Hop supplémentaire 25.2
Guide de l'API REST ExtraHop

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

Publié: 2025-03-28

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 6
Exigences relatives à l'API ExtraHop 6

Accédez à l'API REST ExtraHop et authentifiez-vous 7
Niveaux de privilèges 7
Gérer l'accès aux clés d'API 10
Générer une clé API 10
Configurer le partage de ressources entre origines (CORS) 11
Configurer un certificat TLS 11

En savoir plus sur l'explorateur d'API REST 13
Ouvrez l'explorateur d'API REST 13
Afficher les informations sur les opérations 13
Identifier les objets sur le système ExtraHop 13

Ressources de l'API ExtraHop 15
Carte des activités 15
 Détails de l'opération 16
Alerte 23
 Détails de l'opération 24
 Niveaux de gravité des alertes 34
Priorité d'analyse 35
 Détails de l'opération 35
Clé API 37
 Détails de l'opération 37
Appareil 38
 Détails de l'opération 39
Demande 44
 Détails de l'opération 45
Journal d'audit 49
 Détails de l'opération 49
Auth 49
 Détails de l'opération 50
Forfait 52
 Détails de l'opération 52
Nuage 54
 Détails de l'opération 54
équipement personnalisé 55
 Détails de l'opération 55
Personnalisation 58
 Détails de l'opération 58
Tableaux de bord 59
 Détails de l'opération 60
Appareil 62
 Détails de l'opération 63
 Valeurs d'opérandes pour la recherche d'équipements 74
 Unités de temps prises en charge 81
Groupe d'appareils 82

Détails de l'opération 83
Unités de temps prises en charge 91
Valeurs d'opérandes pour les groupes d'équipements 92
Détections 97
Détails de l'opération 98
Valeurs d'opérande pour les règles de réglage des propriétés de détection 114
Catégories de détection 116
Groupe de messagerie 117
Détails de l'opération 117
Intervalles d'exclusion 118
Détails de l'opération 119
ExtraHop 121
Détails de l'opération 122
Enquêtes 130
Détails de l'opération 131
Emplois 134
Détails de l'opération 134
Types d'emplois 135
Licence 135
Détails de l'opération 136
Métriques 136
Détails de l'opération 140
Unités de temps prises en charge 145
Réseau 146
Détails de l'opération 147
Entrée de localité du réseau 149
Détails de l'opération 149
Nœud 151
Détails de l'opération 151
Observations 152
Détails de l'opération 152
Flux de données ouvert 153
Détails de l'opération 154
Recherche par paquets 164
Détails de l'opération 164
Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley 167
Ajouter un filtre avec la syntaxe BPF 168
Syntaxe BPF prise en charge 168
Couplage 170
Détails de l'opération 170
Journal des enregistrements 170
Détails de l'opération 171
Valeurs des opérandes dans les requêtes d'enregistrement 174
Interrogez les enregistrements à l'aide d'un filtre de groupe déquipements 175
Interroger les enregistrements à l'aide d'un filtre de localité du réseau 176
Unités de temps prises en charge 176
Rapport 177
Détails de l'opération 178
Configuration en cours 186
Détails de l'opération 186
Logiciel 187
Détails de l'opération 187
Clé de déchiffrement TLS 187
Détails de l'opération 188
Pack de support 190
Détails de l'opération 190

Tag 191
Détails de l'opération 192
Collecte des menaces 194
Détails de l'opération 194
Gâchette 195
Détails de l'opération 196
Options de déclencheur avancées 200
Utilisateur 203
Détails de l'opération 204
Groupe d'utilisateurs 206
Détails de l'opération 207
VLAN 209
Détails de l'opération 210
Liste de surveillance 210
Détails de l'opération 211

Exemples d'API REST ExtraHop 212

Mettre à jour le firmware ExtraHop via l'API REST 212
Mettez à niveau le firmware ExtraHop via l'explorateur d'API REST 213
Téléchargez le microprogramme et mettez à niveau l'appliance 213
Surveillez la progression de la tâche de mise à niveau 213
Mettre à jour le firmware ExtraHop avec cURL 213
Récupérez et exécutez l'exemple de script Python 214
Mise à niveau des magasins de disques ExtraHop 215
Modifier le propriétaire d'un tableau de bord via l'API REST 215
Récupérez les identifiants du tableau de bord 215
Changer le propriétaire du tableau de bord 216
Exemple de script Python 218
Extraire la liste des équipements via l'API REST 218
Récupérez la liste des équipements à l'aide de la commande cURL 218
Récupérez la liste des équipements depuis RevealX 360 à l'aide de la commande cURL 220
Récupérez et exécutez l'exemple de script Python 221
Créez un certificat TLS fiable via l'API REST 222
Création d'une demande de signature de certificat TLS 222
Ajoutez un certificat TLS fiable à votre sonde ou à votre console 224
Créez des appareils personnalisés via l'API REST 225
Créez un équipement personnalisé via l'explorateur d'API REST 225
Récupérez et exécutez l'exemple de script Python 225
Création et attribution d'une étiquette d'équipement via l'API REST 226
Requête de métriques relatives à un équipement spécifique via l'API REST 228
Création, récupération et suppression d'un objet via l'API REST 229
Interroger le journal des enregistrements 230

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**.

Générer une clé 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 des accès. Après avoir généré une clé d'API, ajoutez-la à vos en-têtes de demande ou à l'explorateur d'API ExtraHop REST.

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 sur **Accès à l'API**.
2. Dans le Générer une clé API section, tapez la description de la nouvelle clé, puis cliquez sur **Générez**.
3. Faites défiler l'écran vers le bas jusqu'à Clés d'API section et copiez la clé API qui correspond 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. 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 sur **Accès à l'API**.
3. 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.
4. Cliquez **Enregistrer les paramètres** puis cliquez sur **Terminé**.

Configurer un certificat TLS

Avant d'adresser des requêtes à un système ExtraHop doté d'un certificat auto-signé, vous devez configurer un certificat TLS pour chaque utilisateur qui accédera au système ExtraHop depuis un ordinateur spécifique.

Dans chacun des exemples suivants, remplacez {HOST} par le nom d'hôte de votre système ExtraHop.

Note: Le certificat TLS s'applique uniquement à l'utilisateur qui exécute la commande. Chaque utilisateur doit exécuter la commande avec ses informations dcessaires d'identification pour configurer le certificat TLS.

Configuration du protocole TLS via Windows PowerShell

```
Invoke-WebRequest "http://{HOST}/public.cer" -OutFile ($env:USERPROFILE +
"\ex.cer"); Import-Certificate ($env:USERPROFILE + "\ex.cer")
-CertStoreLocation Cert:\CurrentUser\Root
```

Configuration du protocole TLS via OS X

```
curl -O http://{HOST}/public.cer; security add-trusted-cert -r trustRoot -k
~/Library/Keychains/login.keychain public.cer
```

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

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'ID 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 de la balise comme `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 son 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
},
```

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.

Carte des activités

Une carte dactivity est une représentation visuelle dynamique de l'activité du protocole L4-L7 entre les appareils de votre réseau. Créez un schéma 2D ou 3D des connexions des équipements en temps réel pour en savoir plus sur le flux de trafic et les relations entre les appareils.

Voici quelques points importants à prendre en compte au sujet des cartes d'activités :

- Vous ne pouvez créer des cartes d'activité pour les appareils que dans l'analyse standard et l'analyse avancée. Les appareils en mode découverte ne sont pas inclus dans les cartes d'activités. Pour plus d'informations, voir Niveaux d'analyse.
- Si vous créez une carte d'activités pour un équipement, un groupe d'activités ou un groupe d'équipements sans aucune activité de protocole pendant l'intervalle de temps sélectionné, la carte apparaît sans aucune donnée. Modifiez l'intervalle de temps ou votre sélection d'origine et réessayez.
- Vous pouvez créer une carte dactivitiés dans un console pour visualiser les connexions des équipements entre tous vos capteurs.

Pour en savoir plus sur la configuration et la navigation dans les cartes d'activité, voir Cartes d'activités.

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

Fonctionnement	Descriptif
OBTENIR /activitymaps	Récupérez toutes les cartes d'activités.
POST/Activitymaps	Créez une nouvelle carte dactivitiés.
POST /activitymaps/query	Exécutez une requête de topologie du réseau, qui renvoie les données de la carte dactivités sous forme de fichier plat.
SUPPRIMER /activitymaps/ {id}	Supprimez une carte dactivitiés spécifique.
OBTENEZ /activitymaps/ {id}	Récupérez une carte dactivitiés spécifique.
PATCH /activitymaps/ {id}	Mettez à jour une carte dactivitiés spécifique.
POST /activitymaps/ {id} /requête	Exécutez une requête topologique pour une carte d'activités spécifique, qui renvoie les données de la carte d'activités sous forme de fichier plat.
GET /activitymaps/ {id} /partage	Récupérez les utilisateurs et leurs autorisations de partage pour une carte dactivitiés spécifique.
PATCH /activitymaps/ {id} /partage	Mettez à jour les utilisateurs et leurs autorisations de partage pour une carte dactivitiés spécifique.
PUT /activitymaps/ {id} /partage	Remplacez les utilisateurs et leurs autorisations de partage pour une carte dactivitiés spécifique.

Détails de l'opération

`POST /activitymaps`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de la carte dactivities.

`name:` ***Corde***

Nom convivial de la carte dactivités.

`short_code:` ***Corde***

(Facultatif) Le code abrégé unique qui est global à toutes les cartes d'activités.

`description:` ***Corde***

Description de la carte dactivitiés.

`weighting:` ***Corde***

(Facultatif) La valeur métrique qui détermine la pondération de l'activité entre les appareils. Les valeurs d'élément prises en charge sont « bytes », « connections » et « turns ».

`mode:` ***Corde***

(Facultatif) La mise en page de la carte dactivités. Les valeurs prises en charge sont « 2dforce » et « 3dforce ».

`show_alert_status:` ***Booléen***

(Facultatif) Indique s'il faut afficher l'état d'alerte des appareils sur la carte dactivités. Si cette option est activée, la couleur de chaque équipement sur la carte représente le niveau d'alerte le plus grave associé à l'équipement.

`walks:` ***Tableau d'objets***

La liste d'un ou de plusieurs objets de promenade. Une promenade est le chemin de circulation composé d'une ou de plusieurs marches. Chaque étape commence par un ou plusieurs appareils d'origine et s'étend aux connexions aux appareils homologues basées sur l'activité du protocole. Chaque extension depuis l'origine est une étape. Le contenu de l'objet est défini dans la section « promenade » ci-dessous.

`origins:` ***Tableau d'objets***

La liste d'un ou de plusieurs appareils d'origine de la première étape de la promenade. Le contenu de l'objet est défini dans la section « source_object » ci-dessous.

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

`steps:` ***Tableau d'objets***

La liste d'une ou de plusieurs étapes de la promenade. Chaque étape est définie par l'activité du protocole entre les appareils de l'étape précédente et un nouvel ensemble de périphériques homologues. Le contenu de l'objet est défini dans la section « étape » ci-dessous.

`relationships:` ***Tableau d'objets***

(Facultatif) Liste d'un ou de plusieurs filtres qui définissent la relation entre deux appareils. Les filtres spécifient les rôles et les protocoles à rechercher lors de la localisation des appareils homologues au cours de l'étape. Les relations sont

représentées sous forme d'arête sur la carte dactivités. Le contenu de l'objet est défini dans la section « relation » ci-dessous. Si aucune valeur n'est spécifiée, l'opération localisera tous les homologues.

`protocol:` ***Corde***

(Facultatif) Le protocole métrique associé à la relation, tel que « HTTP » ou « DNS ». L'opération localise uniquement les connexions entre les appareils via le protocole spécifié.

`role:` ***Corde***

(Facultatif) Rôle d'équipement associé au protocole métrique de la relation. L'opération localise uniquement les connexions entre les appareils via le protocole associé dans le rôle spécifié. Les valeurs de rôle prises en charge sont « client », « serveur » ou « quelconque ». Définissez sur « any » pour localiser toutes les relations client, serveur et équipement homologue associées au protocole spécifié.

`peer_in:` ***Tableau d'objets***

(Facultatif) Liste d'un ou de plusieurs objets d'équipement homologues à inclure dans la carte dactivités. Seules les relations avec les homologues de l'objet source spécifié sont incluses. Le contenu de l'objet est défini dans la section « source_object » ci-dessous.

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

`peer_not_in:` ***Tableau d'objets***

(Facultatif) Liste d'un ou de plusieurs objets d'équipement homologues à exclure de la carte dactivités. Les relations avec les homologues de l'objet source spécifié sont exclues. Le contenu de l'objet est défini dans la section « source_object » ci-dessous.

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "mode": "string",
    "name": "string",
    "short_code": "string",
    "show_alert_status": true,
    "walks": {
        "origins": {
            "object_type": "string",
            "object_id": 0
        },
```

```
        "steps": {
            "relationships": {
                "protocol": "string",
                "role": "string"
            },
            "peer_in": {
                "object_type": "string",
                "object_id": 0
            },
            "peer_not_in": {
                "object_type": "string",
                "object_id": 0
            }
        }
    },
    "weighting": "string"
}
```

`POST /activitymaps/query`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de la requête topologique.

`from:` ***Numéro***

L'horodateur de début de la plage temporelle recherchée par la requête, exprimé en millisecondes depuis l'époque.

`until:` ***Numéro***

(Facultatif) L'horodateur de fin de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Si aucune valeur n'est définie, la fin de la requête est par défaut « maintenant ».

`weighting:` ***Corde***

(Facultatif) La valeur métrique qui détermine la pondération de l'activité entre les appareils.

Les valeurs suivantes sont valides :

- `bytes`
- `connections`
- `turns`

`edge_annotations:` ***Tableau de chaînes***

(Facultatif) La liste d'une ou plusieurs annotations de bord à inclure dans la requête topologique.

Les valeurs suivantes sont valides :

- `protocols`
- `appearances`

`walks:` ***Tableau d'objets***

Liste d'un ou de plusieurs objets de promenade à inclure dans la requête topologique. Une promenade est le chemin de circulation composé d'une ou de plusieurs marches. Chaque étape commence par un ou plusieurs appareils d'origine et s'étend aux connexions aux appareils homologues basées sur l'activité du protocole. Chaque extension depuis l'origine est une étape. Le contenu de l'objet est défini dans la section « topology_walk » ci-dessous.

`origins:` ***Tableau d'objets***

La liste d'un ou de plusieurs appareils d'origine de la première étape de la promenade. Le contenu de l'objet est défini dans la section « topology_source » ci-dessous.

`object_type:` ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

- `all_devices`
- `device_group`
- `device`

`object_id:` ***Numéro***

Identifiant unique de l'objet source. Défini sur 0 si la valeur du paramètre « object_type » est « all_devices ».

`steps:` ***Tableau d'objets***

La liste d'une ou de plusieurs étapes de la promenade. Chaque étape est définie par l'activité du protocole entre les appareils de l'étape précédente et un nouvel ensemble de périphériques homologues. Le contenu de l'objet est défini dans la section « topology_step » ci-dessous.

`relationships:` ***Tableau d'objets***

(Facultatif) Liste d'un ou de plusieurs filtres qui définissent la relation entre deux appareils. Les filtres spécifient les rôles et les protocoles à rechercher lors de la localisation des appareils homologues au cours de l'étape. Les relations sont représentées sous forme d'arête sur la carte dactivités. Si aucune valeur n'est définie, l'opération inclut tous les homologues. Le contenu de l'objet est défini dans la section « topology_relationship » ci-dessous.

`role:` ***Corde***

(Facultatif) Le rôle de l'équipement homologue par rapport à l'équipement d'origine.

Les valeurs suivantes sont valides :

- `client`
- `server`
- `any`

`protocol:` ***Corde***

(Facultatif) Le protocole par lequel l'équipement d'origine communique, tel que « HTTP ». Si aucune valeur n'est définie, l'objet inclut un protocole.

`peer_in:` ***Tableau d'objets***

(Facultatif) La liste d'un ou de plusieurs appareils homologues à inclure dans le graphe topologique. Seules les relations avec les homologues de l'objet source spécifié sont incluses. Le contenu de l'objet est défini dans la section « topology_source » ci-dessous.

`object_type:` ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

- `all_devices`
- `device_group`
- `device`

`object_id:` ***Numéro***

Identifiant unique de l'objet source. Défini sur 0 si la valeur du paramètre « object_type » est « all_devices ».

`peer_not_in`: ***Tableau d'objets***

(Facultatif) La liste d'un ou de plusieurs appareils homologues à exclure du graphe topologique. Les relations avec les appareils homologues de l'objet source spécifié sont exclues. Le contenu de l'objet est défini dans la section « topology_source » ci-dessous.

`object_type`: ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

- `all_devices`
- `device_group`
- `device`

`object_id`: ***Numéro***

Identifiant unique de l'objet source. Défini sur 0 si la valeur du paramètre « object_type » est « all_devices ».

Spécifiez le paramètre body au format JSON suivant.

```
{
    "edge_annotations": [],
    "from": 0,
    "until": 0,
    "walks": {
        "origins": {
            "object_type": "string",
            "object_id": 0
        },
        "steps": {
            "relationships": {
                "role": "string",
                "protocol": "string"
            },
            "peer_in": {
                "object_type": "string",
                "object_id": 0
            },
            "peer_not_in": {
                "object_type": "string",
                "object_id": 0
            }
        }
    },
    "weighting": "string"
}
```

`GET /activitymaps`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "mode": "string",
    "name": "string",
    "owner": "string",
    "rights": [
```

```
        "string"
    ],
    "short_code": "string",
    "show_alert_status": true,
    "walks": [],
    "weighting": "string"
}
```

`GET /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "mode": "string",
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "show_alert_status": true,
    "walks": [],
    "weighting": "string"
}
```

`POST /activitymaps/{id}/query`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

`body:` ***Objet***

Les propriétés de la requête topologique.

`from:` ***Numéro***

L'horodateur de début de la plage temporelle recherchée par la requête, exprimé en millisecondes depuis l'époque.

`until:` ***Numéro***

(Facultatif) L'horodateur de fin de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Si aucune valeur n'est définie, la fin de la requête est par défaut « maintenant ».

`edge_annotations:` ***Tableau de chaînes***

(Facultatif) La liste d'une ou plusieurs annotations de bord à inclure dans la requête topologique.

Les valeurs suivantes sont valides :

- `protocols`
- `appearances`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "edge_annotations": [],
    "from": 0,
    "until": 0
}
```

`DELETE /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de la carte dactivités.

`PATCH /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de la carte dactivités.

`body:` ***Objet***
Les propriétés de la carte dactivités à mettre à jour.

`GET /activitymaps/{id}/sharing`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de la carte dactivités.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "anyone": "string",
    "groups": {},
    "users": {}
}
```

`PUT /activitymaps/{id}/sharing`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les utilisateurs et leurs niveaux d'autorisation.

`id:` ***Numéro***
Identifiant unique de la carte dactivités.

`PATCH /activitymaps/{id}/sharing`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les utilisateurs et leurs niveaux d'autorisation.

`id:` ***Numéro***
Identifiant unique de la carte dactivités.

Alerte

Les alertes sont des notifications du système qui sont générées selon des critères d'alerte spécifiés. Les alertes par défaut sont disponibles dans le système, ou vous pouvez créer une alerte personnalisée.

Les détections et les seuils d'alerte peuvent être définis pour vous avertir si une métrique dépasse la valeur définie dans la configuration des alertes. Les alertes de tendance ne peuvent pas être configurées via l'API REST. Pour plus d' informations, voir Alertes.

Note: Les détections par apprentissage automatique nécessitent connexion aux services cloud ExtraHop.

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

Fonctionnement	Descriptif
GET /alertes	Récupérez toutes les alertes.
POST /alertes	Créez une nouvelle alerte avec des valeurs spécifiées.
SUPPRIMER /alerts/ {id}	Supprimez une alerte spécifique.
OBTENIR /alerts/ {id}	Récupérez une alerte spécifique.
PATCH /alerts/ {id}	Appliquez les mises à jour à une alerte spécifique.
GET /alerts/ {id} /applications	Récupérez toutes les applications auxquelles une alerte spécifique a été attribuée.
POST /alerts/ {id} /applications	Attribuez et annulez l'attribution d'une alerte spécifique aux applications.
SUPPRIMER /alerts/ {id} /applications/ {child-id}	Annuler l'attribution d'une application à une alerte spécifique.
POST /alerts/ {id} /applications/ {child id}	Assignez une application à une alerte spécifique.
GET /alerts/ {id} /devicegroups	Tout récupérer groupes d'équipements auxquels une alerte spécifique est attribuée.
POST /alerts/ {id} /devicegroups	Attribuez et annulez l'attribution d'une alerte spécifique à des groupes d'équipements.
SUPPRIMER /alerts/ {id} /devicegroups/ {child-id}	Annuler l'attribution d'un groupe déquipements à une alerte spécifique.
POST /alerts/ {id} /devicegroups/ {child id}	Assignez un groupe déquipements à une alerte spécifique.
GET /alerts/ {id} /appareils	Récupérez tous les appareils auxquels une alerte spécifique a été attribuée.
POST /alerts/ {id} /appareils	Attribuez et annulez l'attribution d'une alerte spécifique aux appareils.
SUPPRIMER /alerts/ {id} /appareils/ {child id}	Annuler l'attribution d'un équipement à une alerte spécifique.
POST /alerts/ {id} /appareils/ {child id}	Assignez un équipement à une alerte spécifique.
GET /alerts/ {id} /emailgroups	Récupérez tous les groupes d'e-mails auxquels une alerte spécifique est attribuée.

Fonctionnement	Descriptif
POST /alerts/ {id} /emailgroups	Attribuez et annulez l'attribution d'une alerte spécifique à des groupes de messagerie.
SUPPRIMER /alerts/ {id} /emailgroups/ {child-id}	Annuler l'attribution d'un groupe d'e-mails à une alerte spécifique.
POST /alerts/ {id} /emailgroups/ {child id}	Attribuez un groupe d'e-mails à une alerte spécifique.
GET /alerts/ {id} /intervalles d'exclusion	Récupérez tous les intervalles d'exclusion auxquels une alerte spécifique est attribuée.
POST /alerts/ {id} /intervalles d'exclusion	Attribuez et annulez l'attribution d'une alerte spécifique à des intervalles d'exclusion.
SUPPRIMER /alerts/ {id} /exclusionintervals/ {child-id}	Annulez l'attribution d'un intervalle d'exclusion à une alerte spécifique.
POST /alerts/ {id} /exclusionintervals/ {child id}	Attribuez un intervalle d'exclusion à une alerte spécifique.
GET /alerts/ {id} /réseaux	Récupérez tous les réseaux auxquels une alerte spécifique est attribuée.
POST /alerts/ {id} /réseaux	Attribuez et annulez l'attribution d'une alerte spécifique aux réseaux.
SUPPRIMER /alerts/ {id} /networks/ {child-id}	Annuler l'attribution d'un réseau à une alerte spécifique.
POST /alerts/ {id} /réseaux/ {child id}	Assignez un réseau à une alerte spécifique.
OBTENIR /alerts/ {id} /statistiques	Récupérez toutes les statistiques supplémentaires relatives à une alerte spécifique.

Détails de l'opération

```
GET /alerts
```

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.


```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
    "field_op": "string",
    "id": 0,
    "interval_length": 0,
    "mod_time": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
```

```
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`POST /alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées à la nouvelle alerte.

`description:` ***Corde***

Description facultative de l'alerte.

`notify_snmp:` ***Booléen***

(Facultatif) Indique s'il faut envoyer une interruption SNMP lorsqu'une alerte est générée.

`field_op:` ***Corde***

Type de comparaison entre les champs field_name et field_name2 lors de l'application d'un ratio. Applicable uniquement aux alertes de seuil.

Les valeurs suivantes sont valides :

- `/`
- `null`

`stat_name:` ***Corde***

Le nom statistique de l'alerte. Applicable uniquement aux alertes de seuil.

`disabled:` ***Booléen***

(Facultatif) Indique si l'alerte est désactivée.

`operator:` ***Corde***

Opérateur logique appliqué lors de la comparaison de la valeur du champ d'opérande avec les conditions d'alerte. Applicable uniquement aux alertes de seuil.

Les valeurs suivantes sont valides :

- `==`
- `>`
- `<`
- `>=`
- `<=`

`operand:` ***Corde***

La valeur à comparer aux conditions d'alerte. La méthode de comparaison est spécifiée par la valeur du champ opérateur. Applicable uniquement aux alertes de seuil.

`field_name:` ***Corde***

Nom de la métrique surveillée. Applicable uniquement aux alertes de seuil.

`name:` ***Corde***

Le nom unique et convivial de l'alerte.

`cc:` ***Tableau de cordes***

La liste des adresses e-mail, non incluses dans un groupe d'e-mails, pour recevoir des notifications.

`apply_all:` ***Booléen***

Indique si l'alerte est attribuée à toutes les sources de données disponibles.

`severity:` ***Numéro***

(Facultatif) Le niveau de gravité de l'alerte, qui est affiché dans l'historique des alertes, les notifications par e-mail et les interruptions SNMP. Les niveaux de gravité 0 à 2 nécessitent une attention immédiate. Les niveaux de gravité sont décrits dans Guide de l'API REST.

- `0`
- `1`
- `2`
- `3`
- `4`
- `5`
- `6`
- `7`

`author:` ***Corde***

Le nom de l'utilisateur qui a créé l'alerte.

`param:` ***Objet***

Le premier paramètre d'alerte, qui est soit un modèle clé, soit un point de données. Applicable uniquement aux alertes de seuil.

`interval_length:` ***Numéro***

Durée de l'intervalle d'alerte, exprimée en secondes. Applicable uniquement aux alertes de seuil.

Les valeurs suivantes sont valides :

- `30`
- `60`
- `120`
- `300`
- `600`
- `900`
- `1200`
- `1800`

`param2:` ***Objet***

Le deuxième paramètre d'alerte, qui est soit un modèle clé, soit un point de données. Applicable uniquement aux alertes de seuil.

`units:` ***Corde***

Intervalle dans lequel évaluer la condition d'alerte. Applicable uniquement aux alertes de seuil.

Les valeurs suivantes sont valides :

- `none`
- `period`
- `1 sec`
- `1 min`
- `1 hr`

`field_name2:` ***Corde***

La deuxième métrique surveillée lors de l'application d'un ratio. Applicable uniquement aux alertes de seuil.

`refire_interval:` ***Numéro***

(Facultatif) Intervalle de temps pendant lequel les conditions d'alerte sont surveillées, exprimé en secondes.

Les valeurs suivantes sont valides :

- `300`
- `600`
- `900`
- `1800`
- `3600`
- `7200`
- `14400`

`type:` ***Corde***

Type d'alerte.

Les valeurs suivantes sont valides :

- `threshold`

`object_type:` ***Corde***

Type de source métrique surveillée par la configuration des alertes. Applicable uniquement aux alertes de détection.

Les valeurs suivantes sont valides :

- `application`
- `device`

`protocols:` ***Tableau de cordes***

(Facultatif) La liste des protocoles surveillés. Applicable uniquement aux alertes de détection.

`categories:` ***Tableau de cordes***

(Facultatif) Liste d'une ou de plusieurs catégories de détection. Une alerte est générée uniquement si une détection est identifiée dans les catégories spécifiées. Applicable uniquement aux alertes de détection.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
    "field_op": "string",
    "interval_length": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
```

```
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`GET /alerts/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
    "field_op": "string",
    "id": 0,
    "interval_length": 0,
    "mod_time": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`DELETE /alerts/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

`PATCH /alerts/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour des valeurs de propriété spécifiées à l'alerte.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/stats`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "alert_id": 0,
    "field_name": "string",
    "id": 0,
    "param": "string",
    "stat_name": "string"
}
```

`GET /alerts/{id}/devicegroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les groupes d'équipements attribués et non affectés à l'alerte.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`DELETE /alerts/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/emailgroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/emailgroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les groupes de messagerie attribués et non attribués à l'alerte.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/emailgroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique du groupe de messagerie.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`DELETE /alerts/{id}/emailgroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique du groupe de messagerie.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/exclusionintervals`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/exclusionintervals`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les intervalles d'exclusion attribués et non attribués à l'alerte.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/exclusionintervals/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`DELETE /alerts/{id}/exclusionintervals/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/devices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les appareils affectés et non affectés à l'alerte.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique de l'équipement.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`DELETE /alerts/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique de l'équipement.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/networks`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/networks`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les réseaux attribués et non attribués à l'alerte.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/networks/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique du réseau.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`DELETE /alerts/{id}/networks/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique du réseau.
`id:` ***Numéro***
L'identifiant unique de l'alerte.

`GET /alerts/{id}/applications`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'alerte.

`POST /alerts/{id}/applications`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les applications attribuées et non attribuées à l'alerte.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
```

```
}
```

`id:` ***Numéro***

L'identifiant unique de l'alerte.

