuds mis à niveau jusqu'à ce que tous les nœuds du cluster soient mis à niveau. Ces erreurs sont attendues et peuvent être ignorées.

1. Ouvrez une application de terminal.
2. Exécutez la commande suivante, où `YOUR_KEY` est l'API de votre compte utilisateur, et `HOSTNAME` est le nom d'hôte de votre espace de stockage des enregistrements ExtraHop :

```
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}"
```

Tâches post-mise à niveau

Après avoir mis à niveau tous les nœuds du cluster d'espace de stockage des enregistrements, activez l' ingestion d'enregistrements.

1. Ouvrez une application de terminal.
2. Exécutez la commande suivante, où `YOUR_KEY` est l'API de votre compte utilisateur, et `HOSTNAME` est le nom d'hôte de votre espace de stockage des enregistrements ExtraHop :

```
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}"
```