```
POST /alerts/{id}/applications/{child-id}
```

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'application.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

```
DELETE /alerts/{id}/applications/{child-id}
```

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'application.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

Niveaux de gravité des alertes

Le niveau de gravité que vous spécifiez pour une alerte est affiché sur la page Alertes, les notifications par e-mail et les interruptions SNMP.

Les niveaux de gravité suivants sont pris en charge. Les niveaux de gravité de 0 à 2 nécessitent une attention immédiate.

Valeur	Nom	Descriptif
0	Urgence	Les fonctionnalités du système ne sont pas disponibles.
1	Alerte	Une action immédiate est requise.
2	Critique	Des conditions critiques se produisent.
3	Erreur	Des conditions d'erreur se produisent.
4	Avertissement	Des conditions d'avertissement se produisent.
5	Avis	Les opérations normales se produisent dans des conditions importantes, telles qu'un redémarrage.
6	Infos	Les opérations normales se produisent avec les mises à jour des processus.
7	Déboguer	Les messages de niveau de débogage sont disponibles.

Priorité d'analyse

Le système ExtraHop analyse et classe le trafic pour chaque équipement qu'il découvre. Votre licence réserve au système ExtraHop la capacité de collecter des métriques pour les appareils à valeur élevée. Cette capacité est associée à deux niveaux d'analyse : Analyse avancée et Analyse standard.

Vous pouvez spécifier quels appareils reçoivent les niveaux d'Analyse avancée et d'Analyse standard en configurant règles de priorité d'analyse. Les priorités d'analyse aident le système ExtraHop à identifier les appareils importants dans votre environnement. Un troisième niveau d' analyse, le mode découverte, est disponible pour les appareils qui ne sont pas en analyse avancée ou standard.

Note: Par défaut, chaque sonde gère ses propres priorités d'analyse. Si la sonde est connectée à une console, vous pouvez les gérer de manière centralisée paramètres système partagés depuis la console.

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

opération	Descriptif
GET /analysispriority/config/ {sensor_id}	Récupérez les règles de priorité d'analyse pour un objet spécifique sonde.
PUT /analysispriority/config/ {sensor_id}	Remplacer les règles de priorité d'analyse pour un objet spécifique sonde.
GET /analysispriority/{sensor_id} /manager	Récupérez le système configuré pour gérer les règles de priorité d'analyse pour le sonde.
PATCH /priorité d'analyse/{sensor_id} /gestionnaire	Mettre à jour le système qui gère les règles de priorité d'analyse pour un domaine spécifique sonde.

Détails de l'opération

`GET /analysispriority/{appliance_id}/manager`

Spécifiez les paramètres suivants.

`appliance_id:` ***Numéro***
Identifiant de la sonde locale. Cette valeur doit être définie sur 0.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "manager": {}
}
```

`GET /analysispriority/config/{appliance_id}`

Spécifiez les paramètres suivants.

`appliance_id:` ***Numéro***
Identifiant d'une sonde. Définissez cette valeur sur 0 si vous faites appel à une sonde.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "advanced_rules": [],
    "autofill_advanced": true,
    "autofill_standard": true,
```

```
    "is_in_effect": true,
    "standard_rules": []
}
```

`PUT /analysispriority/config/{appliance_id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Propriétés des règles d'analyse des priorités.

`autofill_advanced:` ***Booléen***

Indique s'il faut placer automatiquement les appareils dans Analyse avancée jusqu'à ce que leur capacité soit atteinte. Les appareils de la liste advanced_rules sont priorisés, suivis des appareils de la liste standard_rules, puis de l'heure de découverte de l'équipement. La capacité d'Analyse avancée est déterminée par la licence du système ExtraHop.

`advanced_rules:` ***Tableau d'objets***

(Facultatif) Les règles de priorité de l'Analyse avancée pour un groupe de déquipements.

`type:` ***Corde***

Type de groupe auquel les règles de priorité d'analyse s'appliquent.

Les valeurs suivantes sont valides :

- `device_group`

`object_id:` ***Numéro***

Identifiant unique du groupe.

`description:` ***Corde***

(Facultatif) Description des règles de priorité d'analyse.

`autofill_standard:` ***Booléen***

Indique s'il faut placer automatiquement les appareils dans l'analyse standard jusqu'à ce que leur capacité totale soit atteinte. Les appareils de la liste standard_rules sont priorisés, suivis de l'heure de découverte de l'équipement. La capacité totale est déterminée par la licence du système ExtraHop.

`standard_rules:` ***Tableau d'objets***

(Facultatif) Les règles de priorité d'analyse standard pour un groupe déquipements.

`type:` ***Corde***

Type de groupe auquel les règles de priorité d'analyse s'appliquent.

Les valeurs suivantes sont valides :

- `device_group`

`object_id:` ***Numéro***

Identifiant unique du groupe.

`description:` ***Corde***

(Facultatif) Description des règles de priorité d'analyse.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "advanced_rules": {
        "type": "string",
        "object_id": 0,
        "description": "string"
    },
    "autofill_advanced": true,
    "autofill_standard": true,
```

```
    "standard_rules": {
        "type": "string",
        "object_id": 0,
        "description": "string"
    }
}
```

`appliance_id:` ***Numéro***

Identifiant d'une sonde. Définissez cette valeur sur 0 si vous faites appel à une sonde.

`PATCH /analysispriority/{appliance_id}/manager`

Spécifiez les paramètres suivants.

`body:` ***Objet***

ID du capteur ou de la console qui gérera les règles de priorité d'analyse pour le capteur local. Définissez cette valeur sur 0 pour rétablir la gestion sur la sonde locale.

`manager:` ***Numéro***

Identifiant unique de la sonde ou de la console de gestion.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "manager": 0
}
```

`appliance_id:` ***Numéro***

Identifiant de la sonde locale. Cette valeur doit être définie sur 0.

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.

Détails de l'opération

`GET /apikeys`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "key": "string",
    "time_added": 0,
```

```
    "user_id": 0,
    "username": "string"
}
```

`GET /apikeys/{keyid}`

Spécifiez les paramètres suivants.

`keyid:` ***Numéro***

Identifiant unique de la clé d'API.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "key": "string",
    "time_added": 0,
    "user_id": 0,
    "username": "string"
}
```

`POST /apikeys`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Le mot de passe de l'utilisateur d'installation.

`password:` ***Corde***

Le mot de passe de l'utilisateur d'installation.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "password": "string"
}
```

Appareil

Le système ExtraHop consiste en un réseau d'appareils ExtraHop connectés, tels que capteurs, consoles, des magasins d'enregistrements et des magasins de paquets qui effectuent 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 pouvez uniquement établir une connexion entre des appliances ExtraHop similaires, telles que RevealX Enterprise ou Performance.

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

opération	Descriptif
GET /appareils	Récupérez toutes les appliances ExtraHop distantes connectées à l'appliance locale.
POST /appareils	Établissez une nouvelle connexion à une appliance ExtraHop distante.

opération	Descriptif
SUPPRIMER /appliances/ {id}	Déconnectez un appareil ExtraHop spécifique de celui-ci console.
GET /appliances/ {id}	Récupérez une appliance ExtraHop distante spécifique connectée à l'appliance locale (valable uniquement sur les consoles).
GET /appliances/ {id} /cloudservices	Récupérez l'état des services cloud ExtraHop sur cette appliance.
POST /appliances/ {id} /cloudservices	Modifiez les paramètres des services cloud ExtraHop sur cette appliance.
GET /appliances/ {id} /productkey	Récupérez la clé de produit pour une appliance spécifiée (valable uniquement sur les consoles).
GET /appliances/ {ids_id} /association	Récupérez l'ID de la sonde réseau d'analyse de paquets à laquelle la sonde IDS est connectée.
POST /appliances/{ids_id} /association	Joignez une sonde IDS à une sonde réseau dveloppe d'analyse de paquets.
GET /appliances/firmware/next	Récupérez les versions du microprogramme vers lesquelles les systèmes ExtraHop distants peuvent être mis à niveau (uniquement valable sur consoles).
POST /Appliances/firmware/upgrade	Mettez à niveau le microprogramme des systèmes ExtraHop distants connectés au système local. Les images du firmware sont téléchargées depuis ExtraHop Cloud Services (uniquement valable sur les consoles).
`GET /appliances/{ids_id}/association`	Récupérez l'ID de la sonde réseau d'analyse de paquets à laquelle la sonde IDS est connectée (valable uniquement sur consoles).
`POST /appliances/{ids_id}/association`	Associez une sonde IDS à une sonde réseau dveloppe d'analyse de paquets (uniquement valable sur consoles).

Détails de l'opération

`GET /appliances`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "add_time": 0,
    "advanced_analysis_capacity": 0,
    "analysis_levels_managed": true,
    "connection_type": "string",
    "data_access": true,
    "display_name": "string",
    "fingerprint": "string",
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_platform": "string",
```

```
    "license_status": "string",
    "licensed_features": {},
    "licensed_modules": [
        "string"
    ],
    "managed_by_local": true,
    "manages_local": true,
    "nickname": "string",
    "platform": "string",
    "status_message": "string",
    "sync_time": 0,
    "total_capacity": 0,
    "uuid": "string"
}
```

`GET /appliances/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Spécifiez l'identifiant unique de l'appliance. Spécifiez 0 pour sélectionner l'appliance locale.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "add_time": 0,
    "advanced_analysis_capacity": 0,
    "analysis_levels_managed": true,
    "connection_type": "string",
    "data_access": true,
    "display_name": "string",
    "fingerprint": "string",
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_platform": "string",
    "license_status": "string",
    "licensed_features": {},
    "licensed_modules": [
        "string"
    ],
    "managed_by_local": true,
    "manages_local": true,
    "nickname": "string",
    "platform": "string",
    "status_message": "string",
    "sync_time": 0,
    "total_capacity": 0,
    "uuid": "string"
}
```

`GET /appliances/{ids_id}/association`

Spécifiez les paramètres suivants.

`ids_id:` ***Numéro***
Spécifiez l'ID de la sonde IDS.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
```

```
    "associated_sensor_id": 0
}
```

`POST /appliances/{ids_id}/association`

Spécifiez les paramètres suivants.

`ids_id:` ***Numéro***
Spécifiez l'ID de la sonde IDS.

`body:` ***Objet***
Spécifiez l'ID de la sonde réseau dveloppe analyse de paquets.

`associated_sensor_id:` ***Numéro***
L'ID de la sonde réseau dveloppe l'analyse de paquets.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "associated_sensor_id": 0
}
```

`GET /appliances/{id}/productkey`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Spécifiez l'identifiant unique de l'appliance.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "product_key": "string"
}
```

`GET /appliances/firmware/next`

Spécifiez les paramètres suivants.

`ids:` ***Corde***
(Facultatif) Une liste CSV d'identifiants uniques pour les appareils distants. Si ce paramètre est spécifié, l'opération renvoie les versions du microprogramme vers lesquelles toutes les appliances distantes spécifiées peuvent être mises à niveau. Si ce paramètre n'est pas spécifié, l'opération renvoie les versions du microprogramme vers lesquelles n'importe quelle appliance distante peut être mise à niveau.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "release": "string",
    "versions": []
}
```

`GET /appliances/{id}/cloudservices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Spécifiez l'identifiant unique de l'appliance. Cette valeur doit être définie sur 0, ce qui permet de sélectionner l'appliance locale.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "connection_status": "string",
    "connection_status_color": "string",
    "enabled_services": [],
    "last_active_time": 0,
    "last_analyzed_time": 0
}
```

`POST /appliances/{id}/cloudservices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Spécifiez l'identifiant unique de l'appliance. Cette valeur doit être définie sur 0, ce qui permet de sélectionner l'appliance locale.

`body:` ***Objet***

Spécifiez l'action pour modifier les paramètres des services cloud ExtraHop.

`action:` ***Corde***

Spécifiez l'action pour modifier les paramètres des services cloud ExtraHop.

Les valeurs suivantes sont valides :

- `unenroll`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "action": "string"
}
```

`POST /appliances/firmware/upgrade`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les options de mise à niveau du microprogramme.

`version:` ***Corde***

Version du microprogramme vers laquelle effectuer la mise à niveau des appliances. Vous pouvez récupérer la liste des versions valides à l'aide de l'opération GET /api/v1/appliances/firmware/next.

`system_ids:` ***Tableau de nombres***

Une liste d'identifiants uniques pour les appareils distants. Vous pouvez récupérer les ID d'appliance à l'aide de l'opération GET /api/v1/appliances ; les ID d'appliance sont renvoyés dans les champs ID de la réponse.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "system_ids": [],
    "version": "string"
}
```

`POST /appliances`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Spécifiez les propriétés de la nouvelle connexion.

`host:` ***Corde***

Le nom d'hôte de l'appliance distante.

`remote_setup_password:` ***Corde***

(Facultatif) Le mot de passe du compte utilisateur de configuration sur le stockage des paquets EXA ou ExtraHop cible. Ce paramètre n'est pas obligatoire si l'appliance distante est un nœud d'un cluster Explore déjà connecté à la console. Ce paramètre n'est pas valide si l'appliance distante est une sonde.

`remote_pairing_token:` ***Corde***

(Facultatif) Le jeton généré sur la sonde cible ou l'espace de stockage des enregistrements EXA 5300. Vous devez spécifier ce paramètre pour vous authentifier auprès de la sonde ou de l'espace de stockage des enregistrements cible. Ce paramètre n'est pas valide si vous vous connectez à un espace de stockage des paquets ExtraHop ou à un espace de stockage des enregistrements EXA 5200.

`fingerprint:` ***Corde***

(Facultatif) L'empreinte digitale de l'appliance distante. Si vous connectez une console à une boutique de paquets EXA ou ExtraHop, ce champ est obligatoire. Sinon, pour contourner la vérification de l'empreinte digitale, spécifiez « insecure_skip_verification ». Notez que le contournement de la vérification peut permettre des attaques de type « man-in-the-middle ».

`reset_configuration:` ***Booléen***

(Facultatif) Indique s'il faut réinitialiser la configuration de l'appliance distante.

`remote_nickname_for_local:` ***Corde***

(Facultatif) Le surnom de l'appliance distante, auquel fait référence l'appliance locale. Si vous connectez une sonde à un autre appareil, ce champ est obligatoire.

`local_nickname_for_remote:` ***Corde***

(Facultatif) Le surnom de l'appliance locale, auquel fait référence l'appliance distante.

`remote_appliance_type:` ***Corde***

Type d'appliance pour la nouvelle connexion.

Les valeurs suivantes sont valides :

- `command`
- `explore`
- `discover`
- `trace`

`manages_local:` ***Booléen***

(Facultatif) Indique si l'appliance distante gère l'appliance locale.

`managed_by_local:` ***Booléen***

(Facultatif) Indique si l'appliance distante est gérée par l'appliance locale. Si vous connectez une console à un capteur, ce champ n'est pas obligatoire car la console gère toujours les capteurs connectés.

`data_access:` ***Booléen***

Indique si les données peuvent être partagées entre les appareils locaux et distants.

`product_key:` ***Corde***

(Facultatif) La clé de produit de l'appliance distante. Si ce paramètre est spécifié, l'appliance distante reçoit une licence avec la clé de produit. Ce paramètre n'est pas valide lorsque le paramètre remote_pairing_token est spécifié.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "data_access": true,
    "fingerprint": "string",
    "host": "string",
    "local_nickname_for_remote": "string",
    "managed_by_local": true,
    "manages_local": true,
    "product_key": "string",
    "remote_appliance_type": "string",
    "remote_nickname_for_local": "string",
    "remote_pairing_token": "string",
    "remote_setup_password": "string",
    "reset_configuration": true
}
```

`DELETE /appliances/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Spécifiez l'identifiant unique de l'appliance distante.

Demande

Les applications sont des groupes définis par l'utilisateur qui collectent des métriques identifiées par le biais de déclencheurs pour plusieurs types de trafic. L'application All Activity par défaut contient toutes les métriques collectées.

Le tableau suivant présente toutes les opérations que vous pouvez effectuer sur la ressource de l'application :

Fonctionnement	Descriptif
OBTENIR /applications	Récupérez toutes les applications qui étaient actives au cours d'une période donnée.
POST/applications	Créez une nouvelle application.
OBTENEZ /applications/ {id}	Récupérez une application spécifique.
CORRECTIF /applications/ {id}	Mettez à jour une application spécifique.
GET /applications/ {id} /activité	Récupérez toutes les activités d'une application spécifique.
GET /applications/ {id} /alertes	Tout récupérer alertes qui sont affectés à une application spécifique.
POST /applications/ {id} /alertes	Attribuez et annulez l'attribution d'alertes à une application spécifique.
SUPPRIMER /applications/ {id} /alerts/ {child-id}	Annuler l'attribution d'une alerte à une application spécifique.

Fonctionnement	Descriptif
POST /applications/ {id} /alerts/ {child id}	Attribuez une alerte à une application spécifique.
GET /applications/ {id} /tableaux de bord	Récupérez tous les tableaux de bord relatifs à une application spécifique.

Détails de l'opération

`GET /applications/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de l'application.

`include_criteria:` ***Booléen***

(Facultatif) Indique s'il faut inclure les critères associés à l'application dans la réponse.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "criteria": [],
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "node_id": 0,
    "user_mod_time": 0
}
```

`POST /applications`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de l'application.

`node_id:` ***Numéro***

(Facultatif) L'identifiant unique de la sonde à laquelle cette application est associée. L'identifiant peut être récupéré via l'opération GET /appliances. Ce champ n'est valide que sur une console.

`discovery_id:` ***Corde***

L'identifiant unique de l'application, qui est affiché sur la page de l'application dans le système ExtraHop.

`display_name:` ***Corde***

Nom convivial de l'application.

`description:` ***Corde***

(Facultatif) Description facultative de l'application.

`criteria:` ***Tableau d'objets***

(Facultatif) Tableau de critères de protocole et de source associés à l'application. Le contenu de ce tableau est défini dans la section « critères » ci-dessous.

`protocol_default:` ***Corde***

Protocoles par défaut surveillés par l'application. Les valeurs prises en charge sont « any » et « none ».

`sources:` ***Tableau d'objets***

Tableau contenant une ou plusieurs sources métriques associées à l'application. L'application collecte uniquement les métriques provenant des sources spécifiées. Le contenu de ce tableau est défini dans la section « source » ci-dessous.

`type:` ***Corde***

Type de source métrique associée à l'application. Les valeurs de type source prises en charge sont « device » et « device_group ».

`id:` ***Numéro***

Identifiant unique de l'équipement ou du groupe d'équipements associé à l'application.

`protocols:` ***Objet***

(Facultatif) Liste d'un ou de plusieurs mappages de protocoles et de rôles associés à l'application. L'application collecte uniquement des métriques à partir des protocoles spécifiés. Le format de chaque protocole est {'protocol' : 'role'}. Exemple : {'http' : 'serveur'}. Les valeurs de rôle prises en charge sont « client », « serveur », « any » ou « none ».

Spécifiez le paramètre body au format JSON suivant.

```
{
    "criteria": {
        "protocol_default": "string",
        "sources": {
            "type": "string",
            "id": 0
        },
        "protocols": {}
    },
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "node_id": 0
}
```

`PATCH /applications/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour de propriétés spécifiées à l'application.

`id:` ***Numéro***

Identifiant unique de l'application.

`GET /applications`

Spécifiez les paramètres suivants.

`active_from:` ***Numéro***

(Facultatif) Renvoie uniquement les applications actives après la durée spécifiée. Les valeurs positives indiquent le temps en millisecondes écoulé depuis l'époque. Les valeurs négatives indiquent l'heure en millisecondes avant l'heure actuelle.

`active_until:` ***Numéro***

(Facultatif) Renvoie uniquement les applications actives avant l'heure spécifiée. Les valeurs positives indiquent le temps en millisecondes écoulé depuis l'époque. Les valeurs négatives indiquent l'heure en millisecondes avant l'heure actuelle.

`limit:` ***Numéro***

(Facultatif) Limitez le nombre de demandes renvoyées au nombre maximum spécifié.

`offset:` ***Numéro***

(Facultatif) Ignorez les n premiers résultats de l'application. Ce paramètre est souvent associé au paramètre limite.

`search_type:` ***Corde***

Type d'objet à rechercher.

Les valeurs suivantes sont valides :

- `any`
- `name`
- `node`
- `discovery_id`
- `extrahop-id`

`value:` ***Corde***

(Facultatif) Les critères de recherche. Ajoutez une barre oblique avant et après les critères pour appliquer la correspondance RegEx.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "criteria": [],
    "description": "string",
    "discovery_id": "string",
    "display_name": "string",
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "node_id": 0,
    "user_mod_time": 0
}
```

`GET /applications/{id}/activity`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de l'application.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "application_id": 0,
    "from_time": 0,
    "id": 0,
    "mod_time": 0,
    "stat_name": "string",
    "until_time": 0
}
```

`GET /applications/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Récupérez l'identifiant unique de l'application.

`direct_assignments_only:` ***Booléen***
(Facultatif) Indique si les résultats sont limités aux alertes directement attribuées à l'application.

`POST /applications/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Attribuez ou annulez l'attribution de la liste spécifiée d'identifiants uniques pour les alertes.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
Fournissez un identifiant unique pour l'application.

`POST /applications/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'alerte.

`id:` ***Numéro***
Identifiant unique de l'application.

`DELETE /applications/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'alerte.

`id:` ***Numéro***
Identifiant unique de l'application.

`GET /applications/{id}/dashboards`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de l'application.

Journal d'audit

Le journal d'audit affiche un enregistrement de toutes les activités d'administration et de configuration du système enregistrées, telles que l'heure de l'activité, l'utilisateur qui a effectué l'activité, l'opération, les détails de l'opération et les composants du système.

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

Fonctionnement	Descriptif
OBTENIR /auditlog	Récupérez tous les messages du journal dÈRE d'audit.

Détails de l'opération

```
GET /auditlog
```

Spécifiez les paramètres suivants.

`limit:` ***Numéro***

(Facultatif) Nombre maximal de messages de journal à renvoyer.

`offset:` ***Numéro***

(Facultatif) Nombre de messages de journal à ignorer dans les résultats. Renvoie les messages du journal à partir de la valeur de décalage.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "body": {},
    "id": 0,
    "occur_time": 0,
    "time": 0
}
```

Auth

Vous pouvez configurer une authentification unique (SSO) sécurisée sur le système ExtraHop via un ou plusieurs fournisseurs d'identité SAML (Security Assertion Markup Language).

Lorsqu'un utilisateur se connecte à un système ExtraHop configuré en tant que fournisseur de services (SP) pour l'authentification SSO SAML, le système ExtraHop demande l'autorisation au fournisseur d'identité (IdP) approprié. Le fournisseur d'identité authentifie les informations dcredentiation de l'utilisateur, puis renvoie l'autorisation de l'utilisateur au système ExtraHop. L'utilisateur peut alors accéder au système ExtraHop.

Opération	Descriptif
GET /auth/fournisseurs d'identité	Récupérez tous les fournisseurs d'identité.
POST/auth/fournisseurs d'identité	Ajoutez un fournisseur d'identité pour l'authentification à distance.
SUPPRIMER /auth/identityproviders/ {id}	Supprimez un fournisseur d'identité spécifique.
OBTENEZ /auth/identityproviders/ {id}	Récupérez un fournisseur d'identité spécifique.
PATCH /auth/identityproviders/ {id}	Mettez à jour un fournisseur d'identité existant.

Opération	Descriptif
GET /auth/identityproviders/ {id} /privilèges	Récupérez les paramètres de privilège pour un fournisseur d'identité spécifique.
PATCH /auth/identityproviders/ {id} /privilèges	Mettez à jour les paramètres de privilège pour un fournisseur d'identité spécifique.
OBTENEZ /auth/samlsp	Récupérez les métadonnées du fournisseur de sécurité (SP) SAML pour ce système ExtraHop.

Détails de l'opération

`POST /auth/identityproviders`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Paramètres du fournisseur d'identité.

`name:` ***Corde***

Le nom du fournisseur d'identité.

`enabled:` ***Booléen***

Indique si l'authentification via le fournisseur d'identité est activée sur le système ExtraHop.

`entity_id:` ***Corde***

(Facultatif) Identifiant d'entité SAML 2.0.

`sso_url:` ***Corde***

(Facultatif) L'URL d'authentification unique (SSO) SAML 2.0.

`signing_certificate:` ***Corde***

(Facultatif) Le certificat de signature SAML 2.0 X.509 au format PEM.

`type:` ***Corde***

Type de fournisseur d'identité.

Les valeurs suivantes sont valides :

- `saml`

`auto_provision_users:` ***Booléen***

Indique si un utilisateur peut être créé sur le système ExtraHop à partir du fournisseur d'identité.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "auto_provision_users": true,
    "enabled": true,
    "entity_id": "string",
    "name": "string",
    "signing_certificate": "string",
    "sso_url": "string",
    "type": "string"
}
```

`GET /auth/identityproviders`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
```

```
    "auto_provision_users": true,
    "enabled": true,
    "entity_id": "string",
    "id": 0,
    "name": "string",
    "signing_certificate": "string",
    "sso_url": "string",
    "type": "string"
}
```

`GET /auth/identityproviders/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fournisseur d'identité.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "auto_provision_users": true,
    "enabled": true,
    "entity_id": "string",
    "id": 0,
    "name": "string",
    "signing_certificate": "string",
    "sso_url": "string",
    "type": "string"
}
```

`PATCH /auth/identityproviders/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fournisseur d'identité.

`body:` ***Objet***
Les paramètres du fournisseur d'identité.

`DELETE /auth/identityproviders/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fournisseur d'identité.

`GET /auth/identityproviders/{id}/privileges`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fournisseur d'identité.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "detectionsaccesslevel": {},
    "ndrlevel": {},
    "npmlevel": {},
```

```
    "packetslevel": {},
    "writelevel": {}
}
```

`PATCH /auth/identityproviders/{id}/privileges`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fournisseur d'identité.

`body:` ***Objet***
Objet contenant les paramètres de privilèges.

`GET /auth/samlsp`

Spécifiez les paramètres suivants.

`xml:` ***Booléen***
(Facultatif) Indique s'il faut récupérer les métadonnées XML SAML 2.0.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "acs_url": "string",
    "entity_id": "string",
    "xml": "string"
}
```

Forfait

Les bundles sont des documents au format JSON qui contiennent des informations sur la configuration système sélectionnée, telles que les déclencheurs, tableaux de bord, des applications ou alertes.

Vous pouvez créer un bundle, puis transférer ces configurations vers un autre système ExtraHop, ou enregistrer le bundle en tant que sauvegarde. Pour plus d'informations, voir Lots.

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

opération	Descriptif
GET /bundles	Récupérez les métadonnées de tous les bundles du système ExtraHop.
POST /lots	Téléchargez un nouveau bundle dans le système ExtraHop.
SUPPRIMER /bundles/ {id}	Supprimez un bundle spécifique.
GET /bundles/ {id}	Récupérez une exportation de bundle spécifique.
POST /bundles/ {id} /appliquer	Appliquez un bundle enregistré au système ExtraHop.

Détails de l'opération

`GET /bundles`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "built_in": true,
    "created_time": 0,
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`POST /bundles`

Spécifiez les paramètres suivants.

`body:` ***Corde***

Une exportation de bundle au format JSON.

`name:` ***Corde***

Le nom convivial du bundle.

`description:` ***Corde***

(Facultatif) Description facultative du bundle.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "name": "string"
}
```

`GET /bundles/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du bundle.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "built_in": true,
    "created_time": 0,
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`DELETE /bundles/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du bundle.

`POST /bundles/{id}/apply`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du bundle.

`body:` ***Objet***

Les options de configuration pour appliquer le bundle.

`policy:` ***Corde***

Indique si les objets en conflit doivent être remplacés ou ignorés.

Les valeurs suivantes sont valides :

- `overwrite`
- `skip`

`include_assignments:` ***Booléen***

Indique si les assignations d'objets doivent être restaurées avec le bundle.

`node_ids:` ***Tableau de nombres***

Une liste d'identifiants uniques pour les capteurs sur lesquels appliquer le bundle. Ce champ n'est valide que sur une console.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "include_assignments": true,
    "node_ids": [],
    "policy": "string"
}
```

Nuage

Cette ressource vous permet de connecter votre site capteurs à RevealX 360 Pour plus d' informations, consultez Connecter une sonde à RevealX 360.

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

opération	Descriptif
POST /cloud/connect	Connectez le système ExtraHop à RevealX 360.

Détails de l'opération

`POST /cloud/connect`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Le jeton que vous avez généré à partir de RevealX 360.

`cloud_token:` ***Corde***

Le jeton que vous avez généré à partir de RevealX 360.

`nickname:` ***Corde***

Un surnom permettant d'identifier facilement la sonde.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cloud_token": "string",
    "nickname": "string"
```

```
}
```

équipement personnalisé

Vous pouvez créer un équipement personnalisé en définissant un ensemble de règles.

Par exemple, vous pouvez créer un équipement personnalisé doté d'une adresse IP sur un VLAN spécifié. Par défaut, toutes les adresses IP situées en dehors des domaines de diffusion surveillés localement sont agrégées derrière un routeur. Pour identifier les appareils qui se trouvent derrière ce routeur, vous pouvez créer un appareil personnalisé, puis collecter des métriques à partir de celui-ci. Pour plus d'informations, voir Créez des appareils personnalisés via l'API REST.

Note: La ressource d'équipement personnalisée n'est pas disponible sur les consoles.

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

Opération	Descriptif
GET/appareils personnalisés	Récupérez tous les appareils personnalisés.
POST/appareils personnalisés	Créez un équipement personnalisé.
SUPPRIMER /customdevices/ {id}	Supprimez un équipement personnalisé spécifique.
OBTENEZ /customdevices/ {id}	Récupérez un équipement personnalisé spécifique.
PATCH /appareils personnalisés/ {id}	Mettez à jour un équipement personnalisé spécifique.

Détails de l'opération

`GET /customdevices`

Spécifiez les paramètres suivants.

`include_criteria:` ***Booléen***
(Facultatif) Indique si les critères d'équipement personnalisés doivent être inclus.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "criteria": [],
    "description": "string",
    "disabled": true,
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`GET /customdevices/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'équipement personnalisé.

`include_criteria:` ***Booléen***
(Facultatif) Indique si les critères d'équipement personnalisés doivent être inclus.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "criteria": [],
    "description": "string",
    "disabled": true,
    "extrahop_id": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`DELETE /customdevices/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'équipement personnalisé.

`POST /customdevices`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées au nouvel équipement personnalisé.

`author:` ***Corde***

Le nom du créateur de l'équipement personnalisé.

`extrahop_id:` ***Corde***

(Facultatif) Un identifiant unique pour l'équipement personnalisé. Si ce champ n'est pas spécifié, un identifiant est généré à partir du nom de l'équipement personnalisé. L'ID ne peut pas contenir d'espaces et ne peut pas être modifié une fois l'équipement personnalisé enregistré.

`name:` ***Corde***

Le nom convivial de l'équipement personnalisé.

`description:` ***Corde***

(Facultatif) Description facultative de l'équipement personnalisé.

`disabled:` ***Booléen***

Indique si l'équipement personnalisé est inactif.

`criteria:` ***Tableau d'objets***

(Facultatif) Un ensemble de critères d'équipement personnalisés pour cet appareil. Si ce champ est spécifié avec la méthode PATCH, tous les critères précédemment spécifiés sont supprimés.

`ipaddr:` ***Corde***

L'adresse IP à laquelle doit correspondre l'équipement personnalisé.

`ipaddr_direction:` ***Corde***

Direction du trafic à laquelle doit correspondre l'adresse ipaddr. Les critères déterminent la direction du trafic à destination ou en provenance de l'adresse ipaddr qui correspond.

Les valeurs suivantes sont valides :

- `any`
- `dst`

- src

`ipaddr_peer:` ***Corde***

L'adresse IP avec laquelle l'adresse IPadder communique pour correspondre à l'équipement personnalisé. S'il est spécifié, ce paramètre limite le trafic correspondant à l'équipement personnalisé. Par exemple, si ipaddr_direction est « src », l'équipement personnalisé ne fait correspondre que le trafic vers l'adresse ipaddr_peer à partir de l'adresse ipaddr. Ce paramètre n'est valide que si ipaddr est spécifié et si ipaddr_direction n'a pas la valeur « any ».

`src_port_min:` ***Numéro***

Limite inférieure du port source à laquelle correspond l'équipement personnalisé. Valeurs prises en charge : 1-65535.

`src_port_max:` ***Numéro***

Limite maximale du port source à laquelle l'équipement personnalisé doit correspondre. Valeurs prises en charge : 1-65535.

`dst_port_min:` ***Numéro***

Limite inférieure du port de destination correspondant à l'équipement personnalisé. Valeurs prises en charge : 1-65535.

`dst_port_max:` ***Numéro***

Limite maximale du port de destination à laquelle l'équipement personnalisé doit correspondre. Valeurs prises en charge : 1-65535.

`vlan_min:` ***Numéro***

La limite inférieure du VLAN à laquelle correspond l'équipement personnalisé.

`vlan_max:` ***Numéro***

La limite maximale du VLAN à laquelle l'équipement personnalisé doit correspondre.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "author": "string",
    "criteria": {
        "ipaddr": "string",
        "ipaddr_direction": "string",
        "ipaddr_peer": "string",
        "src_port_min": 0,
        "src_port_max": 0,
        "dst_port_min": 0,
        "dst_port_max": 0,
        "vlan_min": 0,
        "vlan_max": 0
    },
    "description": "string",
    "disabled": true,
    "extrahop_id": "string",
    "name": "string"
}
```

`PATCH /customdevices/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour des valeurs de propriété spécifiées à l'équipement personnalisé.

`id:` ***Numéro***

L'identifiant unique de l'équipement personnalisé.

Personnalisation

La ressource Personnalisation vous permet de gérer les fichiers de sauvegarde sur le système ExtraHop. Vous devez disposer des privilèges d'administration du système et des droits d'accès pour effectuer des opérations sur cette ressource.

Les fichiers de sauvegarde contiennent à la fois des personnalisations et des ressources système. Les personnalisations sont des objets définis par l'utilisateur, tels que des alertes, des tableaux de bord, des déclencheurs et des mesures personnalisées. Les ressources système sont des éléments tels que les ensembles, les utilisateurs et les groupes locaux et le certificat TLS. Pour plus d'informations, voir Sauvegarder et restaurer une sonde ou une console.

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

opération	Descriptif
GET /personnalisations	Récupérez tous les fichiers de sauvegarde.
POST /personnalisations	Créez un fichier de sauvegarde.
GET /personnalisations/status	Récupérez les informations relatives à l'état de la dernière tentative de sauvegarde.
SUPPRIMER /customizations/ {id}	Supprimez un fichier de sauvegarde spécifique.
GET /personnalisations/ {id}	Récupérez un fichier de sauvegarde spécifique.
POST /personnalisations/ {id} /appliquer	Restaurez uniquement les personnalisations à partir d'un fichier de sauvegarde spécifique.
POST /personnalisations/ {id} /téléchargement	Téléchargez un fichier de sauvegarde spécifique.

Détails de l'opération

`GET /customizations`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "auto": true,
    "create_time": 0,
    "id": 0,
    "name": "string",
    "recovered": true
}
```

`POST /customizations`

Spécifiez les paramètres suivants.

`body` : ***Objet***

Nom unique pour le fichier de sauvegarde.

`name` : ***Corde***

Nom unique pour le fichier de sauvegarde.

Spécifiez le paramètre body au format JSON suivant.

```
{
```

```
    "name": "string"
}
```

`GET /customizations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fichier de sauvegarde.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "auto": true,
    "create_time": 0,
    "id": 0,
    "name": "string",
    "recovered": true
}
```

`DELETE /customizations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fichier de sauvegarde.

`POST /customizations/{id}/apply`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fichier de sauvegarde.

`POST /customizations/{id}/download`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du fichier de sauvegarde.

`GET /customizations/status`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "did_last_succeed": true,
    "last_attempt_time": 0,
    "last_success_time": 0
}
```

Tableaux de bord

Les tableaux de bord sont des vues intégrées ou personnalisées des informations de vos métriques ExtraHop. Pour plus d' informations, voir Tableaux de bord.

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

Opération	Description
GET/Tableaux de bord	Récupérez tous les tableaux de bord.
SUPPRIMER /dashboards/ {id}	Supprimez un tableau de bord spécifique.
GET /dashboards/ {id}	Récupérez un tableau de bord spécifique.
PATCH /tableaux de bords/ {id}	Mettez à jour la propriété d'un tableau de bord spécifique.
GET /dashboards/ {id} /rapports	Récupérez les rapports de tableau de bord contenant un tableau de bord spécifique. **Note:** Cette opération n'est disponible que depuis une console.
GET /dashboards/ {id} /partage	Récupérez les utilisateurs et leurs autorisations de partage pour un tableau de bord spécifique.
PATCH /dashboards/ {id} /partage	Mettez à jour les utilisateurs et leurs autorisations de partage pour un tableau de bord spécifique.
PUT /dashboards/ {id} /partage	Remplacez les utilisateurs et leurs autorisations de partage pour un tableau de bord spécifique.

Détails de l'opération

`GET /dashboards`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "comment": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "owner": "string",
    "rights": [
        "string"
    ],
    "short_code": "string",
    "type": "string"
}
```

`GET /dashboards/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du tableau de bord.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "comment": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "owner": "string",
```

```
    "rights": [
        "string"
    ],
    "short_code": "string",
    "type": "string"
}
```

`DELETE /dashboards/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du tableau de bord.

`PATCH /dashboards/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Le nom d'utilisateur du propriétaire du tableau de bord.
`id:` ***Numéro***
Identifiant unique du tableau de bord.

`GET /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du tableau de bord.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "anyone": "string",
    "groups": {},
    "users": {}
}
```

`PUT /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les utilisateurs et leurs niveaux d'autorisation.
`id:` ***Numéro***
Identifiant unique du tableau de bord.

`PATCH /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les utilisateurs et leurs niveaux d'autorisation.
`id:` ***Numéro***
Identifiant unique du tableau de bord.

```
GET /dashboards/{id}/reports
```

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du tableau de bord.

Appareil

Les appareils sont des objets de votre réseau qui ont été identifiés et classés par votre système ExtraHop. Pour plus d'informations, voir Appareils.

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

Fonctionnement	Descriptif
GET /appareils	Récupérez tous les appareils actifs au cours d'une période donnée. Pour plus d' informations, voir Extraire la liste des équipements via l'API REST. **Note:** Un équipement est considéré comme inactif après cinq minutes sans envoi ni réception de paquets. Toutefois, si un équipement recommence à envoyer ou à recevoir des paquets après une période d' inactivité inférieure à cinq jours, l'équipement est considéré comme ayant été actif de manière continue, y compris pendant la période d'inactivité.
POST /appareils/recherche	Récupérez tous les appareils qui répondent à des critères spécifiques. Pour plus d'informations, voir Rechercher un équipement via l'API REST. **Note:** Un équipement est considéré comme inactif après cinq minutes sans envoi ni réception de paquets. Toutefois, si un équipement recommence à envoyer ou à recevoir des paquets après une période d' inactivité inférieure à cinq jours, l'équipement est considéré comme ayant été actif de manière continue, y compris pendant la période d'inactivité.
OBTENIR /appareils/ {id}	Récupérez un équipement spécifique.
PATCH /appareils/ {id}	Mettez à jour un équipement spécifique.
GET /devices/ {id} /activité	Récupérez toutes les activités d'un équipement.
GET /devices/ {id} /alertes	Tout récupérer alertes qui sont assignés à un équipement spécifique.
POST /devices/ {id} /alertes	Attribuez et annulez l'attribution d'un équipement spécifique aux alertes.
SUPPRIMER /devices/ {id} /alerts/ {child-id}	Annuler l'attribution d'une alerte à un équipement spécifique.
POST /appareils/ {id} /alerts/ {child id}	Attribuez une alerte à un équipement spécifique.

Fonctionnement	Descriptif
GET /devices/ {id} /tableaux de bord	Récupérez tous les tableaux de bord relatifs à un équipement spécifique.
GET /appareils/ {id} /groupes de périphériques	Tout récupérer groupes d'équipements qui sont assignés à un équipement spécifique.
POST /appareils/ {id} /devicegroups	Attribuez et annulez l'attribution d'un équipement spécifique à des groupes d'équipements.
SUPPRIMER /devices/ {id} /devicegroups/ {child-id}	Annuler l'attribution d'un groupe déquipements à un équipement spécifique.
POST /appareils/ {id} /devicegroups/ {child id}	Assignez un groupe déquipements à un équipement spécifique.
GET /devices/ {id} /dnsnames	Récupérez tous les noms DNS associés à un équipement spécifique.
GET /appareils/ {id} /ipaddrs	Récupérez toutes les adresses IP associées à un équipement spécifique au cours d'une période donnée.
GET /devices/ {id} /software	Récupérez la liste des logiciels exécutés sur l'équipement spécifié.
GET /devices/ {id} /tags	Récupérez toutes les balises attribuées à un équipement spécifique.
POST /appareils/ {id} /tags	Attribuez et annulez l'attribution d'un équipement spécifique aux tags.
SUPPRIMER /devices/ {id} /tags/ {child-id}	Annuler l'attribution d'un tag à un équipement spécifique.
POST /appareils/ {id} /tags/ {child id}	Attribuez une étiquette à un équipement spécifique.
GET /appareils/ {id} /déclencheurs	Récupérez tous les déclencheurs assignés à un équipement spécifique.
POST /appareils/ {id} /déclencheurs	Attribuez et annulez l'attribution d'un équipement spécifique aux déclencheurs.
SUPPRIMER /devices/ {id} /triggers/ {child-id}	Annuler l'attribution d'un déclencheur à un équipement spécifique.
POST /appareils/ {id} /triggers/ {child id}	Assignez un déclencheur à un équipement spécifique.

Détails de l'opération

`GET /devices`

Spécifiez les paramètres suivants.

`active_from:` ***Numéro***

(Facultatif) L'horodateur de début de la demande. Renvoie uniquement les appareils actifs après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`active_until:` ***Numéro***

(Facultatif) L'horodateur de fin de la demande. Renvoie uniquement l'équipement actif avant cette heure. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre active_from.

`limit:` ***Numéro***

(Facultatif) Limitez le nombre d'appareils renvoyés au nombre maximum spécifié.

`offset:` ***Numéro***

(Facultatif) Ignorez les premiers résultats de l'équipement. Ce paramètre est souvent associé au paramètre limite.

`search_type:` ***Corde***

Indique le champ dans lequel effectuer la recherche.

Les valeurs suivantes sont valides :

- `any`
- `name`
- `discovery_id`
- `ip address`
- `mac address`
- `vendor`
- `type`
- `tag`
- `activity`
- `node`
- `vlan`
- `discover time`

`value:` ***Corde***

(Facultatif) Spécifie les critères de recherche.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.


```
{
    "activity": [],
    "analysis": "string",
    "analysis_level": 0,
    "auto_role": "string",
    "cdp_name": "string",
    "cloud_account": "string",
    "cloud_instance_description": "string",
    "cloud_instance_id": "string",
    "cloud_instance_name": "string",
    "cloud_instance_type": "string",
    "critical": true,
    "custom_criticality": "string",
    "custom_make": "string",
    "custom_model": "string",
    "custom_name": "string",
    "custom_type": "string",
    "default_name": "string",
    "description": "string",
    "device_class": "string",
    "dhcp_name": "string",
    "discover_time": 0,
    "discovery_id": "string",
    "display_name": "string",
    "dns_name": "string",
    "extrahop_id": "string",
    "id": 0,
```

```
    "ipaddr4": "string",
    "ipaddr6": "string",
    "is_l3": true,
    "last_seen_time": 0,
    "macaddr": "string",
    "mod_time": 0,
    "model": "string",
    "model_override": "string",
    "netbios_name": "string",
    "node_id": 0,
    "on_watchlist": true,
    "parent_id": 0,
    "role": "string",
    "subnet_id": "string",
    "user_mod_time": 0,
    "vendor": "string",
    "vlanid": 0,
    "vpc_id": "string"
}
```


`POST /devices/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les critères relatifs à l'équipement.

`active_from:` ***Numéro***

(Facultatif) L'horodateur de début de la demande. Renvoie uniquement les appareils actifs après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`active_until:` ***Numéro***

(Facultatif) L'horodateur de fin de la demande. Renvoie uniquement les appareils actifs avant cette heure. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre active_from.

`limit:` ***Numéro***

(Facultatif) Limitez le nombre d'appareils renvoyés au nombre maximum spécifié.

`offset:` ***Numéro***

(Facultatif) Ignorez le nombre d'appareils spécifié. Ce paramètre est souvent associé au paramètre limit pour paginer les ensembles de résultats.

`filter:` ***Objet***

(Facultatif) Spécifiez les critères de filtre pour les résultats de recherche.

`field:` ***Corde***

Le nom du champ sur lequel filtrer les résultats. La recherche compare le contenu du paramètre de champ à la valeur du paramètre d'opérande.

Les valeurs suivantes sont valides :

- `name`
- `discovery_id`
- `ipaddr`
- `macaddr`
- `vendor`

- `tag`
- `activity`
- `node`
- `vlan`
- `discover_time`
- `role`
- `dns_name`
- `dhcp_name`
- `netbios_name`
- `cdp_name`
- `custom_name`
- `software`
- `software_type`
- `model`
- `is_critical`
- `instance_id`
- `instance_name`
- `instance_type`
- `cloud_account`
- `vpc_id`
- `subnet_id`
- `is_active`
- `analysis`
- `network_locality_type`
- `network_locality_id`
- `id`

`operator:` ***Corde***

Méthode de comparaison appliquée lors de la mise en correspondance de la valeur de l'opérande avec le contenu du champ. Tous les objets filtrants nécessitent un opérateur.

Les valeurs suivantes sont valides :

- `>`
- `<`
- `<=`
- `>=`
- `=`
- `!=`
- `startswith`
- `and`
- `or`
- `not`
- `exists`
- `not_exists`
- `~`
- `!~`
- `in`
- `not_in`

`operand:` ***Chaîne ou nombre ou objet ou tableau***

La valeur à laquelle la requête tente de faire correspondre. La requête compare la valeur de l'opérande au contenu du paramètre de champ et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier l'opérande sous la forme d'une chaîne, d'un entier ou d'un objet. Pour plus d'informations sur les valeurs des objets, consultez Guide de l'API REST.

`rules:` ***Tableau d'objets***

Tableau d'un ou de plusieurs objets filtrants, qui peuvent être intégrés de manière récursive. Seuls les opérateurs « et », « ou » et « non » sont autorisés pour ce paramètre.

`result_fields:` ***Tableau de cordes***

(Facultatif) Renvoie les champs spécifiés et l'identifiant de l'équipement. Si cette option n'est pas spécifiée, tous les champs sont renvoyés.

Les valeurs suivantes sont valides :

- `mod_time`
- `node_id`
- `id`
- `extrahop_id`
- `discovery_id`
- `display_name`
- `description`
- `user_mod_time`
- `discover_time`
- `vlanid`
- `parent_id`
- `macaddr`
- `vendor`
- `is_l3`
- `ipaddr4`
- `ipaddr6`
- `device_class`
- `default_name`
- `custom_name`
- `cdp_name`
- `dhcp_name`
- `netbios_name`
- `dns_name`
- `custom_type`
- `auto_role`
- `analysis_level`
- `analysis`
- `role`
- `on_watchlist`
- `last_seen_time`
- `activity`
- `model`
- `model_override`
- `custom_make`
- `custom_model`
- `critical`

- custom_criticality
- cloud_instance_id
- cloud_instance_type
- cloud_instance_description
- cloud_instance_name
- cloud_account
- vpc_id
- subnet_id

Spécifiez le paramètre body au format JSON suivant.

```
{
    "active_from": 0,
    "active_until": 0,
    "filter": {
        "field": "string",
        "operator": "string",
        "operand": "string",
        "rules": []
    },
    "limit": 0,
    "offset": 0,
    "result_fields": []
}
```

`GET /devices/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "activity": [],
    "analysis": "string",
    "analysis_level": 0,
    "auto_role": "string",
    "cdp_name": "string",
    "cloud_account": "string",
    "cloud_instance_description": "string",
    "cloud_instance_id": "string",
    "cloud_instance_name": "string",
    "cloud_instance_type": "string",
    "critical": true,
    "custom_criticality": "string",
    "custom_make": "string",
    "custom_model": "string",
    "custom_name": "string",
    "custom_type": "string",
    "default_name": "string",
    "description": "string",
    "device_class": "string",
    "dhcp_name": "string",
    "discover_time": 0,
    "discovery_id": "string",
    "display_name": "string",
    "dns_name": "string",
```

```
    "extrahop_id": "string",
    "id": 0,
    "ipaddr4": "string",
    "ipaddr6": "string",
    "is_l3": true,
    "last_seen_time": 0,
    "macaddr": "string",
    "mod_time": 0,
    "model": "string",
    "model_override": "string",
    "netbios_name": "string",
    "node_id": 0,
    "on_watchlist": true,
    "parent_id": 0,
    "role": "string",
    "subnet_id": "string",
    "user_mod_time": 0,
    "vendor": "string",
    "vlanid": 0,
    "vpc_id": "string"
}
```


`PATCH /devices/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour des valeurs de propriété spécifiées à l'équipement.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`GET /devices/{id}/activity`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.


```
{
    "device_id": 0,
    "from_time": 0,
    "id": 0,
    "mod_time": 0,
    "stat_name": "string",
    "until_time": 0
}
```


`GET /devices/{id}/ipaddrs`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`from:` ***Numéro***

(Facultatif) Récupère les adresses IP associées à l'équipement après la date spécifiée, exprimée en millisecondes depuis l'époque.

`until:` ***Numéro***

(Facultatif) Récupère les adresses IP associées à l'équipement avant la date spécifiée, exprimées en millisecondes depuis l'époque.

`GET /devices/{id}/dnsnames`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`from:` ***Numéro***

(Facultatif) Récupère les noms DNS associés à l'équipement après la date spécifiée, exprimés en millisecondes depuis l'époque.

`until:` ***Numéro***

(Facultatif) Récupère les noms DNS associés à l'équipement avant la date spécifiée, exprimés en millisecondes depuis l'époque.

`GET /devices/{id}/triggers`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`direct_assignments_only:` ***Booléen***

(Facultatif) Limitez les résultats aux seuls déclencheurs directement attribués à l'équipement.

`POST /devices/{id}/triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Liste d'identifiants uniques pour les déclencheurs attribués et non attribués à l'équipement.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`POST /devices/{id}/triggers/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du déclencheur.

`id:` ***Numéro***
L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`DELETE /devices/{id}/triggers/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du déclencheur.

`id:` ***Numéro***
L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`GET /devices/{id}/dashboards`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`GET /devices/{id}/devicegroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique de l'équipement.

`active_from:` ***Numéro***
(Facultatif) L'horodateur de début de la demande. Renvoie uniquement les groupes d'équipements dynamiques auxquels l'équipement appartenait après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`active_until:` ***Numéro***
(Facultatif) L'horodateur de fin de la demande. Renvoie uniquement les groupes d'équipements dynamiques auxquels l'équipement appartenait avant cette heure. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre active_from.

`POST /devices/{id}/devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les groupes d'appareils qui sont attribués et non attribués à l'appareil.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`POST /devices/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`DELETE /devices/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`GET /devices/{id}/tags`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`POST /devices/{id}/tags`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Liste d'identifiants uniques pour les étiquettes attribuées et non attribuées à l'équipement.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
```

```
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`POST /devices/{id}/tags/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de la balise.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`DELETE /devices/{id}/tags/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de la balise.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`GET /devices/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`direct_assignments_only:` ***Booléen***

(Facultatif) Limitez les résultats aux seules alertes directement attribuées à l'équipement.

`POST /devices/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La liste des identifiants uniques pour les alertes attribuées et non attribuées à l'équipement.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

```
POST /devices/{id}/alerts/{child-id}
```

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

```
DELETE /devices/{id}/alerts/{child-id}
```

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

```
GET /devices/{id}/software
```

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'appareil, qui est affiché en tant qu'ID API sur la page de l'équipement dans le système ExtraHop.

`from:` ***Numéro***

(Facultatif) Renvoie le logiciel observé sur l'équipement après la date spécifiée, exprimée en millisecondes depuis l'époque.

`until:` ***Numéro***

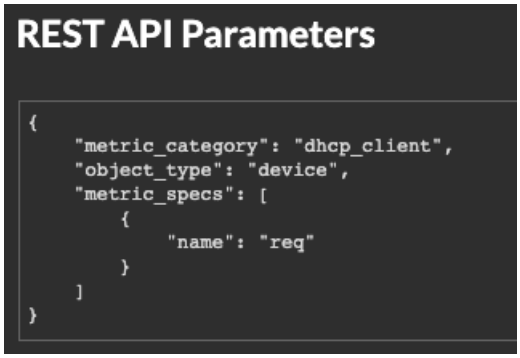
(Facultatif) Renvoie le logiciel observé sur l'équipement avant la date spécifiée, exprimée en millisecondes depuis l'époque.

Valeurs d'opérandes pour la recherche d'équipements

L'opération POST /devices/search vous permet de rechercher des appareils selon des critères spécifiés dans les objets de filtre. Chaque objet doit contenir une valeur unique pour `operand` champ valide pour le champ spécifié `field` valeur.

```
activity
```

Pour effectuer une recherche par activité métrique, spécifiez `field` valeur en tant que `activity` et le `operand` valeur en tant que `metric_category`. Vous pouvez trouver `metric_category` valeurs dans la section Paramètres de l'API REST du catalogue de métriques.



L'exemple suivant renvoie des résultats pour les périphériques qui correspondent à toutes les activités métriques classées pour un client DHCP, telles que le nombre de requêtes DHCP envoyées.

```
{
    "filter":  {
        "field": "activity",
        "operand": "dhcp_client",
        "operator": "="
    }
}
```

Conseil Récupérez par programmation une liste de toutes les activités métriques d'un équipement via `GET /devices/{id}/activity` opération. Le `stat_name` la valeur correspond à `metric_category` valeur dans `metric_catalog`, après le dernier point.

Dans l'exemple de réponse suivant, `stat_name` la valeur est `extrahop.device.dhcp_client`. Supprimez le texte avant le dernier point pour identifier `metric_catalog` valeur de `dhcp_client`.

```
{
    "id": 198606,
    "from_time": 1581537120000,
    "until_time": 1581542520000,
    "mod_time": 1581542533963,
    "device_id": 30096,
    "stat_name": "extrahop.device.dhcp_client"
}
```

analyse

Pour effectuer une recherche par niveau d'analyse de l'équipement, spécifiez `field` valeur en tant que `analysis` et le `operand` valeur sous la forme de l'une des chaînes suivantes :

standard
: Appareils en Analyse standard.

avancé
: Appareils en Analyse avancée.

découverte
: Appareils en mode de découverte.

l2_exempt
: Appareils dans L2 Parent Analysis.

journal des flux
: Appareils utilisés pour l'analyse des flux.

`discover_time`

Pour effectuer une recherche par plage de temps, spécifiez `field` valeur en tant que `discover_time` et un `operand` valeur avec `from` et `until` paramètres, où les valeurs sont des dates, exprimées en millisecondes depuis l'époque.

L'exemple suivant renvoie les résultats de toutes les activités de l'équipement survenues entre 13 h 00 et 15 h 00 le 21 août 2019.

```
{
    "filter":  {
        "field": "discover_time",
        "operand": {
            "from": "1566392400000",
            "until": "1566399600000"
        },
        "operator": "="
    }
}
```

`discovery_id`

Pour effectuer une recherche à l'aide de l'identifiant unique de l'équipement, spécifiez `field` valeur en tant que `discovery_id` et le `operand` valeur en tant qu'ID de découverte.

```
{
  "filter": {
    "field": "discovery_id",
    "operand": "c12vf90qpg290000",
    "operator": "="
  }
}
```

identifiant

Pour récupérer plusieurs appareils, spécifiez la valeur du champ comme `id`, le `operator` valeur comme `in`, et le `operand` valeur sous forme de tableau d'identifiants.

```
{
  "filter": {
    "field": "id",
    "operand": [5388,5387],
    "operator": "in"
  }
}
```

Pour exclure des appareils des résultats de recherche, spécifiez un filtre comportant plusieurs règles et spécifiez une règle dont la valeur du champ est `id`, le `operator` valeur en tant que `not_in`, et le `operand` valeur sous forme de tableau d'identifiants.

```
{
  "filter": {
    "operator": "and",
    "rules": [
      {
        "field": "id",
        "operand": [5388,5387],
        "operator": "not_in"
      },
      {
        "field": "discover_time",
```

```
        "operand": {
          "from": "1692984750000",
          "until": "1693416750000"
        },
        "operator": "="
      }
    ]
  }
}
```

est_actif

Pour effectuer une recherche en fonction des appareils qui ont été actifs au cours des 30 dernières minutes, spécifiez la valeur du champ comme `is_active` et le `operand` valeur sous forme de booléen.

```
{
  "filter": {
    "field": "is_active",
    "operand": true,
    "operator": "="
  }
}
```

`ipaddr`

Pour effectuer une recherche par adresse IP, spécifiez `field` valeur en tant que `ipaddr` et le `operand` valeur sous forme d'adresse IP ou de bloc CIDR.

```
{
  "filter": {
    "field": "ipaddr",
    "operand": "192.168.12.0/28",
    "operator": "="
  }
}
```

`node`

Pour effectuer une recherche à l'aide de l'identifiant unique d'un sonde, spécifiez `field` valeur en tant que `node` et le `operand` valeur en tant que sonde UUID.

```
{
  "filter": {
    "field": "node",
    "operand": "qqvsplfa-zxsk-32l0-19g1-076vfr42pw31",
    "operator": "="
  }
}
```

`macaddr`

Pour effectuer une recherche par adresse MAC d'un équipement, spécifiez la valeur du champ comme `macaddr` et la valeur de l'opérande en tant qu'adresse MAC de l'équipement. L'exemple suivant renvoie les résultats pour les appareils dont l'adresse MAC est `C1:1C:N2:0Q:PJ:10` ou `C1:1C:N2:0Q:PJ:11`.

```
{
  "filter": {
    "operator": "or",
    "rules": [
```

```
      {
        "field": "macaddr",
        "operand": "C1:1C:N2:0Q:PJ:10",
        "operator": "="
      },
      {
        "field": "macaddr",
        "operand": "C1:1C:N2:0Q:PJ:11",
        "operator": "="
      }
    ]
  }
}
```

`model`

Pour effectuer une recherche par modèle d'équipement, spécifiez `field` valeur en tant que `model`. Si l'opérateur est =, `!=`, `exists`, ou `not_exists`, spécifiez l'opérande comme identifiant de modèle, que vous pouvez afficher dans le `model` champ de `POST /device/search` réponses.

```
{
  "filter": {
    "field": "model",
    "operand": "apple_ipad_pro_12_9_inch_wifi_cellular_5th_gen",
    "operator": "="
  }
}
```

Si l'opérateur est ~ ou `!~`, spécifiez l'opérande comme nom de la marque et du modèle, que vous pouvez afficher dans le système ExtraHop lorsque vous recherchez un équipement.

```
{
  "filter": {
    "field": "model",
    "operand": "Apple iPad Pro",
    "operator": "~"
  }
}
```

`name`

Pour effectuer une recherche par nom d'affichage de l'équipement, spécifiez `field` valeur en tant que nom et `operand` valeur en tant que nom de l'équipement ou en tant que chaîne regex.

```
{
  "filter": {
    "field": "name",
    "operand": "VMware B2CEB6",
    "operator": "="
  }
}
```

id de localité du réseau

Pour effectuer une recherche par localité du réseau, spécifiez `field` valeur en tant que `network_locality_id` et la valeur de l'opérande en tant qu'ID de localité du réseau.

```
{
  "filter": {
    "field": "network_locality_id",
```

```
    "operand": 123,
    "operator": "="
  }
}
```

`role`

Pour effectuer une recherche par rôle d'équipement, spécifiez `field` valeur en tant que `role` et le `operand` valeur en tant que rôle de l'équipement.

```
{
  "filter": {
    "field": "role",
    "operand": "voip_phone",
    "operator": "="
  }
}
```

`software`

Pour effectuer une recherche à l'aide du logiciel exécuté sur l'équipement, spécifiez `field` valeur en tant que `software` et le `operand` valeur en tant qu'ID associé à ce logiciel sur le système ExtraHop.

```
{
  "filter": {
    "field": "software",
    "operand": "windows_10",
    "operator": "="
  }
}
```

Conseil Récupérez par programmation une liste de tous les identifiants logiciels associés à un équipement via `GET /devices/{id}/software` opération.

Dans l'exemple de réponse suivant, `id` la valeur du logiciel est `windows_10`.

```
[
  {
    "software_type": "OS",
    "name": "Windows",
    "version": "10",
    "description": null,
    "id": "windows_10"
  }
]
```

`software_type`

Pour effectuer une recherche par type de logiciel exécuté sur l'équipement, spécifiez `field` valeur en tant que `software_type` et le `operand` valeur en tant qu'ID de type de logiciel.

```
{
  "filter": {
    "field": "software_type",
    "operand": "OS",
    "operator": "="
  }
}
```

Conseil Récupérez par programmation une liste de tous les identifiants de type de logiciel associés à un équipement via `GET /devices/{id}/software` opération.

Dans l'exemple de réponse suivant, la valeur d'ID pour le type de logiciel est `OS`.

```
[
  {
    "software_type": "OS",
    "name": "Windows",
    "version": "10",
    "description": null,
    "id": "windows_10"
  }
]
```

`tag`

Pour effectuer une recherche par étiquette d'équipement, spécifiez `field` valeur en tant que `tag` et le `operand` valeur en tant que nom de balise ou en tant que chaîne regex.

```
{
  "filter": {
    "field": "tag",
    "operand": "Custom Tag",
    "operator": "="
  }
}
```

Conseil Récupérez par programmation une liste de toutes les étiquettes de l'équipement via `GET /devices/{id}/tags` opération.

Dans l'exemple de réponse suivant, `name` la valeur de la balise est `Custom Tag`.

```
[
  {
    "mod_time": 1521577040934,
    "id": 19,
    "name": "Custom Tag"
  }
]
```

`user`

Pour effectuer une recherche par utilisateur, spécifiez `field` valeur comme `user` et le `operand` valeur en tant que nom d'utilisateur ou en tant que chaîne regex .

```
{
  "filter": {
    "field": "user",
    "operand": "user@example.extrahop.com",
    "operator": "="
  }
}
```

vlan

Pour effectuer une recherche par l'ID d'un VLAN, spécifiez `field` valeur en tant que `vlan` et le `operand` valeur en tant qu'ID du VLAN.

```
{
```

```
  "filter": {
    "field": "vlan",
    "operand": "0",
    "operator": "="
  }
}
```

Recherche à l'aide d'expressions régulières (regex)

Pour certains `field` valeurs, la chaîne peut être en syntaxe regex. Spécifiez le `operand` valeur en tant qu'objet ayant un `value` paramètre avec la syntaxe regex que vous souhaitez faire correspondre et un `is_regex` paramètre défini sur `true`. L'exemple suivant renvoie les résultats pour tous les noms DNS qui se terminent par `com`.

```
{
    "filter":  {
        "field": "dns_name",
        "operand": {
            "value": ".*?com",
            "is_regex": true
        },
        "operator": "="
    }
}
```

Un `operand` le champ avec la syntaxe regex est valide pour les éléments suivants `field` valeurs :

- nom_cdp
- nom_personnalisé
- nom_DNS
- nom_dhcp
- modèle
- nom
- nom_netbios
- logiciel
- étiquette
- fournisseur

Unités de temps prises en charge

Pour la plupart des paramètres, l'unité par défaut pour la mesure du temps est la milliseconde. Toutefois, les paramètres suivants renvoient ou acceptent des unités de temps alternatives telles que les minutes et les heures :

- Appareil
  - actif_depuis
  - actif_jusqu'à
- Groupe d'appareils
  - actif_depuis
  - actif_jusqu'à
- Métriques
  - à partir de
  - jusqu'à
- Journal d'enregistrement
  - à partir de

- jusqu'à
- context_ttl

Le tableau suivant indique les unités de temps prises en charge :

Unité de temps	Suffixe d'unité
Année	`y`
Mois	`M`
Semaine	`w`
Journée	`d`
Heure	`h`
Minutes	`m`
Deuxième	`s`
Milliseconde	`ms`

Pour spécifier une unité de temps autre que les millisecondes pour un paramètre, ajoutez le suffixe de l'unité à la valeur. Par exemple, pour demander des appareils actifs au cours des 30 dernières minutes, spécifiez la valeur de paramètre suivante :

```
GET /api/v1/devices?active_from=-30m
```

L'exemple suivant indique une recherche pour HTTP records créés il y a 1 à 2 heures :

```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Groupe d'appareils

Groupes d'appareils peut être statique ou dynamique.

Un groupe de dispositifs statique est défini par l'utilisateur ; vous créez un groupe de dispositifs, puis vous identifiez et attribuez manuellement chaque équipement à ce groupe. Un groupe dequipment dynamique est défini et géré automatiquement par un ensemble de règles configurées.

Par exemple, vous pouvez créer un groupe d'équipements, puis définir une règle pour classer tous les appareils appartenant à une certaine plage d'adresses IP à ajouter automatiquement à ce groupe. Pour plus d'informations, voir Groupes d'appareils.

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

Fonctionnement	Descriptif
GET /devicegroups	Récupérez tous les groupes d'équipements actifs au cours d'une période donnée.
POST/groupes d'appareils	Créez un nouveau groupe d'équipements.
SUPPRIMER /devicegroups/ {id}	Supprimez un groupe déquipements.
OBTENEZ /devicegroups/ {id}	Récupérez un groupe déquipements spécifique.

Fonctionnement	Descriptif
PATCH /devicegroups/ {id}	Mettez à jour un groupe d'équipements spécifique.
GET /devicegroups/ {id} /alertes	Tout récupérer alertes qui sont affectés à un groupe d'équipements spécifique.
POST /devicegroups/ {id} /alertes	Attribuez et annulez l'attribution d'un groupe déquipements spécifique aux alertes.
SUPPRIMER /devicegroups/ {id} /alerts/ {child-id}	Annuler l'attribution d'une alerte à un groupe déquipements spécifique.
POST /devicegroups/ {id} /alerts/ {child id}	Attribuez une alerte à un groupe déquipements spécifique.
GET /devicegroups/ {id} /tableaux de bord	Récupérez tous les tableaux de bord associés à un groupe déquipements spécifique.
GET /devicegroups/ {id} /appareils	Récupérez tous les appareils du groupe déquipements actifs au cours d'une période donnée. **Note:** Un équipement est considéré comme inactif après cinq minutes sans envoi ni réception de paquets. Toutefois, si un équipement recommence à envoyer ou à recevoir des paquets après une période d' inactivité inférieure à cinq jours, l'équipement est considéré comme ayant été actif de manière continue, y compris pendant la période d'inactivité.
POST /devicegroups/ {id} /appareils	Attribuez et annulez l'attribution d'appareils à un groupe de dispositifs statique spécifique.
SUPPRIMER /devicegroups/ {id} /devices/ {child-id}	Annulation de l'attribution d'un équipement à un groupe de dispositifs statique spécifique.
POST /devicegroups/ {id} /appareils/ {child id}	Assignez un équipement à un groupe de dispositifs statique spécifique.
GET /devicegroups/ {id} /déclencheurs	Récupérez tous les déclencheurs assignés à un groupe déquipements spécifique.
POST /devicegroups/ {id} /déclencheurs	Attribuez et annulez l'attribution d'un groupe déquipements spécifique aux déclencheurs.
SUPPRIMER /devicegroups/ {id} /triggers/ {child-id}	Annulez l'attribution d'un déclencheur à un groupe déquipements spécifique.
POST /devicegroups/ {id} /triggers/ {child id}	Assignez un déclencheur à un groupe déquipements spécifique.

Détails de l'opération

`GET /devicegroups`

Spécifiez les paramètres suivants.

`since:` ***Numéro***

(Facultatif) Renvoie uniquement les groupes d'équipements qui ont été modifiés après cette période, exprimés en millisecondes depuis l'époque.

`all:` ***Booléen***

(Facultatif) Obsolète. Remplacé par le paramètre type.

`name:` ***Corde***

(Facultatif) La valeur de recherche Regex pour filtrer les groupes d'équipements par nom.

`type:` ***Corde***

(Facultatif) Renvoie uniquement les groupes d'équipements du type spécifié.

Les valeurs suivantes sont valides :

- `user_created`
- `built_in`
- `all`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "built_in": true,
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {},
    "id": 0,
    "include_custom_devices": true,
    "mod_time": 0,
    "name": "string",
    "value": "string"
}
```

`GET /devicegroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "built_in": true,
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {},
    "id": 0,
    "include_custom_devices": true,
    "mod_time": 0,
    "name": "string",
    "value": "string"
}
```

`POST /devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées au nouveau groupe dcesséquipements.

`description:` ***Corde***

Description facultative du groupe dO'équipements.

`name:` ***Corde***

Le nom convivial du groupe dcesséquipements.

`include_custom_devices:` ***Booléen***

(Facultatif) Obsolète. Remplacé par le paramètre de filtre.

`dynamic:` ***Booléen***

(Facultatif) Indique si le groupe dafficheurs est dynamique.

`field:` ***Corde***

Obsolète. Remplacé par le paramètre de filtre.

Les valeurs suivantes sont valides :

- `any`
- `name`
- `ip address`
- `mac address`
- `vendor`
- `type`
- `tag`
- `vlan`
- `activity`
- `node`
- `discover time`

`value:` ***Objet***

(Facultatif) Obsolète. Remplacé par le paramètre de filtre.

`filter:` ***Objet***

(Facultatif) Spécifiez les critères de filtre pour les résultats de recherche.

`field:` ***Corde***

Le nom du champ sur lequel filtrer les résultats. La recherche compare le contenu du paramètre de champ à la valeur du paramètre d'opérande.

Les valeurs suivantes sont valides :

- `name`
- `ipaddr`
- `macaddr`
- `vendor`
- `tag`
- `activity`
- `node`
- `vlan`
- `discover_time`
- `role`
- `dns_name`
- `dhcp_name`
- `netbios_name`
- `cdp_name`
- `custom_name`
- `software`
- `model`

- `is_critical`
- `instance_id`
- `instance_name`
- `instance_type`
- `cloud_account`
- `vpc_id`
- `subnet_id`
- `is_active`
- `network_locality_type`
- `network_locality_id`
- `id`

`operator:` ***Corde***

Méthode de comparaison appliquée lors de la mise en correspondance de la valeur de l'opérande avec le contenu du champ. Tous les objets filtrants nécessitent un opérateur.

Les valeurs suivantes sont valides :

- `>`
- `<`
- `<=`
- `>=`
- `=`
- `!=`
- `startswith`
- `and`
- `or`
- `not`
- `exists`
- `not_exists`
- `~`
- `!~`

`operand:` ***Chaîne, numéro ou objet***

La valeur à laquelle la requête tente de faire correspondre. La requête compare la valeur de l'opérande au contenu du paramètre de champ et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier l'opérande sous la forme d'une chaîne, d'un entier ou d'un objet. Pour plus d'informations sur les valeurs des objets, consultez Guide de l'API REST.

`rules:` ***Tableau d'objets***

Tableau d'un ou de plusieurs objets filtrants, qui peuvent être intégrés de manière récursive. Seuls les opérateurs « et », « ou » et « non » sont autorisés pour ce paramètre.

`editors:` ***Tableau de cordes***

(Facultatif) La liste des utilisateurs qui peuvent modifier le groupe dcesséquipements.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "dynamic": true,
    "editors": [],
    "field": "string",
    "filter": {
        "field": "string",
        "operator": "string",
```

```
        "operand": "string",
        "rules": []
    },
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`DELETE /devicegroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`PATCH /devicegroups/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Applique les mises à jour des valeurs de propriétés spécifiées à un groupe dcesséquipements spécifique.

`description:` ***Corde***

Description facultative du groupe dO'équipements.

`name:` ***Corde***

Le nom convivial du groupe dcesséquipements.

`include_custom_devices:` ***Booléen***

(Facultatif) Obsolète. Remplacé par le paramètre de filtre.

`field:` ***Corde***

Obsolète. Remplacé par le paramètre de filtre.

Les valeurs suivantes sont valides :

- `any`
- `name`
- `ip address`
- `mac address`
- `vendor`
- `type`
- `tag`
- `vlan`
- `activity`
- `node`
- `discover time`

`value:` ***Objet***

(Facultatif) Obsolète. Remplacé par le paramètre de filtre.

`filter:` ***Objet***

(Facultatif) Spécifiez les critères de filtre pour les résultats de recherche.

`editors:` ***Tableau de cordes***

(Facultatif) La liste des utilisateurs qui peuvent modifier le groupe dcesséquipements.

Spécifiez le paramètre body au format JSON suivant.

```
{
```

```
    "description": "string",
    "editors": [],
    "field": "string",
    "filter": {},
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`direct_assignments_only:` ***Booléen***

(Facultatif) Limitez les résultats aux seules alertes directement attribuées au groupe dcesséquipements.

`POST /devicegroups/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`DELETE /devicegroups/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La liste des identifiants uniques pour les alertes attribuées et non attribuées au groupe dcesséquipements.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
```

```
    "unassign": []
}
```

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/triggers`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`direct_assignments_only:` ***Booléen***

(Facultatif) Limitez les résultats aux seuls déclencheurs qui sont directement affectés au groupe dcesséquipements.

`POST /devicegroups/{id}/triggers/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`DELETE /devicegroups/{id}/triggers/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La liste des identifiants uniques pour les déclencheurs attribués et non attribués au groupe dcesséquipements.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique d'un équipement.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`DELETE /devicegroups/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique d'un équipement.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La liste des identifiants uniques pour les appareils attribués et non attribués au groupe dcesséquipements.

`assign:` ***Tableau de nombres***

Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/devices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`active_from:` ***Numéro***

(Facultatif) L'horodateur de début de la demande. Renvoie uniquement les appareils actifs après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`active_until:` ***Numéro***

(Facultatif) L'horodateur de fin de la demande. Renvoie uniquement l'équipement actif avant cette heure. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre active_from.

`limit:` ***Numéro***

(Facultatif) Limitez le nombre d'appareils retournés.

`offset:` ***Numéro***

(Facultatif) Ignorez les premiers résultats de l'équipement. Ce paramètre est souvent associé au paramètre limite.

```
GET /devicegroups/{id}/dashboards
```

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

Unités de temps prises en charge

Pour la plupart des paramètres, l'unité par défaut pour la mesure du temps est la milliseconde. Toutefois, les paramètres suivants renvoient ou acceptent des unités de temps alternatives telles que les minutes et les heures :

- Appareil
  - actif_depuis
  - actif_jusqu'à
- Groupe d'appareils
  - actif_depuis
  - actif_jusqu'à
- Métriques
  - à partir de
  - jusqu'à
- Journal d'enregistrement
  - à partir de
  - jusqu'à
  - context_ttl

Le tableau suivant indique les unités de temps prises en charge :

Unité de temps	Suffixe d'unité
Année	`y`
Mois	`M`
Semaine	`w`
Journée	`d`
Heure	`h`
Minutes	`m`
Deuxième	`s`
Milliseconde	`ms`

Pour spécifier une unité de temps autre que les millisecondes pour un paramètre, ajoutez le suffixe de l'unité à la valeur. Par exemple, pour demander des appareils actifs au cours des 30 dernières minutes, spécifiez la valeur de paramètre suivante :

```
GET /api/v1/devices?active_from=-30m
```

L'exemple suivant indique une recherche pour HTTP records créés il y a 1 à 2 heures :

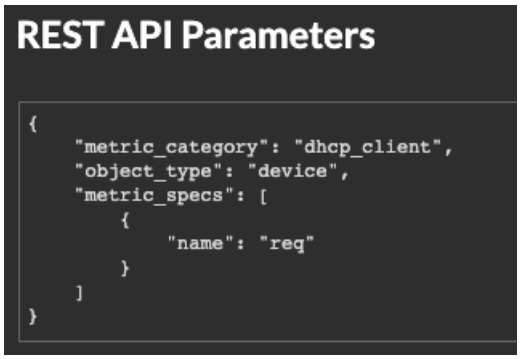
```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Valeurs d'opérandes pour les groupes d'équipements

L'opération POST /devicegroups vous permet de créer des groupes d'équipements en fonction de critères spécifiés dans les objets de filtre. Chaque objet doit contenir une valeur unique pour `operand` champ valide pour le champ spécifié `field` valeur.

`activity`

Pour sélectionner les appareils par activité métrique, spécifiez `field` valeur en tant que `activity` et le `operand` valeur en tant que `metric_category`. Vous pouvez trouver `metric_category` valeurs dans la section Paramètres de l'API REST du catalogue de métriques.



L'exemple suivant sélectionne les périphériques dont l'activité est classée de manière métrique pour un client DHCP, comme le nombre de requêtes DHCP envoyées.

```
{
    "filter":  {
        "field": "activity",
        "operand": "dhcp_client",
        "operator": "="
    }
}
```

Conseil: Récupérez par programmation une liste de toutes les activités métriques d'un équipement via `GET /devices/{id}/activity` opération. Le `stat_name` la valeur correspond à `metric_category` valeur dans `metric_catalog`, après le dernier point.

Dans l'exemple de réponse suivant, `stat_name` la valeur est `extrahop.device.dhcp_client`. Supprimez le texte avant le dernier point pour identifier `metric_catalog` valeur de `dhcp_client`.

```
{
    "id": 198606,
    "from_time": 1581537120000,
```

```
    "until_time": 1581542520000,
    "mod_time": 1581542533963,
    "device_id": 30096,
    "stat_name": "extrahop.device.dhcp_client"
}
```

`discover_time`

Pour sélectionner les appareils en fonction d'une plage de temps, spécifiez `field` valeur en tant que `discover_time` et un `operand` valeur avec `from` et `until` paramètres, où les valeurs sont des dates, exprimées en millisecondes depuis l'époque.

L'exemple suivant sélectionne les appareils dont l'activité s'est produite entre 13 h 00 et 15 h 00 le 21 août 2019.

```
{
    "filter":  {
        "field": "discover_time",
        "operand": {
            "from": "1566392400000",
            "until": "1566399600000"
        },
        "operator": "="
    }
}
```

`discovery_id`

Pour sélectionner des appareils par identifiant d'équipement unique, spécifiez `field` valeur en tant que `discovery_id` et le `operand` valeur en tant qu'ID de découverte.

```
{
  "filter": {
    "field": "discovery_id",
    "operand": "c12vf90qpg290000",
    "operator": "="
  }
}
```

`ipaddr`

Pour sélectionner les appareils par adresse IP, spécifiez `field` valeur en tant que `ipaddr` et le `operand` valeur sous forme d'adresse IP ou de bloc CIDR.

```
{
  "filter": {
    "field": "ipaddr",
    "operand": "192.168.12.0/28",
    "operator": "="
  }
}
```

`node`

Pour sélectionner des appareils à l'aide de l'identifiant unique d'un sonde, spécifiez le `field` valeur en tant que `node` et le `operand` valeur en tant qu' UUID de l'appliance.

```
{
  "filter": {
```

```
    "field": "node",
    "operand": "qqvsplfa-zxsk-32l0-19g1-076vfr42pw31",
    "operator": "="
  }
}
```

`macaddr`

Pour sélectionner les appareils par adresse MAC, spécifiez la valeur du champ comme `macaddr` et la valeur de l'opérande en tant qu'adresse MAC de l'équipement. L'exemple suivant renvoie les résultats pour les appareils dont l'adresse MAC est `C1:1C:N2:0Q:PJ:10` ou `C1:1C:N2:0Q:PJ:11`.

```
{
  "filter": {
    "operator": "or",
    "rules": [
      {
        "field": "macaddr",
        "operand": "C1:1C:N2:0Q:PJ:10",
        "operator": "="
      },
      {
        "field": "macaddr",
        "operand": "C1:1C:N2:0Q:PJ:11",
        "operator": "="
      }
    ]
  }
}
```

`name`

Pour sélectionner les appareils par nom d'affichage, spécifiez `field` valeur en tant que nom et `operand` valeur en tant que nom de l'équipement ou en tant que chaîne regex.

```
{
  "filter": {
    "field": "name",
    "operand": "VMware B2CEB6",
    "operator": "="
  }
}
```

id de localité du réseau

Pour sélectionner les appareils par localité du réseau, spécifiez `field` valeur en tant que `network_locality_id` et la valeur de l'opérande en tant qu'ID de localité du réseau.

```
{
  "filter": {
    "field": "network_locality_id",
    "operand": 123,
    "operator": "="
  }
}
```

`role`

Pour sélectionner les appareils par rôle, spécifiez `field` valeur en tant que `role` et le `operand` valeur en tant que rôle de l'équipement.

```
{
  "filter": {
    "field": "role",
    "operand": "voip_phone",
    "operator": "="
  }
}
```

`software`

Pour sélectionner des appareils à l'aide du logiciel qui s'exécute sur l'équipement, spécifiez `field` valeur en tant que `software` et le `operand` valeur en tant qu'identifiant associé à ce logiciel sur le système ExtraHop ou en tant que chaîne regex.

```
{
  "filter": {
    "field": "software",
    "operand": "windows_10",
    "operator": "="
  }
}
```

Conseil Récupérez par programmation une liste de tous les identifiants logiciels associés à un équipement via `GET /devices/{id}/software` opération.

Dans l'exemple de réponse suivant, `id` la valeur du logiciel est `windows_10`.

```
[
  {
    "software_type": "OS",
    "name": "Windows",
    "version": "10",
    "description": null,
    "id": "windows_10"
  }
]
```

`tag`

Pour sélectionner les appareils par tag, spécifiez `field` valeur en tant que `tag` et le `operand` valeur en tant que nom de balise ou en tant que chaîne regex.

```
{
  "filter": {
    "field": "tag",
    "operand": "Custom Tag",
    "operator": "="
  }
}
```

Conseil Récupérez par programmation une liste de toutes les étiquettes de l'équipement via `GET /devices/{id}/tags` opération.

Dans l'exemple de réponse suivant, `name` la valeur de la balise est `Custom Tag`.

```
[
```

```
  {
    "mod_time": 1521577040934,
    "id": 19,
    "name": "Custom Tag"
  }
]
```

`user`

Pour sélectionner les appareils par utilisateur, spécifiez `field` valeur en tant que `user` et le `operand` valeur en tant que nom d'utilisateur ou en tant que chaîne regex .

```
{
  "filter": {
    "field": "user",
    "operand": "user@example.extrahop.com",
    "operator": "="
  }
}
```

vlan

Pour sélectionner les appareils en fonction de l'ID d'un VLAN, spécifiez le `field` valeur en tant que `vlan` et le `operand` valeur en tant qu'ID du VLAN.

```
{
  "filter": {
    "field": "vlan",
    "operand": "0",
    "operator": "="
  }
}
```

Recherche à l'aide d'expressions régulières (regex)

Pour certains `field` valeurs, la chaîne peut être en syntaxe regex. Spécifiez le `operand` valeur en tant qu'objet ayant un `value` paramètre avec la syntaxe regex que vous souhaitez faire correspondre et un `is_regex` paramètre défini sur `true`. L'exemple suivant sélectionne les appareils dont les noms DNS se terminent par `com`.

```
{
    "filter":  {
        "field": "dns_name",
        "operand": {
            "value": ".*?com",
            "is_regex": true
        },
        "operator": "="
    }
}
```

Un `operand` le champ avec la syntaxe regex est valide pour les éléments suivants `field` valeurs :

- nom_cdp
- nom_personnalisé
- nom_DNS
- nom_dhcp
- modèle
- nom

- nom_netbios
- logiciel
- étiquette
- fournisseur

Spécifiez plusieurs critères

Vous pouvez spécifier plusieurs critères à l'aide du `rules` champ. L'exemple suivant renvoie les résultats pour les appareils dont l'adresse IP est `192.168.12.0` ou `192.168.12.1`.

```
{
  "filter": {
    "operator": "or",
    "rules": [
      {
        "field": "ipaddr",
        "operand": "192.168.12.0",
        "operator": "="
      },
      {
        "field": "ipaddr",
        "operand": "192.168.12.1",
        "operator": "="
      }
    ]
  }
}
```

Note: Vous ne pouvez pas spécifier plus de 1 000 règles pour un groupe d'équipements.

Détections

La ressource Détections vous permet de récupérer les détections qui ont été identifiées par le système ExtraHop.

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

opération	Descriptif
GET /détections	Récupérez toutes les détections.
GET /detections/formats	Récupérez tous les types de détection.
GET /detections/formats/ {id}	Récupérez un type de détection spécifique.
POST /détections/formats	Créez un nouveau type de détection personnalisé.
SUPPRIMER /detections/formats/ {id}	Supprimez un type de détection personnalisé spécifique.
PATCH /detections/formats/ {id}	Mettez à jour un type de détection personnalisé spécifique.
GET /detections/rules/masquage	Récupérez toutes les règles d'exceptions.
GET /detections/rules/masquage/ {id}	Récupérez une règle de réglage spécifique.
POST /détections/règles/masquage	Créez une règle de réglage.
SUPPRIMER /detections/rules/hiding/ {id}	Supprimez une règle de réglage.

opération	Descriptif
PATCH /detections/rules/masquage/ {id}	Mettez à jour une règle de réglage.
POST /détections/recherche	Récupérez les détections qui correspondent aux critères de recherche spécifiés.
PATCH /détections/tickets	Mettez à jour un ticket associé à des détections.
GET /detections/ {id}	Récupérez une détection spécifique.
GET /detections/ {id} /investigations	Récupérez toutes les enquêtes faisant l'objet d'une détection spécifique
PATCH /detections/ {id}	Mettez à jour une détection.
SUPPRIMER /detections/ {id} /notes	Supprimez les notes relatives à une détection donnée.
GET /detections/ {id} /notes	Récupérez les notes pour une détection donnée.
PUT /detections/ {id} /notes	Créez ou remplacez des notes pour une détection donnée.
GET /detections/ {id} /related	Récupérez toutes les détections liées à une détection spécifique.

Détails de l'opération

`GET /detections/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique pour la détection.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.


```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "create_time": 0,
    "description": "string",
    "end_time": 0,
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
```

```
    "type": "string",
    "update_time": 0,
    "url": "string"
}
```

`GET /detections`

Spécifiez les paramètres suivants.

`limit:` ***Numéro***

(Facultatif) Limitez le nombre de détections renvoyées au nombre maximum spécifié. Une sélection aléatoire de détections est renvoyée.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "create_time": 0,
    "description": "string",
    "end_time": 0,
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0,
    "url": "string"
}
```

`POST /detections/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de recherche de détection.

`filter:` ***Objet***

Filtres spécifiques à la détection.

`category:` ***Corde***

Obsolète. Remplacé par le champ des catégories.

`categories:` ***Tableau de cordes***

Renvoie les détections provenant des catégories spécifiées.

`assignee:` ***Tableau de cordes***

Renvoie les détections attribuées à l'utilisateur spécifié. Spécifiez « .none » pour rechercher les détections non attribuées ou « .me » pour rechercher les détections attribuées à l'utilisateur authentifié.

`ticket_id:` ***Tableau de cordes***

Renvoie les détections associées aux tickets spécifiés. Spécifiez « .none » pour rechercher les détections qui ne sont pas associées à des tickets.

`status:` ***Tableau de cordes***

Renvoie les détections dont l'état est spécifié. Pour rechercher des détections dont le statut est nul, qui s'affiche dans le système ExtraHop comme Ouvert, spécifiez « .none ». Vous ne pouvez modifier le statut d'une détection en « nouveau » via l'API REST que lorsque le suivi des billets par des tiers est activé.

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***Tableau de cordes***

Renvoie les détections pour les tickets avec la résolution spécifiée. Spécifiez « .none » pour rechercher les détections sans résolution.

Les valeurs suivantes sont valides :

- `action_taken`
- `no_action_taken`

`types:` ***Tableau de cordes***

Renvoie les détections avec les types spécifiés.

`risk_score_min:` ***Numéro***

Renvoie les détections dont les scores de risque sont supérieurs ou égaux à la valeur spécifiée.

`recommended:` ***Booléen***

Renvoie les détections recommandées pour le triage. Ce champ n'est valide que sur une console.

`from:` ***Numéro***

Renvoie les détections survenues après la date spécifiée, exprimée en millisecondes depuis l'époque. Les détections qui ont débuté avant la date spécifiée sont renvoyées si la détection était en cours à ce moment-là.

`limit:` ***Numéro***

Ne renvoie pas plus que le nombre de détections spécifié.

`offset:` ***Numéro***

Le nombre de détections à ignorer pour la pagination.

`sort:` ***Tableau d'objets***

Trie les détections renvoyées en fonction des champs spécifiés. Par défaut, les détections sont triées par date de dernière mise à jour, puis par identifiant dans l'ordre croissant.

`direction:` ***Corde***

L'ordre dans lequel les détections renvoyées sont triées.

Les valeurs suivantes sont valides :

- `asc`
- `desc`

`field:` ***Corde***

Le champ permettant de trier les détections.

`until:` ***Numéro***

Renvoie les détections qui se sont terminées avant la date spécifiée, exprimée en millisecondes depuis l'époque.

`update_time:` ***Numéro***

Renvoie les détections liées à des événements survenus après la date spécifiée, exprimées en millisecondes depuis l'époque. Notez que le service d'apprentissage automatique ExtraHop analyse les données historiques pour générer des détections. Il existe donc un délai entre le moment où les événements à l'origine de ces détections se produisent et le moment où les détections sont générées. Si vous recherchez plusieurs fois des détections dans la même fenêtre update_time, la recherche ultérieure peut renvoyer des détections qui n'ont pas été renvoyées par la recherche précédente.

`mod_time:` ***Numéro***

Renvoie les détections qui ont été mises à jour après la date spécifiée, exprimées en millisecondes depuis l'époque.

`create_time:` ***Numéro***

Renvoie les détections créées après la date spécifiée, exprimée en millisecondes depuis l'époque. Pour les capteurs, cela renvoie les détections qui ont été générées après la date spécifiée. Pour les consoles, cela renvoie les détections qui ont été synchronisées pour la première fois avec la console après la date spécifiée.

`id_only:` ***Booléen***

(Facultatif) Renvoie uniquement les identifiants des détections.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "create_time": 0,
    "filter": {
        "category": "string",
        "categories": [],
        "assignee": [],
        "ticket_id": [],
        "status": [],
        "resolution": [],
        "types": [],
        "risk_score_min": 0,
        "recommended": true
    },
    "from": 0,
    "id_only": true,
    "limit": 0,
    "mod_time": 0,
    "offset": 0,
    "sort": {
        "direction": "string",
        "field": "string"
    },
    "until": 0,
    "update_time": 0
}
```

`PATCH /detections/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique pour la détection.

`body:` ***Objet***

Les paramètres de détection à mettre à jour.

`ticket_id:` ***Corde***

L'ID du ticket associé à la détection.

`assignee:` ***Corde***

Le destinataire de la détection ou le ticket associé à la détection.

`status:` ***Corde***

État de la détection ou du ticket associé à la détection. Si la valeur est nulle, l'état affiché dans le système ExtraHop est Open. La valeur « new » ne peut être spécifiée via l'API REST que lorsque le suivi des billets par des tiers est activé.

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***Corde***

Résolution de la détection ou du ticket associé à la détection.

Les valeurs suivantes sont valides :

- `action_taken`
- `no_action_taken`

`participants:` ***Tableau d'objets***

Liste des appareils et des applications associés à la détection. Vous pouvez modifier des champs spécifiques pour un participant, mais vous ne pouvez pas ajouter de nouveaux participants à une détection.

`id:` ***Numéro***

L'identifiant du participant associé à la détection.

`usernames:` ***Tableau de cordes***

Les noms d'utilisateur associés au participant via l'API REST.

`origins:` ***Tableau de cordes***

Les adresses IP d'origine associées au participant via l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assignee": "string",
    "participants": {
        "id": 0,
        "usernames": [],
        "origins": []
    },
    "resolution": "string",
    "status": "string",
    "ticket_id": "string"
}
```

`PATCH /detections/tickets`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les valeurs des tickets de détection à mettre à jour.

`ticket_id:` ***Corde***

L'ID du ticket associé à la détection.

`assignee:` ***Corde***

L'assigné du ticket associé à la détection.

`status:` ***Corde***

État du ticket associé à la détection.

Les valeurs suivantes sont valides :

- `new`
- `in_progress`
- `closed`
- `acknowledged`

`resolution:` ***Corde***

Résolution du ticket associé à la détection.

Les valeurs suivantes sont valides :

- `action_taken`
- `no_action_taken`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assignee": "string",
    "resolution": "string",
    "status": "string",
    "ticket_id": "string"
}
```

`GET /detections/{id}/related`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'ID de la détection pour laquelle récupérer les détections associées.

`from:` ***Numéro***

Renvoie les détections survenues après la date spécifiée, exprimée en millisecondes depuis l'époque. Les détections qui ont débuté avant la date spécifiée sont renvoyées si la détection était en cours à ce moment-là.

`until:` ***Numéro***

Renvoie les détections qui se sont terminées avant la date spécifiée, exprimée en millisecondes depuis l'époque.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "create_time": 0,
    "description": "string",
    "end_time": 0,
```

```
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0,
    "url": "string"
}
```


`GET /detections/{id}/investigations`

Spécifiez les paramètres suivants.

`id`: ***Numéro***

L'ID de la détection pour laquelle récupérer les enquêtes associées.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.


```
{
    "appliance_id": 0,
    "assignee": "string",
    "categories": [
        "string"
    ],
    "create_time": 0,
    "description": "string",
    "end_time": 0,
    "id": 0,
    "is_user_created": true,
    "mitre_tactics": [],
    "mitre_techniques": [],
    "mod_time": 0,
    "participants": [],
    "properties": {},
    "recommended": true,
    "recommended_factors": [],
    "resolution": "string",
    "risk_score": 0,
    "start_time": 0,
    "status": "string",
    "ticket_id": "string",
    "ticket_url": "string",
    "title": "string",
    "type": "string",
    "update_time": 0,
    "url": "string"
}
```

`GET /detections/formats`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "categories": [],
    "display_name": "string",
    "is_user_created": true,
    "last_updated": 0,
    "mitre_categories": [],
    "properties": {},
    "released": 0,
    "status": "string",
    "type": "string"
}
```

`GET /detections/formats/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant de chaîne du format de détection.

`built_in_only:` ***Booléen***

(Facultatif) Si ce champ est vrai, renvoie uniquement les formats de détection intégrés. Si ce champ est faux et qu'un format personnalisé et un format intégré ont le même ID, renvoie le format personnalisé. La valeur par défaut est False.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "categories": [],
    "display_name": "string",
    "is_user_created": true,
    "last_updated": 0,
    "mitre_categories": [],
    "properties": {},
    "released": 0,
    "status": "string",
    "type": "string"
}
```

`POST /detections/formats`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres du format de détection.

`type:` ***Corde***

Identifiant de chaîne pour le type de détection. La chaîne ne peut contenir que des lettres, des chiffres et des traits de soulignement. Bien que les types de détection soient uniques dans tous les formats intégrés et que les types de détection soient uniques dans tous les formats personnalisés, un format intégré et un format personnalisé peuvent partager le même type de détection.

`display_name:` ***Corde***

Nom d'affichage du type de détection qui apparaît sur la page Détections du système ExtraHop.

`mitre_categories:` ***Tableau de cordes***

(Facultatif) Les identifiants des techniques MITRE associées à la détection.

`author:` ***Corde***

(Facultatif) L'auteur du format de détection.

`categories:` ***Tableau de cordes***

(Facultatif) La liste des catégories auxquelles appartient la détection. Pour les opérations POST et PATCH, spécifiez une liste avec une seule chaîne. Vous ne pouvez pas spécifier plus d'une catégorie pour les formats de détection personnalisés. La catégorie « perf » ou « sec » est automatiquement ajoutée à tous les formats de détection.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "author": "string",
    "categories": [],
    "display_name": "string",
    "mitre_categories": [],
    "type": "string"
}
```

`DELETE /detections/formats/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant de chaîne du format de détection.

`PATCH /detections/formats/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant de chaîne du format de détection.

`body:` ***Objet***

Les paramètres du format de détection.

`GET /detections/rules/hiding`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "create_time": 0,
    "description": "string",
    "detection_type": "string",
    "detections_hidden": 0,
    "enabled": true,
    "expiration": 0,
    "hide_past_detections": true,
    "id": 0,
    "offender": {},
    "participants_hidden": 0,
```

```
    "properties": [],
    "victim": {}
}
```

`GET /detections/rules/hiding/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la règle de réglage.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "create_time": 0,
    "description": "string",
    "detection_type": "string",
    "detections_hidden": 0,
    "enabled": true,
    "expiration": 0,
    "hide_past_detections": true,
    "id": 0,
    "offender": {},
    "participants_hidden": 0,
    "properties": [],
    "victim": {}
}
```

`POST /detections/rules/hiding`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de la règle de réglage.

`offender:` ***Objet***

Le délinquant auquel s'applique cette règle de réglage. Spécifiez un objet detection_hiding_participant pour appliquer la règle à une victime spécifique, ou spécifiez « Any » pour appliquer la règle à n'importe quel délinquant.

`object_type:` ***Corde***

Le type de participant.

Les valeurs suivantes sont valides :

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `hostname`
- `scanner_service`
- `username`

`object_id:` ***Numéro***

L'ID de l'équipement, du groupe dcesséquipements ou de la localité du réseau. Cette option n'est valide que si le type d'objet est « équipement », « device_group » ou « network_locality ».

`object_value:` ***Tableau ou chaîne***

L'adresse IP ou le bloc CIDR du participant. Vous pouvez spécifier une adresse ou un bloc unique dans une chaîne ou plusieurs adresses ou blocs dans un tableau. Cette option n'est valide que si l'object_type est « ipaddr ».

`object_locality:` ***Corde***

Type de localité du réseau du participant. Spécifiez « externe » ou « interne ». Cette option n'est valide que si l'object_type est « locality_type ».

Les valeurs suivantes sont valides :

- `internal`
- `external`

`object_scanner:` ***Tableau ou chaîne***

Le nom d'un service de numérisation externe. Vous pouvez spécifier un seul service dans une chaîne ou plusieurs valeurs dans un tableau. Vous pouvez également spécifier « N'importe lequel » pour sélectionner n'importe quel service de numérisation. Cette option n'est valide que si l'object_type est « scanner_service ».

`object_hostname:` ***Tableau ou chaîne***

Le nom d'hôte d'un participant. Vous pouvez spécifier un nom d'hôte unique dans une chaîne ou plusieurs noms d'hôte dans un tableau. Cette option n'est valide que si l'object_type est « hostname ».

`object_username:` ***Tableau ou chaîne***

Le nom d'utilisateur d'un participant. Vous pouvez spécifier un nom d'utilisateur unique dans une chaîne ou plusieurs noms d'utilisateur dans un tableau. Cette option n'est valide que si le type d'objet est « nom d'utilisateur ».

`victim:` ***Objet***

La victime à laquelle s'applique cette règle de réglage. Spécifiez un objet detection_hiding_participant pour appliquer la règle à une victime spécifique, ou spécifiez « Any » pour appliquer la règle à n'importe quelle victime.

`object_type:` ***Corde***

Le type de participant.

Les valeurs suivantes sont valides :

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `hostname`
- `scanner_service`
- `username`

`object_id:` ***Numéro***

L'ID de l'équipement, du groupe dcesséquipements ou de la localité du réseau. Cette option n'est valide que si le type d'objet est « équipement », « device_group » ou « network_locality ».

`object_value:` ***Tableau ou chaîne***

L'adresse IP ou le bloc CIDR du participant. Vous pouvez spécifier une adresse ou un bloc unique dans une chaîne ou plusieurs adresses ou blocs dans un tableau. Cette option n'est valide que si l'object_type est « ipaddr ».

`object_locality:` ***Corde***

Type de localité du réseau du participant. Spécifiez « externe » ou « interne ». Cette option n'est valide que si l'object_type est « locality_type ».

Les valeurs suivantes sont valides :

- `internal`
- `external`

`object_scanner:` ***Tableau ou chaîne***

Le nom d'un service de numérisation externe. Vous pouvez spécifier un seul service dans une chaîne ou plusieurs valeurs dans un tableau. Vous pouvez également spécifier « N'importe lequel » pour sélectionner n'importe quel service de numérisation. Cette option n'est valide que si l'object_type est « scanner_service ».

`object_hostname:` ***Tableau ou chaîne***

Le nom d'hôte d'un participant. Vous pouvez spécifier un nom d'hôte unique dans une chaîne ou plusieurs noms d'hôte dans un tableau. Cette option n'est valide que si l'object_type est « hostname ».

`object_username:` ***Tableau ou chaîne***

Le nom d'utilisateur d'un participant. Vous pouvez spécifier un nom d'utilisateur unique dans une chaîne ou plusieurs noms d'utilisateur dans un tableau. Cette option n'est valide que si le type d'objet est « nom d'utilisateur ».

`expiration:` ***Numéro***

Heure d'expiration de la règle de réglage, exprimée en millisecondes depuis l'époque. Une valeur nulle ou 0 indique que la règle n'expire pas.

`description:` ***Corde***

(Facultatif) Description de la règle de réglage.

`detection_type:` ***Corde***

Type de détection auquel s'applique cette règle de réglage. Affichez la liste des champs valides pour « type » en exécutant l'opération GET /detections/formats. Spécifiez « all_performance » ou « all_security » pour appliquer la règle à toutes les performances ou à toutes les détections de sécurité.

`properties:` ***Tableau d'objets***

(Facultatif) Les critères de filtre pour les propriétés de détection.

`property:` ***Corde***

Le nom de la propriété à filtrer.

`operator:` ***Corde***

Méthode de comparaison appliquée lors de la mise en correspondance de la valeur de l'opérande avec la valeur de la propriété de détection.

Les valeurs suivantes sont valides :

- `=`
- `!=`
- `~`
- `!~`
- `in`

`operand:` ***Chaîne, numéro ou objet***

La valeur que le filtre tente de faire correspondre. Le filtre compare la valeur de l'opérande à la valeur de la propriété de détection et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier l'opérande sous la forme d'une chaîne, d'un entier ou d'un objet. Pour plus d'informations, consultez Guide de l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "detection_type": "string",
    "expiration": 0,
    "offender": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array",
        "object_hostname": "array",
        "object_username": "array"
    },
    "properties": {
        "property": "string",
        "operator": "string",
        "operand": "string"
    },
    "victim": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array",
        "object_hostname": "array",
        "object_username": "array"
    }
}
```

`PATCH /detections/rules/hiding/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la règle de réglage.

`body:` ***Objet***

Les champs des règles de réglage à mettre à jour.

`enabled:` ***Booléen***

Indique si la règle de réglage est activée.

`expiration:` ***Numéro***

Heure d'expiration de la règle de réglage, exprimée en millisecondes depuis l'époque. Une valeur nulle ou 0 indique que la règle n'expire pas.

`description:` ***Corde***

Description de la règle de réglage.

`offender:` ***Objet***

Le délinquant auquel s'applique cette règle de réglage. Spécifiez un objet detection_hiding_participant pour appliquer la règle à une victime spécifique, ou spécifiez « Any » pour appliquer la règle à n'importe quel délinquant.

`object_type:` ***Corde***

Le type de participant.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

- `ipaddr`
- `locality_type`
- `network_locality`
- `hostname`
- `scanner_service`
- `username`

`object_id:` ***Numéro***

L'ID de l'équipement, du groupe dcesséquipements ou de la localité du réseau. Cette option n'est valide que si le type d'objet est « équipement », « device_group » ou « network_locality ».

`object_value:` ***Tableau ou chaîne***

L'adresse IP ou le bloc CIDR du participant. Vous pouvez spécifier une adresse ou un bloc unique dans une chaîne ou plusieurs adresses ou blocs dans un tableau. Cette option n'est valide que si l'object_type est « ipaddr ».

`object_locality:` ***Corde***

Type de localité du réseau du participant. Spécifiez « externe » ou « interne ». Cette option n'est valide que si l'object_type est « locality_type ».

Les valeurs suivantes sont valides :

- `internal`
- `external`

`object_scanner:` ***Tableau ou chaîne***

Le nom d'un service de numérisation externe. Vous pouvez spécifier un seul service dans une chaîne ou plusieurs valeurs dans un tableau. Vous pouvez également spécifier « N'importe lequel » pour sélectionner n'importe quel service de numérisation. Cette option n'est valide que si l'object_type est « scanner_service ».

`object_hostname:` ***Tableau ou chaîne***

Le nom d'hôte d'un participant. Vous pouvez spécifier un nom d'hôte unique dans une chaîne ou plusieurs noms d'hôte dans un tableau. Cette option n'est valide que si l'object_type est « hostname ».

`object_username:` ***Tableau ou chaîne***

Le nom d'utilisateur d'un participant. Vous pouvez spécifier un nom d'utilisateur unique dans une chaîne ou plusieurs noms d'utilisateur dans un tableau. Cette option n'est valide que si le type d'objet est « nom d'utilisateur ».

`victim:` ***Objet***

La victime à laquelle s'applique cette règle de réglage. Spécifiez un objet detection_hiding_participant pour appliquer la règle à une victime spécifique, ou spécifiez « Any » pour appliquer la règle à n'importe quelle victime.

`object_type:` ***Corde***

Le type de participant.

Les valeurs suivantes sont valides :

- `device`
- `device_group`
- `ipaddr`
- `locality_type`
- `network_locality`
- `hostname`
- `scanner_service`
- `username`

`object_id:` ***Numéro***

L'ID de l'équipement, du groupe dcesséquipements ou de la localité du réseau. Cette option n'est valide que si le type d'objet est « équipement », « device_group » ou « network_locality ».

`object_value:` ***Tableau ou chaîne***

L'adresse IP ou le bloc CIDR du participant. Vous pouvez spécifier une adresse ou un bloc unique dans une chaîne ou plusieurs adresses ou blocs dans un tableau. Cette option n'est valide que si l'object_type est « ipaddr ».

`object_locality:` ***Corde***

Type de localité du réseau du participant. Spécifiez « externe » ou « interne ». Cette option n'est valide que si l'object_type est « locality_type ».

Les valeurs suivantes sont valides :

- `internal`
- `external`

`object_scanner:` ***Tableau ou chaîne***

Le nom d'un service de numérisation externe. Vous pouvez spécifier un seul service dans une chaîne ou plusieurs valeurs dans un tableau. Vous pouvez également spécifier « N'importe lequel » pour sélectionner n'importe quel service de numérisation. Cette option n'est valide que si l'object_type est « scanner_service ».

`object_hostname:` ***Tableau ou chaîne***

Le nom d'hôte d'un participant. Vous pouvez spécifier un nom d'hôte unique dans une chaîne ou plusieurs noms d'hôte dans un tableau. Cette option n'est valide que si l'object_type est « hostname ».

`object_username:` ***Tableau ou chaîne***

Le nom d'utilisateur d'un participant. Vous pouvez spécifier un nom d'utilisateur unique dans une chaîne ou plusieurs noms d'utilisateur dans un tableau. Cette option n'est valide que si le type d'objet est « nom d'utilisateur ».

`properties:` ***Tableau d'objets***

Critères de filtre pour les propriétés de détection.

`property:` ***Corde***

Le nom de la propriété à filtrer.

`operator:` ***Corde***

Méthode de comparaison appliquée lors de la mise en correspondance de la valeur de l'opérande avec la valeur de la propriété de détection.

Les valeurs suivantes sont valides :

- `=`
- `!=`
- `~`
- `!~`
- `in`

`operand:` ***Chaîne, numéro ou objet***

La valeur que le filtre tente de faire correspondre. Le filtre compare la valeur de l'opérande à la valeur de la propriété de détection et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier l'opérande sous la forme d'une chaîne, d'un entier ou d'un objet. Pour plus d'informations, consultez Guide de l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "enabled": true,
    "expiration": 0,
    "offender": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array",
        "object_hostname": "array",
        "object_username": "array"
    },
    "properties": {
        "property": "string",
        "operator": "string",
        "operand": "string"
    },
    "victim": {
        "object_type": "string",
        "object_id": 0,
        "object_value": "array",
        "object_locality": "string",
        "object_scanner": "array",
        "object_hostname": "array",
        "object_username": "array"
    }
}
```

`DELETE /detections/rules/hiding/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la règle de réglage.

`GET /detections/{id}/notes`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique pour la détection.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "author": "string",
    "note": "string",
    "update_time": 0
}
```

`DELETE /detections/{id}/notes`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique pour la détection.

`PUT /detections/{id}/notes`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique pour la détection.

`body:` ***Objet***

Les paramètres de la note de détection.

Valeurs d'opérande pour les règles de réglage des propriétés de détection

Le `POST /detections/rules/hiding` cette opération vous permet de créer des règles de réglage qui filtrent les détections en fonction des propriétés de détection. Vous pouvez définir des critères de filtrage pour les propriétés de détection des objets. Chaque objet doit contenir une valeur unique pour `operand` champ valide pour le champ spécifié `property` valeur.

Conseil: Vous pouvez récupérer des valeurs de propriété valides via le `GET /detections/formats` opération. Découvrez les clés du `properties` objet dans la réponse. Dans l'exemple suivant , `property` la valeur est `s3_bucket`:

```
    "properties": {
      "s3_bucket": {
        "is_optional": true,
        "status": "active",
        "is_tunable": true,
        "data_type": "string"
      }
    }
```

Le `is_tunable` un champ indique si vous pouvez créer une règle de réglage basée sur la propriété.

`registered_domain_name`

Pour masquer les règles en fonction d'un nom de domaine enregistré, spécifiez le `property` valeur en tant que `registered_domain_name` et le `operand` valeur en tant que nom de domaine.

L'exemple de règle suivant masque les détections de tunnels DNS pour `example.com`.

```
{
    "detection_type": "dns_tunnel",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "example.com",
            "operator": "=",
            "property": "registered_domain_name"
        }
    ]
}
```

`uris`

Pour masquer les règles par un URI, spécifiez `property` valeur en tant que `uris` et le `operand` valeur sous forme d'URI.

L'exemple de règle suivant masque les détections d'attaques par injection SQL (SQLi) pour `http://example.com/test`.

```
{
    "detection_type": "sqli_attack",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "http://example.com/test",
            "operator": "=",
            "property": "uris"
        }
      ]
}
```

`top_level_domain`

Pour masquer les règles en fonction d'un nom de domaine de premier niveau, spécifiez le `property` valeur en tant que `top_level_domain` et le `operand` valeur en tant que nom de domaine de premier niveau.

L'exemple de règle suivant masque les détections de domaines de premier niveau suspects pour `org` domaine de premier niveau.

```
{
    "detection_type": "suspicious_tld",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": "org",
            "operator": "=",
            "property": "top_level_domain"
        }
    ]
}
```

Recherche avec des expressions régulières (regex)

Pour certain `property` valeurs, la chaîne peut être en syntaxe regex. Spécifiez le `operand` valeur en tant qu'objet doté d'un `value` paramètre avec la syntaxe regex que vous souhaitez associer et un `is_regex` paramètre défini sur `true`. La règle suivante filtre les détections dans les tunnels DNS dont les noms de domaine se terminent par `example.com`.

```
{
    "detection_type": "dns_tunnel",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": {
                "value": ".*?example.com",
                "is_regex": true
            },
            "operator": "=",
            "property": "registered_domain_name"
        }
    ]
```

```
}
```

Désactiver la distinction majuscules

Par défaut, recherche une chaîne `property` les valeurs distinguent les majuscules et minuscules. Toutefois, vous pouvez désactiver la distinction majuscules/minuscules en spécifiant la valeur de l'opérande sous la forme d'un objet doté d'un `case_sensitive` paramètre défini sur `false`.

La règle suivante masque les détections d'accès au domaine de l'outil de piratage avec l'outil de piratage ArchStrike.

```
{
    "detection_type": "hacking_tools",
    "expiration": null,
    "offender": "Any",
    "victim": "Any",
    "properties": [
        {
            "operand": {
                "value": "archstrike",
                "case_sensitive": false
            },
            "operator": "=",
            "property": "hacking_tool"
        }
    ]
}
```

Catégories de détection

Le champ des catégories est un tableau renvoyé dans les réponses pour `GET /detections` et `POST /detections/search` opérations. Le tableau suivant répertorie les entrées valides du tableau :

Valeur	Catégorie
`sec`	Sûreté
`sec.action`	Actions par rapport à l'objectif
`sec.attack`	Attaque
`sec.botnet`	botnet
`sec.caution`	Mise en garde
`sec.command`	Commandement et contrôle
`sec.cryptomining`	Cryptominage
`sec.dos`	Déni de service
`sec.exfil`	Exfiltration
`sec.exploit`	Exploitation
`sec.hardening`	Durcissement
`sec.lateral`	Mouvement latéral
`sec.ransomware`	Un ransomware
`sec.recon`	Reconnaissance
`perf`	Rendement

Valeur	Catégorie
`perf.auth`	Autorisation et contrôle d'accès
`perf.db`	Base de données
`perf.network`	Infrastructure réseau
`perf.service`	Dégradation du service
`perf.storage`	Rangement
`perf.virtual`	Virtualisation des ordinateurs de bureau et des applications
`perf.web`	Application Web

Groupe de messagerie

Vous pouvez ajouter des adresses e-mail individuelles ou de groupe à un groupe de messagerie et les attribuer à un système alerte. Lorsque cette alerte est déclenchée, le système envoie un e-mail à toutes les adresses du groupe de messagerie.

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

Fonctionnement	Descriptif
GET/emailgroups	Récupérez tous les groupes d'e-mails.
POST/groupes d'e-mails	Créez un nouveau groupe de messagerie.
SUPPRIMER /emailgroups/ {id}	Supprimez un groupe d'e-mails à l'aide d'un identifiant unique.
OBTENEZ /emailgroups/ {id}	Récupérez un groupe d'e-mails spécifique à l'aide d'un identifiant unique.
PATCH /emailgroups/ {id}	Appliquez les mises à jour à un groupe de messagerie spécifique.

Détails de l'opération

`GET /emailgroups`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "email_addresses": [],
    "group_name": "string",
    "id": 0,
    "system_notifications": true
}
```

`POST /emailgroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriétés spécifiées au nouveau groupe de messagerie.

`group_name:` ***Corde***

Nom convivial du groupe de messagerie.

`email_addresses:` ***Tableau de chaînes***

Liste des adresses e-mail du groupe de messagerie.

`system_notifications:` ***Booléen***

Indique si le groupe doit recevoir des notifications du système.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "email_addresses": [],
    "group_name": "string",
    "system_notifications": true
}
```

`GET /emailgroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe de messagerie.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "email_addresses": [],
    "group_name": "string",
    "id": 0,
    "system_notifications": true
}
```

`DELETE /emailgroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe de messagerie.

`PATCH /emailgroups/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour des valeurs de propriété spécifiées au groupe de messagerie.

`id:` ***Numéro***

Identifiant unique du groupe de messagerie.

Intervalles d'exclusion

Un intervalle d'exclusion peut être créé pour définir une période de suppression d'un alerte.

Par exemple, si vous ne souhaitez pas être informé des alertes en dehors des heures de bureau ou le week-end, un intervalle d' exclusion peut créer une règle pour supprimer l'alerte pendant cette période. Pour plus d' informations, voir Alertes.

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

Fonctionnement	Descriptif
GET /intervalles d'exclusion	Récupérez tous les intervalles d'exclusion.
Intervalles POST /exclusion	Créez un nouvel intervalle d'exclusion.
SUPPRIMER /exclusioninterval/{id}	Supprimez un intervalle d'exclusion spécifique.
OBTENEZ /exclusioninterval/{id}	Récupérez un intervalle d'exclusion spécifique.
PATCH /exclusionintervals/ {id}	Appliquez les mises à jour à un intervalle d'exclusion spécifique.

Détails de l'opération

`GET /exclusionintervals`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "id": 0,
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`POST /exclusionintervals`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Définissez les valeurs de propriétés spécifiées sur le nouvel intervalle d'exclusion.

`name:` ***Corde***

Nom convivial de l'intervalle d'exclusion.

`author:` ***Corde***

(Facultatif) Le nom du créateur de l'intervalle d'exclusion.

`description:` ***Corde***

(Facultatif) Description facultative de l'intervalle d'exclusion.

`interval_type:` ***Corde***

La fenêtre temporelle pendant laquelle l'intervalle d'exclusion a été évalué.

Les valeurs suivantes sont valides :

- `onetime`
- `weekly`
- `daily`

`start:` ***Numéro***

Début de la plage de temps de l'intervalle d'exclusion, exprimé en secondes. Cette valeur est relative à l'époque pour les exclusions ponctuelles, par rapport à minuit pour les exclusions quotidiennes et par rapport au lundi à minuit pour les exclusions hebdomadaires.

`end:` ***Numéro***

Fin de la plage de temps de l'intervalle d'exclusion, exprimée en secondes. Cette valeur est relative à l'époque pour les exclusions ponctuelles, par rapport à minuit pour les exclusions quotidiennes et par rapport au lundi à minuit pour les exclusions hebdomadaires.

`alert_apply_all:` ***Booléen***

Indique si cet intervalle d'exclusion doit être appliqué à toutes les alertes.

`trend_apply_all:` ***Booléen***

Indique si cet intervalle d'exclusion doit être appliqué à toutes les tendances.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "interval_type": "string",
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`GET /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de l'intervalle d'exclusion.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "id": 0,
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`DELETE /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de l'intervalle d'exclusion.

`PATCH /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour des valeurs de propriété spécifiées à l'intervalle d'exclusion.

`id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.

ExtraHop

Cette ressource fournit des métadonnées sur le système ExtraHop.

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

opération	Descriptif
GET /extrahop	Récupérez les métadonnées relatives au microprogramme exécuté sur le système ExtraHop.
Ressources POST /extrahop/cloud	Mettez à jour manuellement les ressources sur le système ExtraHop. Ces ressources sont automatiquement mises à jour lorsque le système est connecté à ExtraHop Cloud Services.
GET /extrahop/cluster	Récupérez les paramètres de configuration du cluster Explore.
PATCH /extrahop/cluster	Mettez à jour les paramètres de configuration du cluster Explore.
GET /extrahop/detections/access	Récupérez les paramètres de contrôle d'accès des détections.
PUT /extrahop/detections/access	Mettez à jour les paramètres de contrôle d'accès des détections.
GET /extrahop/edition	Récupérez l'édition du système ExtraHop. **Note:** Cette opération ne nécessite pas de clé API.
POST /extrahop/firmware	Téléchargez une nouvelle image du microprogramme sur le système ExtraHop. Pour plus d'informations, voir Mettre à jour le firmware ExtraHop via l'API REST.
POST /extrahop/firmware/download/url	Téléchargez une nouvelle image du microprogramme sur le système ExtraHop à partir d'une URL.
POST /extrahop/firmware/téléchargement/version	Téléchargez une nouvelle image du firmware sur le système ExtraHop depuis ExtraHop Cloud Services.
POST /extrahop/firmware/dernière/mise à niveau	Mettez à niveau le système ExtraHop vers la dernière image de firmware téléchargée.
GET /extrahop/firmware/next	Mettez à niveau le système ExtraHop vers la dernière image de firmware téléchargée.
GET /extrahop/firmware/previous	Récupérez les informations relatives à la version du microprogramme vers laquelle vous pouvez restaurer le système ExtraHop.
POST /extrahop/firmware/précédent/rollback	Restaurez la version précédente du microprogramme du système ExtraHop.
GET /extrahop/flowlogs/secret	Récupérez le secret du journal de flux.

opération	Descriptif
POST /extrahop/flowlogs/secret	Générez un nouveau secret de journal de flux.
GET /extrahop/idrac	Récupérez l'adresse IP iDRAC du système ExtraHop.
GET /extrahop/platform	Récupérez le nom de plate-forme du système ExtraHop. **Note:** Cette opération ne nécessite pas de clé API.
GET /extrahop/processes	Récupérez la liste des processus en cours d'exécution sur le système ExtraHop.
POST /extrahop/processes/ {process} /restart	Redémarrez un processus en cours d'exécution sur le système ExtraHop.
GET /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.
POST /extrahop/shutdown	Arrêtez le système ExtraHop.
POST/extrahop/sslcert	Régénérez le certificat TLS sur le système ExtraHop. Pour plus d'informations, voir Créez un certificat TLS fiable via l'API REST
PUT /extrahop/sslcert	Remplacez le certificat TLS sur le système ExtraHop.
POST /extrahop/sslcert/demande de signature	Créez une demande de signature de certificat TLS. Pour plus d'informations, voir Créez un certificat TLS fiable via l'API REST.
GET /extrahop/billetterie	Récupérez l'état de l'intégration de la billetterie.
PATCH /extrahop/billetterie	Activez ou désactivez l'intégration de la billetterie.
GET /extrahop/version	Récupérez la version du microprogramme qui s'exécute sur le système ExtraHop. **Note:** Cette opération ne nécessite pas de clé API.

Détails de l'opération

`GET /extrahop/version`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "version": "string"
}
```

`GET /extrahop/platform`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "platform": "string"
}
```

`GET /extrahop/edition`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "edition": "string"
}
```

`GET /extrahop`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "display_host": "string",
    "external_hostname": "string",
    "hostname": "string",
    "mgmt_ipaddr": "string",
    "platform": "string",
    "version": "string"
}
```

`GET /extrahop/idrac`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "ipaddr": "string"
}
```

`POST /extrahop/sslcert`

Il n'existe aucun paramètre pour cette opération.

`PUT /extrahop/sslcert`

Spécifiez les paramètres suivants.

`body`: ***Corde***
Le certificat SSL et éventuellement la clé privée. Entrez en texte brut, séparé par un saut de ligne.

`POST /extrahop/sslcert/signingrequest`

Spécifiez les paramètres suivants.

`body`: ***Objet***
Paramètres de la demande de signature de certificat SSL.

`subject_alternative_names:` ***Tableau d'objets***

Liste des noms auxquels le certificat s'applique, tels que {"type » : « dns », « name » : « www.example.com"}.

`type:` ***Corde***

Type de sujet Nom alternatif.

Les valeurs suivantes sont valides :

- `dns`
- `ip`

`name:` ***Corde***

Nom du sujet Nom alternatif.

`subject:` ***Objet***

L'objet du certificat SSL. Pour consulter la liste des sujets du certificat, voir ci-dessous.

`common_name:` ***Corde***

Le nom commun du sujet (CN).

`country_code:` ***Corde***

(Facultatif) Le pays concerné (C).

`state_or_province_name:` ***Corde***

(Facultatif) L'État ou la province concernés (ST).

`locality_name:` ***Corde***

(Facultatif) La localité concernée (L).

`organization_name:` ***Corde***

(Facultatif) L'organisation concernée (O).

`organizational_unit_name:` ***Corde***

(Facultatif) L'unité organisationnelle (OU) concernée.

`email_address:` ***Corde***

(Facultatif) L'adresse e-mail objet (EmailAddress).

Spécifiez le paramètre body au format JSON suivant.

```
{
    "subject": {
        "common_name": "string",
        "country_code": "string",
        "state_or_province_name": "string",
        "locality_name": "string",
        "organization_name": "string",
        "organizational_unit_name": "string",
        "email_address": "string"
    },
    "subject_alternative_names": {
        "type": "string",
        "name": "string"
    }
}
```

`GET /extrahop/ticketing`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
```

```
    "enabled": true,
    "external_ticketing_enabled": true,
    "internal_ticketing_enabled": true,
    "url_template": "string"
}
```

`PATCH /extrahop/ticketing`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Paramètres de suivi des tickets.

`enabled:` ***Booléen***

(Facultatif) Obsolète. Remplacé par les champs external_ticketing_enabled et internal_ticketing_enabled.

`external_ticketing_enabled:` ***Booléen***

(Facultatif) Indique si les détections sont suivies à partir d'un système de billetterie externe. Ce champ est obligatoire si le champ internal_ticketing_enabled est spécifié.

`internal_ticketing_enabled:` ***Booléen***

(Facultatif) Indique si les détections sont suivies depuis le système ExtraHop. Ce champ est obligatoire si le champ external_ticketing_enabled est spécifié.

`url_template:` ***Corde***

(Facultatif) Modèle d'URL qui relie les détections à des tickets externes. Le modèle doit inclure la variable $ticket_id. Ce champ s'applique uniquement si les détections sont suivies à partir d'un système de billetterie externe.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "enabled": true,
    "external_ticketing_enabled": true,
    "internal_ticketing_enabled": true,
    "url_template": "string"
}
```

`PUT /extrahop/detections/access`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres d'accès aux détections pour l'appliance.

`enabled:` ***Booléen***

Indique si les paramètres d'accès aux détections sont activés. Lorsque cette option est activée, les administrateurs peuvent restreindre l'accès aux détections à des utilisateurs spécifiques. Vous ne pouvez pas désactiver les paramètres d'accès aux détections une fois ceux-ci activés.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "enabled": true
}
```

`GET /extrahop/detections/access`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "enabled": true
}
```

`POST /extrahop/firmware`

Spécifiez les paramètres suivants.

`firmware:` ***Nom de fichier***

Le fichier .tar qui contient l'image du microprogramme. Remarque : Vous ne pouvez pas télécharger d'image de microprogramme via l'explorateur d'API REST. Pour plus d'informations sur la façon de télécharger une image via cURL ou un script Python, voir Mettre à niveau le firmware ExtraHop via l'API REST.

`POST /extrahop/firmware/latest/upgrade`

Spécifiez les paramètres suivants.

`body:` ***Objet***

(Facultatif) Les options d'installation pour la mise à niveau de l'appliance.

`restart_after:` ***Booléen***

(Facultatif) Indique s'il faut redémarrer l'appliance une fois la mise à niveau terminée.

`silent:` ***Booléen***

(Facultatif) Spécifie s'il faut désactiver l'interface utilisateur Web ExtraHop pendant le processus de mise à niveau. En cas d'échec d'une mise à niveau, l'appliance revient automatiquement à la version précédente du microprogramme.

`force:` ***Booléen***

(Facultatif) Spécifie s'il faut ignorer la vérification de compatibilité. Ignorez la vérification uniquement si le support ExtraHop a examiné et approuvé la mise à niveau.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "force": true,
    "restart_after": true,
    "silent": true
}
```

`POST /extrahop/firmware/download/url`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les options de téléchargement.

`firmware_url:` ***Corde***

URL du microprogramme à télécharger. Les schémas HTTPS, HTTP et FTP sont pris en charge.

`upgrade:` ***Booléen***

(Facultatif) Spécifie s'il faut mettre à niveau l'appliance une fois le téléchargement du microprogramme terminé.

`force:` ***Booléen***

(Facultatif) Spécifie s'il faut ignorer la vérification de compatibilité. Ignorez la vérification uniquement si le support ExtraHop a examiné et approuvé la mise à niveau.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "firmware_url": "string",
    "force": true,
    "upgrade": true
}
```

`POST /extrahop/restart`

Il n'existe aucun paramètre pour cette opération.

`POST /extrahop/shutdown`

Il n'existe aucun paramètre pour cette opération.

`GET /extrahop/services`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "admin": {
        "enabled": true
    },
    "keyreceiver": {
        "enabled": true
    },
    "snmp": {
        "enabled": true
    },
    "ssh": {
        "enabled": true
    }
}
```

`PATCH /extrahop/services`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres des services.

`admin:` ***Objet***

(Facultatif) Les paramètres du service d'interface graphique de gestion, qui fournit un accès à l'appliance via un navigateur.

`enabled:` ***Booléen***

Indique si le service est activé.

`snmp:` ***Objet***

(Facultatif) Les paramètres du service SNMP, qui permettent à votre logiciel de surveillance des équipements réseau de collecter des informations à partir du système ExtraHop.

`enabled:` ***Booléen***

Indique si le service est activé.

`ssh:` ***Objet***

(Facultatif) Les paramètres du service SSH, qui permettent aux utilisateurs de se connecter en toute sécurité à l'interface de ligne de commande (CLI) ExtraHop.

`enabled:` ***Booléen***

Indique si le service est activé.

`keyreceiver:` ***Objet***

(Facultatif) Les paramètres du récepteur de clés de session SSL, qui permettent à l'appliance de recevoir et de déchiffrer les clés de session depuis le redirecteur de clés de session.

`enabled:` ***Booléen***

Indique si le service est activé.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "admin": {
        "enabled": true
    },
    "keyreceiver": {
        "enabled": true
    },
    "snmp": {
        "enabled": true
    },
    "ssh": {
        "enabled": true
    }
}
```

`GET /extrahop/processes`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "can_restart": true,
    "cpu": 0.0,
    "cpu_time": 0,
    "mem_percent": 0.0,
    "mem_res": 0,
    "mem_virt": 0,
    "process": "string",
    "start_time": 0
}
```

`POST /extrahop/processes/{process}/restart`

Spécifiez les paramètres suivants.

`process:` ***Corde***

Le nom du processus.

Les valeurs suivantes sont valides :

- `exadmin`
- `exalerts`
- `examf`
- `exapi`
- `exbridge`
- `excap`
- `exconfig`

- exflowlogs
- expktfeeder
- exsnmpq
- exnotify
- exportal
- exremote
- exsearch
- exstatmirror
- extrend
- webserver
- hopcloud-api

`GET /extrahop/cluster`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "ingest_enabled": true,
    "replication_policy": 0
}
```

`PATCH /extrahop/cluster`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de configuration du cluster EXA.

`ingest_enabled:` ***Booléen***

(Facultatif) Indique si l'ingestion d'enregistrements est activée pour le cluster Explore.

`replication_policy:` ***Numéro***

(Facultatif) Le niveau de réplication qui détermine le nombre de copies de chaque enregistrement stockées.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "ingest_enabled": true,
    "replication_policy": 0
}
```

`GET /extrahop/firmware/previous`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "backup_time": 0,
    "version": "string"
}
```

`POST /extrahop/firmware/previous/rollback`

Il n'existe aucun paramètre pour cette opération.

`POST /extrahop/cloudresources`

Spécifiez les paramètres suivants.

`cloudresources:` ***Nom de fichier***
Le fichier du bundle de ressources.

`GET /extrahop/flowlogs/secret`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "secret": "string"
}
```

`POST /extrahop/flowlogs/secret`

Il n'existe aucun paramètre pour cette opération.

`GET /extrahop/firmware/next`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "current_release": true,
    "release": "string",
    "versions": []
}
```

`POST /extrahop/firmware/download/version`

Spécifiez les paramètres suivants.

`body:` ***Objet***
(Facultatif) Les options de téléchargement.
`version:` ***Corde***
Version du microprogramme à télécharger.
`upgrade:` ***Booléen***
(Facultatif) Spécifie s'il faut mettre à niveau l'appliance une fois le téléchargement du microprogramme terminé.

Spécifiez le paramètre body au format JSON suivant.

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

Enquêtes

Les enquêtes vous permettent d'ajouter et de visualiser plusieurs détections sur une seule chronologie et une seule carte. Pour plus d'informations, voir Enquêtes.

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

opération	Descriptif
GET /enquêtes	Récupérez toutes les enquêtes.
POST /enquêtes	Créez une investigation.
POST /enquêtes/recherche	Recherchez des enquêtes.
SUPPRIMER /investigations/ {id}	Supprimer une investigation spécifique.
GET /investigations/ {id}	Récupérez une investigation spécifique.
PATCH /investigations/ {id}	Mettez à jour une enquête.

Détails de l'opération

`GET /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique pour l'investigation.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "created_by": "string",
    "creation_time": 0,
    "description": "string",
    "detections": [
        "string"
    ],
    "end_time": 0,
    "id": 0,
    "investigation_types": [
        "string"
    ],
    "is_user_created": true,
    "last_interaction_by": "string",
    "name": "string",
    "notes": "string",
    "start_time": 0,
    "status": "string",
    "update_time": 0,
    "url": "string"
}
```

`GET /investigations`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "created_by": "string",
    "creation_time": 0,
    "description": "string",
    "detections": [
```

```
        "string"
    ],
    "end_time": 0,
    "id": 0,
    "investigation_types": [
        "string"
    ],
    "is_user_created": true,
    "last_interaction_by": "string",
    "name": "string",
    "notes": "string",
    "start_time": 0,
    "status": "string",
    "update_time": 0,
    "url": "string"
}
```

`POST /investigations/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de l'enquête.

`update_time:` ***Numéro***

Renvoie les recherches qui ont été mises à jour après la date spécifiée, exprimée en millisecondes depuis l'époque.

`creation_time:` ***Numéro***

Renvoie les enquêtes créées après la date spécifiée, exprimée en millisecondes depuis l'époque.

`is_user_created:` ***Booléen***

(Facultatif) Renvoie uniquement les enquêtes créées manuellement par un utilisateur.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "creation_time": 0,
    "is_user_created": true,
    "update_time": 0
}
```

`PATCH /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'ID de l'investigation à mettre à jour.

`body:` ***Objet***

Les champs d'investigation à mettre à jour.

`name:` ***Corde***

(Facultatif) Le nom de l'enquête.

`status:` ***Corde***

(Facultatif) L'état de l'enquête.

Les valeurs suivantes sont valides :

- `open`

- `in_progress`
- `closed`

`notes:` ***Corde***

(Facultatif) Remarques facultatives concernant l'enquête.

`event_ids:` ***Tableau de nombres***

(Facultatif) La liste des identifiants pour les détections dans le cadre de l'investigation. Si vous spécifiez ce champ, la nouvelle liste d'identifiants remplace la liste existante.

`assignee:` ***Corde***

(Facultatif) Le nom d'utilisateur de la personne chargée de l'enquête.

`assessment:` ***Corde***

(Facultatif) L'évaluation de l'enquête.

Les valeurs suivantes sont valides :

- `malicious_true_positive`
- `benign_true_positive`
- `false_positive`
- `undecided`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "event_ids": [],
    "name": "string",
    "notes": "string",
    "status": "string"
}
```

`POST /investigations`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les domaines de la nouvelle enquête.

`name:` ***Corde***

Le nom de l'enquête.

`status:` ***Corde***

(Facultatif) L'état de l'enquête.

Les valeurs suivantes sont valides :

- `open`
- `in_progress`
- `closed`

`notes:` ***Corde***

(Facultatif) Remarques facultatives concernant l'enquête.

`event_ids:` ***Tableau de nombres***

(Facultatif) La liste des identifiants pour les détections dans le cadre de l'investigation.

`assignee:` ***Corde***

(Facultatif) Le nom d'utilisateur de la personne chargée de l'enquête.

`assessment:` ***Corde***

(Facultatif) L'évaluation de l'enquête.

Les valeurs suivantes sont valides :

- `malicious_true_positive`
- `benign_true_positive`
- `false_positive`
- `undecided`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "event_ids": [],
    "name": "string",
    "notes": "string",
    "status": "string"
}
```

`DELETE /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'ID de l'investigation à supprimer.

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.

Détails de l'opération

`GET /jobs/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

L'identifiant unique de la tâche.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "details": "string",
    "id": "string",
```

```
    "remote_jobs": [],
    "status": "string",
    "step_description": "string",
    "step_number": 0,
    "total_steps": 0,
    "type": "string"
}
```

`GET /jobs`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "details": "string",
    "id": "string",
    "remote_jobs": [],
    "status": "string",
    "step_description": "string",
    "step_number": 0,
    "total_steps": 0,
    "type": "string"
}
```

Types d'emplois

Le `GET /jobs` l'opération renvoie les valeurs suivantes dans `type` champ de réponse.

téléchargement extrahop_firmware_download

Le système ExtraHop télécharge une nouvelle image du firmware à partir d'une URL ou des services cloud ExtraHop.

mise à niveau extrahop_firmware_

Le système ExtraHop est en cours de mise à niveau vers une nouvelle version du firmware.

extrahop_firmware_download_upgrade

Le système ExtraHop télécharge une image du microprogramme et effectue une mise à niveau vers une nouvelle version du micrologiciel. L'image est récupérée à partir d'une URL ou d'ExtraHop Cloud Services.

Note: Le `type` le champ est vide pour certaines tâches.

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.
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.

Fonctionnement	Descriptif
PUT/licence/clé de produit	Appliquez la clé de produit spécifiée au système ExtraHop et enregistrez la licence.

Détails de l'opération

`PUT /license`

Spécifiez les paramètres suivants.

`body:` ***Corde***

(Facultatif) Le texte de licence qui vous a été fourni par ExtraHop Support, y compris les lignes de début et de fin.

`GET /license`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "dossier": "string",
    "edition": "string",
    "expires_at": 0,
    "expires_in": 0,
    "modules": {},
    "options": {},
    "platform": "string",
    "product_key": "string",
    "serial": "string"
}
```

`PUT /license/productkey`

Spécifiez les paramètres suivants.

`body:` ***Objet***

(Facultatif) Appliquez la clé de produit spécifiée à l'appliance.

`GET /license/productkey`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "product_key": "string"
}
```

Métriques

Des informations métriques sont collectées sur chaque objet identifié par le système ExtraHop.

Notez que les métriques sont récupérées via la méthode POST, qui crée une requête pour collecter les informations demandées via l'API. Pour plus d'informations, voir Extraire des métriques via l'API REST.

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

opération	Descriptif
POST /métriques	Récupère les métriques pour chaque objet spécifié.
GET /metrics/next/ {xid}	Si vous demandez des statistiques à un console avec le `POST /metrics`, `POST /metrics/total`, ou `POST /metrics/totalbyobject` opération, et vous spécifiez des objets qui ont été observés par plusieurs capteurs, la réponse contient le `xid` champ, plutôt que des données métriques. Vous pouvez récupérer des données métriques en spécifiant `xid` champ dans le `GET /metrics/next/{xid}` opération, qui renvoie des métriques provenant de l'un des capteurs connectés à la console. Répéter le `GET /metrics/next/{xid}` opération pour renvoyer des métriques provenant de capteurs supplémentaires. Une fois toutes les métriques récupérées, l'opération renvoie la valeur null. Si les métriques ne sont pas encore disponibles à partir de la sonde, la chaîne `again` est renvoyé. Patientez quelques secondes, puis réessayez. **Note:** La réponse peut contenir un `xid` champ, même si vous n'avez demandé que des métriques concernant un seul groupe d'équipements, car les groupes d'équipements peuvent contenir des appareils provenant de plusieurs capteurs.
POST /métriques/total	Récupère les totaux métriques combinés pour tous les objets spécifiés.
POST /métriques/total par objet	Récupère les totaux métriques pour chaque objet spécifié.

Par exemple, le corps de requête suivant extrait les réponses HTTP envoyées par deux appareils au cours des 30 dernières minutes.

```
{
  "cycle": "auto",
  "from": -1800000,
  "metric_category": "http_server",
  "metric_specs": [
    {
      "name": "rsp"
    }
  ],
  "object_ids": [
    180, 177
  ],
  "object_type": "device",
  "until": 0
}
```

Pour `POST /metrics` opération, l'exemple de corps de requête précédent renvoie le nombre de réponses HTTP survenues au cours de chaque intervalle de temps, étiqueté avec l'heure de chaque événement et l'ID de l'équipement qui a envoyé les réponses, comme dans l'exemple de réponse suivant :


```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659320000,
  "from": 1709657520000,
  "until": 1709659320000,
  "stats": [
    {
      "oid": 177,
      "time": 1709657520000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 177,
      "time": 1709657550000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 180,
      "time": 1709657520000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 180,
      "time": 1709657550000,
      "duration": 30000,
      "values": [
        4
      ]
    }
  ]
}
```


Pour `POST /metrics/totalbyobject` opération, le même exemple de corps de requête précédent récupère le total combiné pour chaque équipement sur toute la période, comme dans l'exemple de réponse suivant :


```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659620000,
  "from": 1709657820000,
  "until": 1709659620000,
  "stats": [
    {
      "oid": 180,
      "time": 1709659620000,
      "duration": 1830000,
      "values": [
```

```
        8
      ]
    },
    {
      "oid": 177,
      "time": 1709659620000,
      "duration": 1830000,
      "values": [
        8
      ]
    }
  ]
}
```

Pour `POST /metrics/total` opération, le même exemple de corps de requête précédent récupère le total combiné des deux appareils sur toute la période, comme dans l'exemple de réponse suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659830000,
  "from": 1709658030000,
  "until": 1709659830000,
  "stats": [
    {
      "oid": -1,
      "time": 1709659830000,
      "duration": 1830000,
      "values": [
        16
      ]
    }
  ]
}
```

Notez que le comportement du `/metrics/total` et `/metrics/totalbyobject` les points de terminaison dépendent du type de métrique. Pour les mesures de comptage, le `values` Le champ contient la somme totale des valeurs sur l'intervalle de temps spécifié, comme indiqué dans l'exemple ci-dessus. Toutefois, pour les métriques des ensembles de données, le `values` Le champ contient une liste de valeurs et la fréquence à laquelle ces valeurs sont apparues. Par exemple, une requête concernant les temps de traitement du serveur avec le `POST /metrics/total` L'opération renvoie une réponse similaire à l'exemple suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1494541440000,
  "from": 1494539640000,
  "until": 1494541440000,
  "stats": [
    {
      "oid": -1,
      "time": 1494541380000,
      "duration": 1800000,
      "values": [
        [
          {
            "value": 2.271,
            "freq": 5
          },
          {
            "value": 48.903,
```

```
            "freq": 1
          }
        ]
      ]
    }
  ]
}
```

S'il existe plus de 1 000 valeurs d'ensemble de données distinctes au cours de la période spécifiée, les valeurs similaires sont consolidées pour réduire la réponse à 1 000 valeurs. Par exemple, s'il y a moins de 1 000 valeurs, la réponse peut contenir les entrées suivantes :

```
{
  "value": 2.571,
  "freq": 4
},
{
  "value": 2.912,
  "freq": 2
}
```

Toutefois, si la réponse contient plus de 1 000 valeurs, ces entrées peuvent être consolidées dans l'entrée suivante :

```
{
  "value": 2.571,
  "freq": 6
}
```

Si le `calc_type` Le champ est spécifié et la réponse contient plus de 1 000 valeurs, le percentile ou la moyenne est calculé en fonction de l'ensemble de données consolidé.

Détails de l'opération

`POST /metrics`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

L'horodateur de début de la demande. Renvoie uniquement les statistiques collectées après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`
- `1sec`
- `30sec`

- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent également être des expressions régulières délimitées par des barres obliques (« /GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
```

```
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`POST /metrics/total`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

L'horodateur de début de la demande. Renvoie uniquement les statistiques collectées après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /

devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent également être des expressions régulières délimitées par des barres obliques (« /GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`POST /metrics/totalbyobject`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

L'horodateur de début de la demande. Renvoie uniquement les statistiques collectées après cette période. Le temps est exprimé en millisecondes depuis l'époque. 0 indique l'heure de la demande. Une valeur négative est évaluée par rapport à l'heure actuelle. L'unité par défaut pour une valeur négative est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent

également être des expressions régulières délimitées par des barres obliques (« / GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`GET /metrics/next/{xid}`

Spécifiez les paramètres suivants.

`xid:` ***Numéro***

Identifiant unique renvoyé par une requête métrique.

Unités de temps prises en charge

Pour la plupart des paramètres, l'unité par défaut pour la mesure du temps est la milliseconde. Toutefois, les paramètres suivants renvoient ou acceptent des unités de temps alternatives telles que les minutes et les heures :

- Appareil
  - actif_depuis
  - actif_jusqu'à
- Groupe d'appareils
  - actif_depuis
  - actif_jusqu'à
- Métriques
  - à partir de

    - jusqu'à
- Journal d'enregistrement
    - à partir de
    - jusqu'à
    - context_ttl

Le tableau suivant indique les unités de temps prises en charge :

Unité de temps	Suffixe d'unité
Année	`y`
Mois	`M`
Semaine	`w`
Journée	`d`
Heure	`h`
Minutes	`m`
Deuxième	`s`
Milliseconde	`ms`

Pour spécifier une unité de temps autre que les millisecondes pour un paramètre, ajoutez le suffixe de l'unité à la valeur. Par exemple, pour demander des appareils actifs au cours des 30 dernières minutes, spécifiez la valeur de paramètre suivante :

```
GET /api/v1/devices?active_from=-30m
```

L'exemple suivant indique une recherche pour HTTP records créés il y a 1 à 2 heures :

```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Réseau

Les réseaux sont corrélés à la carte d'interface réseau qui reçoit les entrées de tous les objets identifiés par le système ExtraHop.

Sur un console, chaque sonde connectée est identifiée comme une capture réseau. Pour plus d'informations, voir Réseaux.

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

Opération	Descriptif
GET /réseaux	Récupérez tous les réseaux.
GET /networks/ {id}	Récupérez un réseau spécifique par identifiant.
PATCH /networks/ {id}	Mettez à jour un réseau spécifique par identifiant.
GET /networks/ {id} /alertes	Tout récupérer alertes qui sont affectés à un réseau spécifique.

Opération	Descriptif
POST /networks/ {id} /alertes	Attribuez et annulez les alertes à un réseau spécifique.
SUPPRIMER /networks/ {id} /alerts/ {child-id}	Annuler l'attribution d'une alerte à un réseau spécifique.
POST /networks/ {id} /alerts/ {child id}	Attribuez une alerte à un réseau spécifique.
GET /networks/ {id} /vlan	Récupérez tous les VLAN assignés à un réseau spécifique.

Détails de l'opération

`GET /networks`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
    "name": "string",
    "node_id": 0
}
```

`PATCH /networks/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Mises à jour de la valeur des propriétés à appliquer au réseau.

`id:` ***Numéro***
Identifiant unique du réseau.

`GET /networks/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
    "name": "string",
    "node_id": 0
}
```

`GET /networks/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

`direct_assignments_only:` ***Booléen***
(Facultatif) Limitez les résultats aux seules alertes directement attribuées au réseau.

`POST /networks/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Listes d'identifiants d'alerte à attribuer et/ou à annuler.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
Identifiant unique du réseau.

`POST /networks/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'alerte.

`id:` ***Numéro***
Identifiant unique du réseau.

`DELETE /networks/{id}/alerts/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'alerte.

`id:` ***Numéro***
Identifiant unique du réseau.

`GET /networks/{id}/vlans`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

Entrée de localité du réseau

Vous pouvez gérer une liste qui spécifie la localité réseau des adresses IP.

Par exemple, vous pouvez créer une entrée dans la liste des localités du réseau qui spécifie qu'une adresse IP ou un bloc CIDR est interne ou externe.

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

opération	Descriptif
GET/localités du réseau	Récupérez toutes les entrées de localité du réseau.
LOCALITÉS POST/réseau	Créez une entrée de localité réseau.
SUPPRIMER /networklocalities/ {id}	Supprimez une entrée de localité du réseau. **Note:** Cette opération n'est pas disponible sur les capteurs connectés à RevealX 360. Cependant, cette opération est disponible dans le API REST RevealX 360.
GET /networklocalities/ {id}	Récupérez une entrée de localité réseau spécifique.
PATCH /networklocalities/ {id}	Appliquez les mises à jour à une entrée de localité réseau spécifique. **Note:** Cette opération n'est pas disponible sur les capteurs connectés à RevealX 360. Cependant, cette opération est disponible dans le API REST RevealX 360.

Détails de l'opération

`GET /networklocalities`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "external": true,
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`POST /networklocalities`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées à la nouvelle entrée de localité du réseau.

`name:` ***Corde***

(Facultatif) Le nom de la localité du réseau. Si ce champ n'est pas spécifié, la localité du réseau est nommée au format suivant : « Locality_ID », où ID est l'identifiant unique de la localité du réseau.

`network:` ***Corde***

(Facultatif) Obsolète. Spécifiez les blocs CIDR ou les adresses IP dans le champ réseaux.

`networks:` ***Tableau de chaînes***

(Facultatif) Tableau de blocs CIDR ou d'adresses IP qui définissent la localité du réseau.

`external:` ***Booléen***

Indique si le réseau est interne ou externe.

`description:` ***Corde***

(Facultatif) Description facultative de l'entrée de localité du réseau.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "external": true,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`GET /networklocalities/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique pour l'entrée de localité du réseau.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "external": true,
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`DELETE /networklocalities/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique pour l'entrée de localité du réseau.

`PATCH /networklocalities/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les mises à jour des valeurs de propriété spécifiées à l'entrée de localité du réseau.

`network:` ***Corde***

(Facultatif) Obsolète. Spécifiez les blocs CIDR ou les adresses IP dans le champ réseaux.

`networks:` ***Tableau de chaînes***

(Facultatif) Tableau de blocs CIDR ou d'adresses IP qui définissent la localité du réseau.

`name:` ***Corde***

(Facultatif) Le nom de la localité du réseau.

`external:` ***Booléen***

(Facultatif) Indique si le réseau est interne ou externe.

`description:` ***Corde***

(Facultatif) Description facultative de l'entrée de localité du réseau.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "external": true,
    "name": "string",
    "network": "string",
    "networks": []
}
```

`id:` ***Numéro***

Identifiant unique pour l'entrée de localité du réseau.

Nœud

Un nœud est un sonde qui est connecté à un console.

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

Fonctionnement	Descriptif
GET /nœuds	Tout récupérer capteurs connecté à cela console.
OBTENEZ /nodes/ {id}	Récupérez un élément spécifique sonde qui est connecté à cela console.
PATCH /nodes/ {id}	Mettre à jour un élément spécifique sonde qui est connecté à cela console.

Détails de l'opération

`GET /nodes`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "add_time": 0,
    "display_name": "string",
    "enabled": true,
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_status": "string",
    "nickname": "string",
    "ntp_sync": true,
    "product_key": "string",
    "status_code": "string",
    "status_message": "string",
    "time_added": 0,
    "time_offset": 0,
```

```
    "uuid": "string"
}
```

`GET /nodes/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
ID de la sonde.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "add_time": 0,
    "display_name": "string",
    "enabled": true,
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_status": "string",
    "nickname": "string",
    "ntp_sync": true,
    "product_key": "string",
    "status_code": "string",
    "status_message": "string",
    "time_added": 0,
    "time_offset": 0,
    "uuid": "string"
}
```

`PATCH /nodes/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour spécifiées au nœud Discover.

`id:` ***Numéro***
Identifiant unique du nœud Discover.

Observations

Une observation associe l'adresse IP d'un équipement du système ExtraHop à une adresse IP extérieure à votre réseau. Par exemple, vous pouvez suivre l'activité d'un utilisateur VPN en associant l'adresse IP du client VPN sur votre réseau interne à l' adresse IP externe attribuée à l'utilisateur sur l'Internet public.

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

Fonctionnement	Descriptif
POST /observations/associatedipaddrs	Ajoutez une observation pour créer une association entre les adresses IP des équipements.

Détails de l'opération

`POST /observations/associatedipaddrs`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres d'observation.

`observations:` ***Tableau d'objets***

Une série d'observations.

`ipaddr:` ***Corde***

L'adresse IP de l'équipement observée par la sonde ou la console.

`associated_ipaddr:` ***Corde***

L'adresse IP associée.

`timestamp:` ***Numéro***

Heure à laquelle l'observation a été créée par la source, exprimée en millisecondes depuis l'époque.

`source:` ***Corde***

La source des observations.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "observations": {
        "ipaddr": "string",
        "associated_ipaddr": "string",
        "timestamp": 0
    },
    "source": "string"
}
```

Flux de données ouvert

Un flux de données ouvert (ODS) est un canal par lequel vous pouvez envoyer des données métriques spécifiées à partir d'un sonde vers un système tiers externe. Par exemple, vous souhaiterez peut-être stocker ou analyser des données métriques à l'aide d'un outil distant, tel que Splunk, MongoDB ou Amazon Web Services (AWS).

L'envoi de données via un flux de données ouvert est une procédure en deux étapes. Vous devez d'abord configurer une connexion au système cible qui recevra les données. Ensuite, vous écrivez un déclencheur qui indique les données à envoyer au système cible et à quel moment. Pour plus d'informations, voir Flux de données ouverts.

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

Fonctionnement	Descriptif
GET /odstargets	Récupérez toutes les cibles Open Data Stream.
OBTENEZ /odstargets/http	Récupérez toutes les cibles HTTP Open Data Stream.
POSTE/odstargets/http	Créez une nouvelle cible HTTP Open Data Stream.
SUPPRIMER /odstargets/http/ {name}	Supprimez une cible HTTP Open Data Stream.
OBTENEZ /odstargets/http/ {nom}	Récupérez une cible HTTP Open Data Stream spécifique.
OBTENEZ /odstargets/kafka	Récupérez toutes les cibles de Kafka Open Data Stream.
POSTER /odstargets/kafka	Créez une nouvelle cible Kafka Open Data Stream.

Fonctionnement	Descriptif
SUPPRIMER /odstargets/kafka/ {name}	Supprimez une cible Kafka Open Data Stream.
OBTENEZ /odstargets/kafka/ {nom}	Récupérez une cible spécifique de Kafka Open Data Stream.
OBTENEZ /odstargets/mongodb	Récupérez toutes les cibles de MongoDB Open Data Stream.
POSTE/odstargets/mongodb	Créez une nouvelle cible MongoDB Open Data Stream.
SUPPRIMER /odstargets/mongodb/ {name}	Supprimez une cible MongoDB Open Data Stream.
OBTENEZ /odstargets/mongodb/ {nom}	Récupérez une cible MongoDB Open Data Stream spécifique.
OBTENEZ /odstargets/raw	Récupérez toutes les cibles Raw Open Data Stream.
POST/odstargets/raw	Créez une nouvelle cible de flux de données ouvertes brutes.
SUPPRIMER /odstargets/raw/ {name}	Supprimez une cible de flux de données ouvertes brutes.
OBTENEZ /odstargets/raw/ {nom}	Récupérez une cible de flux de données ouvertes brutes spécifique.
OBTENEZ /odstargets/syslog	Récupérez toutes les cibles Syslog Open Data Stream.
POST /odstargets/syslog	Créez une nouvelle cible Syslog Open Data Stream.
SUPPRIMER /odstargets/syslog/ {nom}	Supprimez une cible Syslog Open Data Stream.
OBTENEZ /odstargets/syslog/ {nom}	Récupérez une cible Syslog Open Data Stream spécifique.

Détails de l'opération

`GET /odstargets`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/http`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/http/{name}`

Spécifiez les paramètres suivants.

`name` : ***Corde***

Le nom de la cible.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/kafka`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "brokers": [],
    "compression": "string",
    "name": "string",
    "partition_strategy": "string",
    "protocol": "string",
    "skip_cert_verification": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`GET /odstargets/kafka/{name}`

Spécifiez les paramètres suivants.

`name`: ***Corde***

Le nom de la cible.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "brokers": [],
    "compression": "string",
    "name": "string",
    "partition_strategy": "string",
    "protocol": "string",
    "skip_cert_verification": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`GET /odstargets/mongodb`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/mongodb/{name}`

Spécifiez les paramètres suivants.

`name`: ***Corde***

Le nom de la cible.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/raw`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/raw/{name}`

Spécifiez les paramètres suivants.

`name` : ***Corde***

Le nom de la cible.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{}
```

`GET /odstargets/syslog`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "batch_min_bytes": 0,
    "concurrent_connections": 0,
    "host": "string",
    "localtime": true,
    "name": "string",
    "port": 0,
    "protocol": "string",
    "skip_cert_verification": true,
    "tcp_length_prefix_framing": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`GET /odstargets/syslog/{name}`

Spécifiez les paramètres suivants.

`name` : ***Corde***

Le nom de la cible.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "batch_min_bytes": 0,
    "concurrent_connections": 0,
    "host": "string",
    "localtime": true,
    "name": "string",
    "port": 0,
    "protocol": "string",
    "skip_cert_verification": true,
    "tcp_length_prefix_framing": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`POST /odstargets/http`

Spécifiez les paramètres suivants.

`body:` ***Objet***

`name:` ***Corde***

Le nom de la cible.

`host:` ***Corde***

Le nom d'hôte ou l'adresse IP du serveur HTTP distant.

`port:` ***Numéro***

Numéro de port TCP du serveur HTTP.

`protocol:` ***Corde***

Le protocole de transmission des données.

Les valeurs suivantes sont valides :

- `http`
- `https`

`skip_cert_verification:` ***Booléen***

(Facultatif) Indique s'il faut contourner la vérification du certificat TLS pour les données chiffrées. Ce paramètre n'est valide que si le protocole est défini sur https.

`pipeline:` ***Booléen***

Indique si plusieurs connexions HTTP simultanées sont activées, ce qui peut améliorer la vitesse de débit.

`additional_header:` ***Corde***

(Facultatif) Spécifie un en-tête HTTP supplémentaire à inclure dans chaque demande. Les en-têtes doivent être spécifiés au format suivant : "<key>: <value>». Par exemple : « additional_header » : « Accept : text/html ».

`authentication:` ***Objet***

Objet contenant des identifiants d'authentification HTTP.

`auth_type:` ***Corde***

Type d'authentification HTTP.

Les valeurs suivantes sont valides :

- `none`
- `basic`
- `aws`
- `azure_storage`
- `azure_ad`
- `crowdstrike`

`username:` ***Corde***

(Facultatif) Le nom de l'utilisateur. Cette option est obligatoire si auth_type est défini sur basic ou si auth_type est défini sur azure_ad et grant_type est défini sur resource_owner.

`password:` ***Corde***

(Facultatif) Le mot de passe de l'utilisateur. Cette option est obligatoire si auth_type est défini sur basic ou si auth_type est défini sur azure_ad et grant_type est défini sur resource_owner.

`access_key:` ***Corde***

(Facultatif) L'ID de la clé d'accès. Cette option est requise pour l'authentification entre AWS et Azure Storage.

`secret_key:` ***Corde***

(Facultatif) La clé d'accès secrète. Cette option est requise pour l'authentification AWS.

`service:` ***Corde***

(Facultatif) Le code de service du service AWS, tel que « AmazonEC2 ». Cette option est requise pour l'authentification AWS.

`region:` ***Corde***

(Facultatif) Le nom de la région AWS, par exemple « us-west-1 ». Cette option est requise pour l'authentification AWS.

`grant_type:` ***Corde***

(Facultatif) Type d'autorisation OAuth 2.0. Cette option est requise pour l'authentification par identifiant Microsoft Entra.

Les valeurs suivantes sont valides :

- `client`
- `resource_owner`

`client_id:` ***Corde***

(Facultatif) L'ID du client. Cette option est requise pour l'authentification Microsoft Entra ID et Crowdstrike.

`client_secret:` ***Corde***

(Facultatif) La clé secrète du client. Cette option est requise pour l'authentification Microsoft Entra ID et Crowdstrike.

`resource:` ***Corde***

(Facultatif) L'URI de la ressource Microsoft Entra ID. Cette option est requise pour l'authentification par identifiant Microsoft Entra.

`token_endpoint:` ***Corde***

(Facultatif) Le point de terminaison Microsoft Entra ID /token. Par exemple : « https://login.microsoftonline.com/ <tenant_id>/oauth2/token ». Cette option est requise pour l'authentification par identifiant Microsoft Entra.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "additional_header": "string",
    "authentication": {
        "auth_type": "string",
        "username": "string",
        "password": "string",
        "access_key": "string",
        "secret_key": "string",
        "service": "string",
        "region": "string",
        "grant_type": "string",
        "client_id": "string",
        "client_secret": "string",
        "resource": "string",
        "token_endpoint": "string"
    },
    "host": "string",
    "name": "string",
    "pipeline": true,
    "port": 0,
    "protocol": "string",
    "skip_cert_verification": true
}
```

```
POST /odstargets/kafka
```

Spécifiez les paramètres suivants.

`body:` ***Objet***

`name:` ***Corde***

Le nom de la cible.

`brokers:` ***Tableau d'objets***

Tableau d'un ou de plusieurs objets contenant des informations sur Kafka Brokers.

`host:` ***Corde***

Le nom d'hôte ou l'adresse IP du broker Kafka distant.

`port:` ***Numéro***

Le numéro de port TCP du broker Kafka.

`compression:` ***Corde***

(Facultatif) Méthode de compression à appliquer aux données transmises.

Les valeurs suivantes sont valides :

- `none`
- `gzip`
- `snappy`

`partition_strategy:` ***Corde***

(Facultatif) Méthode de partitionnement à appliquer aux données transmises.

Les valeurs suivantes sont valides :

- `hash_key`
- `manual`
- `random`
- `round_robin`

`protocol:` ***Corde***

Le protocole de transmission des données.

Les valeurs suivantes sont valides :

- `tcp`
- `tls`

`tls_client_cert:` ***Corde***

(Facultatif) Le certificat client TLS qui est envoyé au serveur Kafka lors de l'établissement dproximation TLS. Spécifiez cette option si l'authentification du client est activée sur le serveur Kafka.

`tls_client_key:` ***Corde***

(Facultatif) La clé privée du certificat client TLS spécifiée par le paramètre tls_client_cert. Spécifiez cette option si l'authentification du client est activée sur le serveur Kafka.

`skip_cert_verification:` ***Booléen***

(Facultatif) Indique s'il faut contourner la vérification du certificat TLS pour les données chiffrées. Ce paramètre n'est valide que si le protocole est défini sur tls.

`tls_ca_certs:` ***Corde***

(Facultatif) Les certificats sécurisés avec lesquels valider le certificat du serveur Kafka, au format PEM. Spécifiez cette option si le certificat de votre serveur Kafka n'a pas été signé par une autorité de certification (CA) valide. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides. Cette option n'est valide que si le protocole est TLS.

`authentication:` ***Objet***

(Facultatif) Objet contenant les identifiants d'authentification Kafka.

`auth_type:` ***Corde***

Type d'authentification SASL.

Les valeurs suivantes sont valides :

- `scram`

`username:` ***Corde***

Le nom d'utilisateur de l'utilisateur SASL.

`password:` ***Corde***

Le mot de passe de l'utilisateur SASL.

`algorithm:` ***Corde***

Algorithme de hachage pour l'authentification SASL.

Les valeurs suivantes sont valides :

- `sha256`
- `sha512`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "authentication": {
        "auth_type": "string",
        "username": "string",
        "password": "string",
        "algorithm": "string"
    },
    "brokers": {
        "host": "string",
        "port": 0
    },
    "compression": "string",
    "name": "string",
    "partition_strategy": "string",
    "protocol": "string",
    "skip_cert_verification": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`POST /odstargets/mongodb`

Spécifiez les paramètres suivants.

`body:` ***Objet***

`name:` ***Corde***

Le nom de la cible.

`host:` ***Corde***

Le nom d'hôte ou l'adresse IP du serveur MongoDB distant.

`port:` ***Numéro***

Numéro de port TCP du serveur MongoDB.

`encrypt:` ***Booléen***

(Facultatif) Indique si les données sont chiffrées avec le protocole TLS.

`skip_cert_verification:` ***Booléen***

(Facultatif) Indique s'il faut contourner la vérification du certificat TLS pour les données chiffrées. Ce paramètre n'est valide que si « encryption » est défini sur « true ».

`authentication:` ***Tableau d'objets***

(Facultatif) Tableau d'objets contenant les identifiants d'authentification MongoDB.

`database:` ***Corde***

Nom de la base de données MongoDB.

`user:` ***Corde***

Le nom de l'utilisateur autorisé à modifier la base de données spécifiée.

`password:` ***Corde***

Le mot de passe de l'utilisateur.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "authentication": {
        "database": "string",
        "user": "string",
        "password": "string"
    },
    "encrypt": true,
    "host": "string",
    "name": "string",
    "port": 0,
    "skip_cert_verification": true
}
```

`POST /odstargets/raw`

Spécifiez les paramètres suivants.

`body:` ***Objet***

`name:` ***Corde***

Le nom de la cible.

`host:` ***Corde***

Le nom d'hôte ou l'adresse IP du serveur distant.

`port:` ***Numéro***

Numéro de port TCP ou UDP du serveur distant.

`protocol:` ***Corde***

Le protocole de transmission des données.

Les valeurs suivantes sont valides :

- `tcp`
- `udp`

`compression:` ***Booléen***

(Facultatif) Indique si la compression gzip est appliquée aux données transmises.

`gzip_threshold_bytes:` ***Numéro***

(Facultatif) Le nombre d'octets qui spécifie le seuil de création d'un nouveau message. Toutes les 30 secondes, la sonde ou la console envoie des messages dont la taille dépasse la taille spécifiée pour éviter que les messages ne deviennent trop volumineux. Cette option n'est valide que si la compression est définie sur true.

`gzip_threshold_seconds:` ***Numéro***

(Facultatif) Le nombre de secondes qui spécifie le seuil de création d'un nouveau message. Toutes les 30 secondes, la sonde ou la console envoie des messages qui ont été écrits pendant une durée supérieure à la période spécifiée afin d'éviter que les messages ne deviennent trop volumineux. Cette option n'est valide que si la compression est définie sur true.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "compression": true,
    "gzip_threshold_bytes": 0,
    "gzip_threshold_seconds": 0,
    "host": "string",
    "name": "string",
    "port": 0,
    "protocol": "string"
}
```

`POST /odstargets/syslog`

Spécifiez les paramètres suivants.

`body:` ***Objet***

`name:` ***Corde***

Le nom de la cible.

`host:` ***Corde***

Le nom d'hôte ou l'adresse IP du serveur Syslog distant.

`port:` ***Numéro***

Numéro de port TCP ou UDP du serveur Syslog distant.

`tcp_length_prefix_framing:` ***Booléen***

(Facultatif) Indique s'il faut ajouter le nombre d'octets d'un message au début du message. Si ce paramètre est défini sur faux, la fin de chaque message est délimitée par une nouvelle ligne de fin.

`batch_min_bytes:` ***Numéro***

(Facultatif) Le nombre minimum d'octets à envoyer simultanément au serveur Syslog.

`concurrent_connections:` ***Numéro***

(Facultatif) Le nombre de connexions simultanées sur lesquelles envoyer des messages.

`localtime:` ***Booléen***

(Facultatif) Indique si les horodatages font référence au fuseau horaire local de la sonde ou de la console. Si ce paramètre est défini sur faux, les horodatages font référence à GMT.

`protocol:` ***Corde***

Le protocole de transmission des données.

Les valeurs suivantes sont valides :

- `tcp`
- `udp`
- `tls`

`tls_client_cert:` ***Corde***

(Facultatif) Le certificat client TLS qui est envoyé au serveur Syslog lors de l'établissement dproximation TLS. Spécifiez cette option si l'authentification du client est activée sur le serveur Syslog.

`tls_client_key:` ***Corde***

(Facultatif) La clé privée du certificat client TLS spécifiée par le paramètre tls_client_cert. Spécifiez cette option si l'authentification du client est activée sur le serveur Syslog.

`skip_cert_verification:` ***Booléen***

(Facultatif) Indique s'il faut contourner la vérification du certificat TLS pour les données chiffrées. Ce paramètre n'est valide que si le protocole est défini sur tls.

`tls_ca_certs:` ***Corde***

(Facultatif) Les certificats sécurisés avec lesquels valider le certificat du serveur Syslog, au format PEM. Spécifiez cette option si le certificat de votre serveur Syslog n'a pas été signé par une autorité de certification (CA) valide. Si cette option n'est pas spécifiée, le certificat de serveur est validé à l'aide de la liste intégrée des certificats CA valides. Cette option n'est valide que si le protocole est TLS et que skip_cert_verification est faux.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "batch_min_bytes": 0,
    "concurrent_connections": 0,
    "host": "string",
    "localtime": true,
    "name": "string",
    "port": 0,
    "protocol": "string",
    "skip_cert_verification": true,
    "tcp_length_prefix_framing": true,
    "tls_ca_certs": "string",
    "tls_client_cert": "string",
    "tls_client_key": "string"
}
```

`DELETE /odstargets/http/{name}`

Spécifiez les paramètres suivants.

`name:` ***Corde***

Le nom de la cible.

`DELETE /odstargets/kafka/{name}`

Spécifiez les paramètres suivants.

`name:` ***Corde***

Le nom de la cible.

`DELETE /odstargets/mongodb/{name}`

Spécifiez les paramètres suivants.

`name:` ***Corde***

Le nom de la cible.

`DELETE /odstargets/raw/{name}`

Spécifiez les paramètres suivants.

`name:` ***Corde***

Le nom de la cible.

```
DELETE /odstargets/syslog/{name}
```

Spécifiez les paramètres suivants.

`name:` ***Corde***
Le nom de la cible.

Recherche par paquets

Vous pouvez rechercher et télécharger des paquets stockés sur le système ExtraHop. Le téléchargé les paquets peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

Pour plus d'informations sur les paquets, voir Paquets.

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

Fonctionnement	Descriptif
GET /packets/search	Recherchez des paquets en spécifiant des paramètres dans une URL.
POST /paquets/search	Recherchez des paquets en spécifiant des paramètres dans une chaîne JSON.

Détails de l'opération

```
GET /packets/search
```

Spécifiez les paramètres suivants.

`output:` ***Corde***
(Facultatif) Format de sortie. * `pcap` - Un fichier PCAP qui contient des paquets. * `keylog_txt` - Un fichier texte keylog contenant des secrets pour le déchiffrement. * `pcapng` - Un fichier PCAPNG qui peut contenir à la fois des paquets et des secrets à déchiffrer. * `zip` - Un fichier ZIP qui contient à la fois un fichier texte PCAP et un keylog. * `extract` - Un fichier ZIP contenant des fichiers extraits de paquets correspondant à la requête. Cette option n'est valide que si vous disposez d'un accès complet au module NDR.

Les valeurs suivantes sont valides :

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`
- `extract`

`include_secrets:` ***Booléen***
(Facultatif) Spécifie s'il faut inclure des secrets dans le fichier PCAPNG. Cette option n'est valide que si la sortie est définie sur pcapng.

`decrypt_files:` ***Booléen***
(Facultatif) Spécifie s'il faut déchiffrer les fichiers extraits contenant des secrets stockés. Cette option n'est valide que si le paramètre « output » est « extract ».

`limit_bytes:` ***Corde***
(Facultatif) Le nombre maximum approximatif d'octets à renvoyer. Une fois que le système ExtraHop a trouvé des paquets correspondant à la taille spécifiée dans les critères de recherche, il arrête de rechercher des paquets supplémentaires. Cependant, étant donné que le système analyse plusieurs paquets à la fois, la taille totale des paquets renvoyés peut être supérieure à la taille spécifiée. L'unité

par défaut est l'octet, mais vous pouvez spécifier d'autres unités avec un suffixe d'unité. La valeur par défaut est « 100 Mo ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 100 Mo », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`limit_search_duration:` ***Corde***

(Facultatif) Durée maximale approximative pour effectuer la recherche de paquets. Une fois le délai spécifié écoulé, le système ExtraHop arrête de rechercher des paquets supplémentaires. Cependant, le système va dépasser la durée spécifiée pour terminer l'analyse des paquets qui étaient recherchés avant l'expiration du délai, et le système analyse plusieurs paquets à la fois. Par conséquent, la recherche peut durer plus longtemps que la durée spécifiée. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. La valeur par défaut est « 5 m ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 5 m », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`always_return_body:` ***Booléen***

(Facultatif) Spécifie le comportement si la requête ne correspond à aucun paquet ou si les paquets correspondants à la requête ne contiennent aucun fichier. Si la valeur est vraie, le système renvoie un fichier vide et un code dquo 200. Si la valeur est fausse, le système renvoie un code dveloppement 204 mais ne renvoie pas de fichier.

`from:` ***Corde***

L'horodateur de début de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -10m pour commencer la recherche avec les paquets capturés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera avec les paquets capturés au moment de la recherche. Une valeur négative indique que la recherche se terminera par des paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -5m pour terminer la recherche avec les paquets capturés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`bpf:` ***Corde***

(Facultatif) La syntaxe du filtre de paquets de Berkeley (BPF) pour la recherche de paquets. Pour plus d'informations sur la syntaxe BPF, consultez Guide de l'API REST.

`ip1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`ip2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`POST /packets/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de la recherche de paquets.

`output:` ***Corde***

(Facultatif) Format de sortie.

Les valeurs suivantes sont valides :

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`
- `extract`

`include_secrets:` ***Booléen***

(Facultatif) Indique s'il faut inclure ou non les secrets TLS avec les données des paquets dans les fichiers .pcapng. Valide uniquement si « output » est « pcapng ».

`decrypt_files:` ***Booléen***

(Facultatif) Spécifie s'il faut déchiffrer les fichiers extraits contenant des secrets stockés. Cette option n'est valide que si le paramètre « output » est « extract ».

`limit_bytes:` ***Corde***

(Facultatif) Le nombre maximum approximatif d'octets à renvoyer. Une fois que le système ExtraHop a trouvé des paquets correspondant à la taille spécifiée dans les critères de recherche, il arrête de rechercher des paquets supplémentaires. Cependant, étant donné que le système analyse plusieurs paquets à la fois, la taille totale des paquets renvoyés peut être supérieure à la taille spécifiée. L'unité par défaut est l'octet, mais vous pouvez spécifier d'autres unités avec un suffixe d'unité. La valeur par défaut est « 100 Mo ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 100 Mo », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`limit_search_duration:` ***Corde***

(Facultatif) Durée maximale approximative pour effectuer la recherche de paquets. Une fois le délai spécifié écoulé, le système ExtraHop arrête de rechercher des paquets supplémentaires. Cependant, le système va dépasser la durée spécifiée pour terminer l'analyse des paquets qui étaient recherchés avant l'expiration du délai, et le système analyse plusieurs paquets à la fois. Par conséquent, la recherche peut durer plus longtemps que la durée spécifiée. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. La valeur par défaut est « 5 m ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 5 m », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`always_return_body:` ***Booléen***

(Facultatif) Spécifie le comportement si la requête ne correspond à aucun paquet ou si les paquets correspondants à la requête ne contiennent aucun fichier. Si la valeur est vraie, le système renvoie un fichier vide et un code dquo 200. Si la valeur est fausse, le système renvoie un code dveloppement 204 mais ne renvoie pas de fichier.

`from:` ***Corde***

L'horodateur de début de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -10m pour commencer la recherche avec les paquets capturés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera avec les paquets capturés au moment de la recherche. Une valeur négative indique que la recherche se terminera par des paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -5m pour terminer la recherche avec les paquets capturés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`bpf:` ***Corde***

(Facultatif) La syntaxe du filtre de paquets de Berkeley (BPF) pour la recherche de paquets. Pour plus d'informations sur la syntaxe BPF, voir Filtrer les paquets avec la syntaxe du filtre de paquets de Berkeley.

`ip1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`ip2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "always_return_body": true,
    "bpf": "string",
    "decrypt_files": true,
    "from": "string",
    "include_secrets": true,
    "ip1": "string",
    "ip2": "string",
    "limit_bytes": "string",
    "limit_search_duration": "string",
    "output": "string",
    "port1": "string",
    "port2": "string",
    "until": "string"
}
```

Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley

Recherchez des paquets à l'aide de la syntaxe du filtre de paquets de Berkeley (BPF) uniquement ou en combinaison avec les filtres intégrés.

Les filtres de paquets Berkeley constituent une interface brute pour les couches de liaison de données et constituent un outil puissant pour l'analyse de détection des intrusions. La syntaxe BPF permet aux utilisateurs d'écrire des filtres qui explorent rapidement des paquets spécifiques pour afficher les informations essentielles.

Le système ExtraHop construit un en-tête de paquet synthétique à partir des données d'index des paquets, puis exécute les requêtes de syntaxe BPF par rapport à l'en-tête du paquet pour garantir que les requêtes sont beaucoup plus rapides que le scan de la charge utile complète du paquet. Notez qu'ExtraHop ne prend en charge qu'un sous-ensemble de la syntaxe BPF. Voir Syntaxe BPF prise en charge.

La syntaxe BPF consiste en une ou plusieurs primitives précédées d'un ou de plusieurs qualificatifs. Les primitives se composent généralement d'un identifiant (nom ou numéro) précédé d'un ou de plusieurs qualificatifs. Il existe trois types de qualifications différents :

type

Des qualificatifs qui indiquent le type auquel le nom ou le numéro d'identification fait référence. Par exemple, `host`, `net`, `port`, et `portrange`. S'il n'y a pas de qualificatif, `host` est supposé.

dir

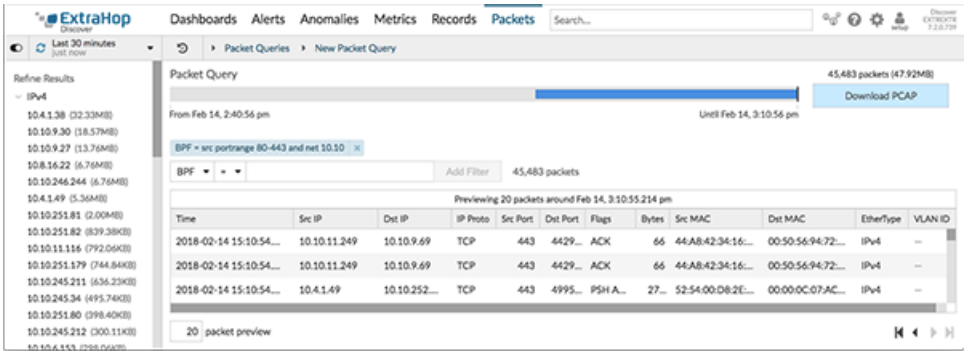
Qualificatifs qui spécifient une direction de transfert particulière vers ou depuis un identifiant. Les directions possibles sont `src`, `dst`, `src and dst`, et `src or dst`. Par exemple, `dst net 128.3`.

proto

Qualificatifs qui limitent la correspondance au protocole en question. Les protocoles possibles sont `ether`, `ip`, `ip6`, `tcp`, et `udp`.

Ajouter un filtre avec la syntaxe BPF

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Paquets**.
3. Dans la section du filtre à trois champs, sélectionnez **BPF**, puis tapez la syntaxe de votre filtre. Par exemple, tapez `src portrange 80-443 and net 10.10`.
4. Cliquez **Télécharger PCAP** pour enregistrer la capture du paquet avec vos résultats filtrés.



Syntaxe BPF prise en charge

Le système ExtraHop prend en charge le sous-ensemble suivant de la syntaxe BPF pour le filtrage des paquets.

Note:
- ExtraHop ne prend en charge que les recherches d'adresses IP numériques. Les noms d'hôtes ne sont pas autorisés.
- Indexation dans les en-têtes, `[...]`, n'est pris en charge que pour `tcpflags` et `ip_offset`. Par exemple, `tcp[tcpflags] & (tcp-syn|tcp-fin) != 0`
- ExtraHop prend en charge les valeurs numériques et hexadécimales pour les champs VLAN ID, EtherType et IP Protocol. Préfixez les valeurs hexadécimales par 0x, par exemple 0x11.

Primitif	Exemples	Descriptif
`[src|dst] host <host ip>`	`host 203.0.113.50` `dst host 198.51.100.200`	Correspond à un hôte en tant que source IP, destination, ou l'une ou l'autre des deux. Ces expressions d'hôte peuvent être spécifiées conjointement avec d'autres protocoles tels que ip, arp, rarp ou ip6.

Primitif	Exemples	Descriptif
`ether [src|dst] host <MAC>`	`ether host 00:00:5E:00:53:00` `ether dst host 00:00:5E:00:53:00`	Fait correspondre un hôte en tant que source Ethernet, destination ou l'une des deux.
`vlan <ID>`	`vlan 100`	Correspond à un VLAN. Les numéros d'identification valides sont `0-4095`. Les bits de priorité du VLAN sont nuls. Si le paquet d'origine comportait plusieurs balises VLAN, le paquet synthétique auquel le BPF correspond n'aura que la balise VLAN la plus interne.

`[src|dst] portrange <p1>-<p2>`
ou
`[tcp|udp] [src|dst] portrange <p1>-<p2>`
	`src portrange 80-88`
	`tcp dst portrange 1501-1549`
		Fait correspondre les paquets à destination ou en provenance d'un port dans la plage donnée. Des protocoles peuvent être appliqués à une plage de ports pour filtrer des paquets spécifiques dans cette plage.

`[ip|ip6][src|dst] proto <protocol>`	`proto 1`
	`src 10.4.9.40 and proto ICMP`
	`ip6 and src fe80::aebc:32ff:fe84:70b7 and proto 47`
	`ip and src 10.4.9.40 and proto 0x0006`
		Correspond aux protocoles IPv4 ou IPv6 autres que TCP et UDP. Le protocole peut être un numéro ou un nom.

`[ip|ip6][tcp|udp] [src|dst] port <port>`	`udp and src port 2005` `ip6 and tcp and src port 80`	Correspond aux paquets IPv4 ou IPv6 sur un port spécifique.

`[src|dst] net <network>`	`dst net 192.168.1.0`
	`src net 10`
	`net 192.168.1.0/24`
		Fait correspondre les paquets à destination ou en provenance d'une source ou d'une destination ou de l'une ou l'autre, qui résident sur un réseau. Un numéro de réseau IPv4 peut être spécifié sous la forme de l'une des valeurs suivantes :
		• Quad pointillé (x.x.x.x)
		• Triple en pointillés (x.x.x)
		• Paire pointillée (x.x)
		• Numéro unique (x)

Primitif	Exemples	Descriptif

`[ip|ip6] tcp tcpflags & (tcp-[ack|fin|syn|rst|push|urg|)`	`tcp[tcpflags] & (tcp-ack) !=0`
	`tcp[13] & 16 !=0`
	`ip6 and (ip6[40+13] & (tcp-syn) != 0)`
		Correspond à tous les paquets avec l'indicateur TCP spécifié

Paquets IPv4 fragmentés (ip_offset ! = 0)	`ip[6:2] & 0x3fff != 0x0000`	Correspond à tous les paquets contenant des fragments.

Couplage

Cette ressource vous permet de générer un jeton nécessaire pour connecter un sonde à un console.

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

Fonctionnement	Descriptif
POST/appariement/jeton	Générez un jeton requis pour connecter le sonde à un console.

Détails de l'opération

```
POST /pairing/token
```

Il n'existe aucun paramètre pour cette opération.

Journal des enregistrements

Les enregistrements sont des informations structurées sur les flux et les transactions concernant les événements de votre réseau.

Après avoir connecté le système ExtraHop à un magasin de disques, vous pouvez générer et envoyer des informations d'enregistrement à l'espace de stockage des enregistrements, et vous pouvez interroger des enregistrements pour récupérer des informations sur n'importe quel objet de votre réseau. Pour plus d'informations, voir Requête d'enregistrements via l'API REST.

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

opération	Descriptif
GET /records/cursor/ {curseur}	Obsolète. Remplacé par `POST /records/cursor`.
POST /enregistrements/curseur	Récupère les enregistrements en commençant par un curseur spécifié. Cette opération n'est prise en charge que si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop (tel que l'EXA 5300) ou sur CrowdStrike LogScale.
POST /enregistrements/recherche	Effectuez une requête dans le journal d'enregistrement.

Détails de l'opération

`POST /records/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Requête du journal d'enregistrement.

`from:` ***Numéro***

L'horodateur de début de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les enregistrements créés dans le passé. Par exemple, spécifiez -600 000 ms pour commencer la recherche avec les enregistrements créés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Numéro***

L'horodateur de fin de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera par les enregistrements créés au moment de la demande. Une valeur négative indique que la recherche se terminera par des enregistrements créés dans le passé. Par exemple, spécifiez -300 000 ms pour terminer la recherche avec les enregistrements créés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`types:` ***Tableau de cordes***

(Facultatif) Tableau d'un ou de plusieurs formats d'enregistrement. La requête renvoie uniquement les enregistrements correspondant aux formats spécifiés. Si aucune valeur n'est spécifiée, la requête renvoie des enregistrements de n'importe quel type. Les valeurs valides pour ce champ sont affichées dans le champ Type d'enregistrement de la page Formats d'enregistrement. Par exemple : « ~cifs ».

`limit:` ***Numéro***

Le nombre maximum d'enregistrements renvoyés par la requête. La valeur maximale ne peut pas dépasser 10 000. La valeur par défaut est 100.

`offset:` ***Numéro***

Le nombre d'enregistrements à ignorer dans les résultats de la requête. La requête renverra des enregistrements à partir de la valeur de décalage. Ce paramètre est souvent associé aux paramètres de limite et de tri. La valeur par défaut est 0. Pour les magasins d'enregistrements ExtraHop, la valeur maximale est de 10 000 ; pour récupérer les enregistrements renvoyés après les 10 000 premiers, consultez POST /records/cursor/. Pour les magasins de disques tiers, il n'y a pas de valeur maximale.

`sort:` ***Tableau d'objets***

Liste d'un ou de plusieurs objets de tri qui spécifient les priorités de tri. Les enregistrements renvoyés sont triés dans l'ordre dans lequel les objets sont répertoriés. Les paramètres sont définis dans la section sort_item ci-dessous. Si aucune valeur sort_item n'est fournie, les enregistrements sont triés par horodateur dans l'ordre décroissant.

`field:` ***Corde***

Le nom du champ qui a renvoyé les enregistrements est trié par.

`direction:` ***Corde***

L'ordre dans lequel les enregistrements renvoyés sont triés. L'ordre par défaut est décroissant. Une fois tous les autres critères de tri appliqués, ou si aucun critère de tri n'a été spécifié, l'ordre par défaut est décroissant par horodateur.

Les valeurs suivantes sont valides :

- `asc`
- `desc`

`filter:` ***Objet***

L'objet contenant les paramètres qui spécifient les critères de filtre. Les paramètres sont définis dans la section des filtres ci-dessous. Si aucune valeur de filtre n'est fournie, la requête renvoie tous les enregistrements correspondant à l'intervalle de temps et à tout format d'enregistrement spécifié.

`field:` ***Corde***

Le nom du champ de l'enregistrement à filtrer. La requête compare le contenu du paramètre de champ à la valeur du paramètre d'opérande. Si le nom de champ spécifié est « .any », l'union de toutes les valeurs de champ sera recherchée. Si le nom de champ spécifié est « .ipaddr » ou « .port », les rôles client, serveur, expéditeur et destinataire sont inclus dans la recherche. Les noms des champs sont situés dans des formats d'enregistrement qui peuvent être visualisés dans le système ExtraHop.

`operator:` ***Corde***

Méthode de comparaison appliquée lors de la mise en correspondance de la valeur de l'opérande avec le contenu du champ. Tous les objets filtrants nécessitent un opérateur.

Les valeurs suivantes sont valides :

- `>`
- `<`
- `<=`
- `>=`
- `=`
- `!=`
- `startswith`
- `~`
- `!~`
- `and`
- `or`
- `not`
- `exists`
- `not_exists`
- `in`
- `not_in`

`operand:` ***Chaîne, numéro ou objet***

La valeur à laquelle la requête tente de faire correspondre. La requête compare la valeur de l'opérande au contenu du paramètre de champ et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier explicitement le type de données d'opérande comme décrit dans le Guide de l'API REST.

`rules:` ***Tableau d'objets***

Liste d'un ou de plusieurs objets filtrants au sein d'un même objet filtrant. Les objets de filtre peuvent être intégrés de manière récursive. Seuls les opérateurs « et », « ou » et « non » sont autorisés pour ce paramètre.

`context_ttl:` ***Numéro***

Durée pendant laquelle le contexte de recherche reste actif. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. Dans

RevealX Enterprise, ce champ n'est valide que si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop (tel qu'un EXA 5300) ou sur CrowdStrike LogScale. Dans RevealX 360, ce champ n'est valide que pour les systèmes dotés d'un espace de stockage des enregistrements basé sur le cloud avec Premium Investigation. Dans RevealX Enterprise avec CrowdStrike LogScale et RevealX 360 avec Premium Investigation, ce champ n'est pas valide si les champs de tri ou de décalage sont spécifiés.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "context_ttl": 0,
    "filter": {
        "field": "string",
        "operator": "string",
        "operand": "string",
        "rules": []
    },
    "from": 0,
    "limit": 0,
    "offset": 0,
    "sort": {
        "field": "string",
        "direction": "string"
    },
    "types": [],
    "until": 0
}
```

`POST /records/cursor`

Spécifiez les paramètres suivants.

`body:` ***Objet***

L'ID du curseur qui indique la page suivante de résultats de la requête.

`cursor:` ***Corde***

Identifiant unique du curseur qui indique la page de résultats suivante de la requête.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cursor": "string"
}
```

`context_ttl:` ***Numéro***

(Facultatif) Durée pendant laquelle le contexte de recherche reste actif, exprimée en millisecondes. Une fois la durée spécifiée écoulée, le curseur devient invalide et vous ne pouvez plus récupérer d'enregistrements supplémentaires à partir de la recherche. Spécifiez ce paramètre pour étendre le contexte de recherche spécifié précédemment.

`GET /records/cursor/{cursor}`

Spécifiez les paramètres suivants.

`cursor:` ***Corde***

L'ID du curseur.

`context_ttl:` ***Numéro***

(Facultatif) Durée pendant laquelle le contexte de recherche reste actif, exprimée en millisecondes.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cursor": "string",
    "from": 0,
    "lookback_exceeded": true,
    "lookback_truncated": true,
    "records": {},
    "total": 0,
    "until": 0,
    "warnings": {}
}
```

Valeurs des opérandes dans les requêtes d'enregistrement

Le `operand` champ dans le `POST /records/search` méthode spécifie la valeur à laquelle une requête d'enregistrement tente de correspondre. Vous pouvez spécifier la valeur uniquement ou à la fois le type de données et la valeur. Si vous spécifiez uniquement la valeur, la requête fera référence au format dac.enregistrement associé au `field` paramètre pour déterminer le type de données de la valeur.

Par exemple, si vous souhaitez rechercher une adresse IP, vous pouvez spécifier un type de données d'adresse IP, puis fournir l'adresse réelle comme valeur.

L'exemple suivant spécifie explicitement le type de données et la valeur de l' opérande :

```
{
    "from": -1000,
    "filter": {
        "field" : "senderAddr",
        "operator": "=",
        "operand" : { "type" : "ipaddr4", "value": "1.2.3.4" }
    }
}
```

L'exemple suivant indique uniquement la valeur de l' opérande :

```
{
    "from": -1000,
    "filter": {
        "field" : "senderAddr",
        "operator": "=",
        "operand" : "1.2.3.4"
    }
}
```

Vous pouvez spécifier explicitement les types de données suivants dans le `operand` champ :

- application
- booléen
- équipement

  Note: Vous devez spécifier l'ID de découverte de l'équipement dans le champ de valeur. Vous pouvez trouver l'identifiant de découverte d'un équipement via le `POST /devices/search` opération.
- filtre_appareil
- groupe_d'appareils
- interface de flux
- réseau de flux
- ipad dr4
- ipad dr6

- nombre
- localité_réseau
- objet
- chaîne

Le `operand` le champ prend en charge la notation CIDR lors du filtrage par adresse IP ; le `operator` le champ doit être défini sur « = » ou « ! = ».

Vous pouvez spécifier plusieurs filtres en incluant `rules` option, comme indiqué dans l' exemple suivant :

```
{
  "filter": {
    "operator": "and",
    "rules": [
      {
        "field": "method",
        "operand": "SMB2_READ",
        "operator": "="
      },
      {
        "field": "reqL2Bytes",
        "operand": "100",
        "operator": ">"
      }
    ]
  },
  "types": [
    "~cifs"
  ],
    "from": "-30m"
}
```

Interrogez les enregistrements à l'aide d'un filtre de groupe déquipements

Pour filtrer les enregistrements par groupe déquipements dans l'API REST, vous devez envoyer un `POST` demande adressée au `/records/search` point de terminaison doté d'un filtre de requête d'enregistrement répondant aux critères suivants :

- Le `field` doit spécifier des périphériques, tels que `client`, `server`, `sender`, ou `receiver`.
- Le `operator` doit être soit `in` ou `not_in`.
- Le `operand type` doit être `device_group`.
- Le `operand value` doit être une représentation sous forme de chaîne de l'identifiant numérique du groupe déquipements. Vous pouvez récupérer les identifiants de groupes d'équipements en exécutant l'opération GET /devicegroup et en consultant le contenu du `id` champ dans la réponse.

Par exemple, la requête suivante recherche des enregistrements dans lesquels l' équipement client était membre d'un groupe déquipements avec un ID de 200 :

```
{
    "from": "-30m",
    "filter": {
        "field": "client",
        "operator": "in",
        "operand": {
            "type": "device_group",
            "value": "200"
        }
    }
}
```

Vous pouvez également filtrer les enregistrements en fonction de critères de groupe d'équipements sans créer de groupe de périphériques en spécifiant le type d'opérande comme `device_filter`. Par exemple, la requête suivante recherche les enregistrements dans lesquels l'équipement client exécute Windows 10 :

```
{
    "from": "-30m",
    "filter": {
        "field": "client",
        "operator": "in",
        "operand": {
            "type": "device_filter",
            "value": {
                "field": "software",
                "operand": "windows_10",
                "operator": "="
            }
        }
    }
}
```

Note: Valeurs d'opérande avec type `device_filter` pour la recherche d'enregistrements sont formatés de la même manière que les filtres de recherche d'équipements. Pour plus d'informations, voir Valeurs d'opérandes pour les groupes d'équipements.

Interroger les enregistrements à l'aide d'un filtre de localité du réseau

Pour filtrer les enregistrements par groupe déquipements dans l'API REST, vous devez envoyer une requête POST au `/records/search` point de terminaison doté d'un filtre de requête d'enregistrement répondant aux critères suivants :

- Le champ doit être un champ d'enregistrement qui spécifie une adresse IP telle que `clientAddr`, `serverAddr`, `senderAddr`, ou `receiverAddr`.
- L'opérateur doit être soit `in` ou `not_in`.
- Le type d'opérande doit être `network_locality`.
- La valeur de l'opérande doit être une représentation sous forme de chaîne d'un identifiant numérique de localité du réseau. Vous pouvez consulter les identifiants des localités à l'aide du `GET /networklocalities` opération.

Par exemple, la requête suivante recherche les enregistrements où l'équipement client se trouve dans une localité du réseau avec un ID de `123`:

```
{
    "from": "-30m",
    "filter": {
        "field": "clientAddr",
        "operand": {
            "type": "network_locality",
            "value": "123"
        },
        "operator": "in"
    }
}
```

Unités de temps prises en charge

Pour la plupart des paramètres, l'unité par défaut pour la mesure du temps est la milliseconde. Toutefois, les paramètres suivants renvoient ou acceptent des unités de temps alternatives telles que les minutes et les heures :

- Appareil

    - actif_depuis
    - actif_jusqu'à
- Groupe d'appareils
    - actif_depuis
    - actif_jusqu'à
- Métriques
    - à partir de
    - jusqu'à
- Journal d'enregistrement
    - à partir de
    - jusqu'à
    - context_ttl

Le tableau suivant indique les unités de temps prises en charge :

Unité de temps	Suffixe d'unité
Année	`y`
Mois	`M`
Semaine	`w`
Journée	`d`
Heure	`h`
Minutes	`m`
Deuxième	`s`
Milliseconde	`ms`

Pour spécifier une unité de temps autre que les millisecondes pour un paramètre, ajoutez le suffixe de l'unité à la valeur. Par exemple, pour demander des appareils actifs au cours des 30 dernières minutes, spécifiez la valeur de paramètre suivante :

```
GET /api/v1/devices?active_from=-30m
```

L'exemple suivant indique une recherche pour HTTP records créés il y a 1 à 2 heures :

```
{
    "from": "-2h",
    "until": "-1h",
    "types": ["~http"]
}
```

Rapport

Un rapport est un fichier PDF d'un tableau de bord que vous pouvez programmer pour l'envoi d'e-mails à un ou plusieurs destinataires. Vous pouvez spécifier la fréquence à laquelle le rapport est envoyé par e-mail et l'intervalle de temps pour les données du tableau de bord incluses dans le fichier PDF.

Important: Vous pouvez uniquement planifier des rapports à partir d'une console ExtraHop.

Voici quelques considérations importantes concernant les rapports sur les tableaux de bord :

- Vous ne pouvez créer un rapport que pour les tableaux de bord qui vous appartiennent ou qui ont été partagés avec vous. Votre capacité à créer un rapport est déterminée par vos privilèges d'utilisateur. Contactez votre administrateur ExtraHop pour obtenir de l'aide.
- Chaque rapport ne peut être lié qu'à un seul tableau de bord.
- Si vous avez créé un rapport pour un tableau de bord qui a ensuite été supprimé ou est devenu inaccessible pour vous, l'e-mail planifié continuera d'être envoyé aux destinataires. Cependant, l'e-mail n'inclura pas le fichier PDF et informera les destinataires que le tableau de bord n'est pas disponible pour le propriétaire du rapport.

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

opération	Descriptif
GET /rapports	Récupérez tous les rapports.
POST /rapports	Créez un rapport.
SUPPRIMER /reports/ {id}	Supprimer un rapport spécifique.
GET /reports/ {id}	Récupérez un rapport spécifique.
PATCH /reports/ {id}	Mettez à jour un rapport spécifique.
GET /reports/ {id} /contents	Récupérez le contenu d'un rapport spécifique.
PUT /reports/ {id} /contents	Remplacez le contenu d'un rapport spécifique.
GET /reports/ {id} /télécharger	Récupérez le PDF d'un rapport.
POST /reports/ {id} /emailgroups	Modifiez le groupe d'e-mails attribué à un rapport de tableau de bord spécifique.
GET /reports/ {id} /emailgroups	Récupérez la liste des groupes d'e-mails affectés à un rapport de tableau de bord spécifique.
SUPPRIMER /reports/ {id} /emailgroups/ {group-id}	Supprimer un groupe d'e-mails d'un rapport de tableau de bord spécifique.
POST /reports/ {id} /emailgroups/ {group-id}	Ajoutez un groupe d'e-mails à un rapport de tableau de bord spécifique.
POST /reports/ {id} /file d'attente	Générez et envoyez immédiatement un rapport spécifique.

Détails de l'opération

`GET /reports`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
```

```
    "schedule": {},
    "until": "string"
}
```

`POST /reports`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Le contenu du rapport.

`name:` ***Corde***

Le nom du rapport.

`description:` ***Corde***

(Facultatif) Description du rapport.

`owner:` ***Corde***

Nom d'utilisateur du propriétaire du rapport.

`cc:` ***Tableau de cordes***

La liste des adresses e-mail, non incluses dans un groupe d'e-mails, pour recevoir des rapports.

`enabled:` ***Booléen***

(Facultatif) Indique si le rapport est activé.

`from:` ***Corde***

L'horodateur de début de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`email_subject:` ***Corde***

(Facultatif) Le contenu de la ligne d'objet de l'e-mail de rapport.

`schedule:` ***Objet***

(Facultatif) Objet contenant les paramètres qui spécifient la plage horaire planifiée pour générer et envoyer le rapport. Les paramètres sont définis dans la section schedule_type ci-dessous.

`type:` ***Corde***

Type de calendrier de livraison du rapport.

Les valeurs suivantes sont valides :

- `hourly`
- `daily`
- `weekly`
- `monthly`

`at:` ***Tableau d'objets***

(Facultatif) La liste des objets qui spécifient les paramètres de diffusion du rapport. Les paramètres sont définis dans la section at_type ci-dessous.

`by_day:` ***Tableau de cordes***

(Facultatif) Les jours de la semaine où le rapport doit être envoyé.

Les valeurs suivantes sont valides :

- `mo`
- `tu`
- `we`

- `th`
- `fr`
- `sa`
- `su`

`on_day:` ***Numéro***

(Facultatif) Le jour du mois auquel le rapport sera exécuté.

`tz:` ***Corde***

(Facultatif) Fuseau horaire dans lequel envoyer le rapport.

`hour:` ***Numéro***

(Facultatif) Heure d'envoi du rapport.

`minute:` ***Numéro***

(Facultatif) La minute à laquelle le rapport doit être envoyé.

`interval:` ***Corde***

(Facultatif) L'intervalle peut être previous_week, previous_month ou rien.

Les valeurs suivantes sont valides :

- `previous_week`
- `previous_month`

`output:` ***Objet***

Objet contenant les paramètres qui spécifient le format de sortie du rapport. Les paramètres sont définis dans la section format_type ci-dessous.

`type:` ***Corde***

Format de sortie du rapport.

Les valeurs suivantes sont valides :

- `pdf`

`width:` ***Corde***

(Facultatif) Option de largeur pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `narrow`
- `medium`
- `wide`

`pagination:` ***Corde***

(Facultatif) Schéma de pagination pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `per_region`

`theme:` ***Corde***

(Facultatif) Thème d'affichage de la sortie du rapport.

Les valeurs suivantes sont valides :

- `light`
- `dark`
- `space`
- `contrast`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cc": [],
```

```
    "description": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "on_day": 0,
            "tz": "string",
            "hour": 0,
            "minute": 0
        },
        "interval": "string"
    },
    "until": "string"
}
```

`POST /reports/{id}/queue`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`PATCH /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`body:` ***Objet***
Le contenu du rapport.

`name:` ***Corde***
Le nom du rapport.

`description:` ***Corde***
(Facultatif) Description du rapport.

`owner:` ***Corde***
Nom d'utilisateur du propriétaire du rapport.

`cc:` ***Tableau de cordes***
La liste des adresses e-mail, non incluses dans un groupe d'e-mails, pour recevoir des rapports.

`enabled:` ***Booléen***
(Facultatif) Indique si le rapport est activé.

`from:` ***Corde***
L'horodateur de début de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`email_subject:` ***Corde***

(Facultatif) Le contenu de la ligne d'objet de l'e-mail de rapport.

`schedule:` ***Objet***

(Facultatif) Objet contenant les paramètres qui spécifient la plage horaire planifiée pour générer et envoyer le rapport. Les paramètres sont définis dans la section schedule_type ci-dessous.

`type:` ***Corde***

Type de calendrier de livraison du rapport.

Les valeurs suivantes sont valides :

- `hourly`
- `daily`
- `weekly`
- `monthly`

`at:` ***Tableau d'objets***

(Facultatif) La liste des objets qui spécifient les paramètres de diffusion du rapport. Les paramètres sont définis dans la section at_type ci-dessous.

`by_day:` ***Tableau de cordes***

(Facultatif) Les jours de la semaine où le rapport doit être envoyé.

Les valeurs suivantes sont valides :

- `mo`
- `tu`
- `we`
- `th`
- `fr`
- `sa`
- `su`

`on_day:` ***Numéro***

(Facultatif) Le jour du mois auquel le rapport sera exécuté.

`tz:` ***Corde***

(Facultatif) Fuseau horaire dans lequel envoyer le rapport.

`hour:` ***Numéro***

(Facultatif) Heure d'envoi du rapport.

`minute:` ***Numéro***

(Facultatif) La minute à laquelle le rapport doit être envoyé.

`interval:` ***Corde***

(Facultatif) L'intervalle peut être previous_week, previous_month ou rien.

Les valeurs suivantes sont valides :

- `previous_week`
- `previous_month`

`output:` ***Objet***

Objet contenant les paramètres qui spécifient le format de sortie du rapport. Les paramètres sont définis dans la section format_type ci-dessous.

`type:` ***Corde***

Format de sortie du rapport.

Les valeurs suivantes sont valides :

- `pdf`

`width:` ***Corde***

(Facultatif) Option de largeur pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `narrow`
- `medium`
- `wide`

`pagination:` ***Corde***

(Facultatif) Schéma de pagination pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `per_region`

`theme:` ***Corde***

(Facultatif) Thème d'affichage de la sortie du rapport.

Les valeurs suivantes sont valides :

- `light`
- `dark`
- `space`
- `contrast`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cc": [],
    "description": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "on_day": 0,
            "tz": "string",
            "hour": 0,
            "minute": 0
        },
        "interval": "string"
    },
    "until": "string"
}
```

`GET /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`GET /reports/{id}/download`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`DELETE /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`GET /reports/{id}/contents`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "dashboard_id": 0,
    "params": {},
    "type": "string"
}
```

`PUT /reports/{id}/contents`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.
`body:` ***Objet***
Le contenu du rapport.

`POST /reports/{id}/emailgroups/{group-id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.
`group-id:` ***Numéro***
L'identifiant unique du groupe de messagerie.

`POST /reports/{id}/emailgroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.
`body:` ***Objet***
La liste des identifiants de groupes de messagerie à attribuer ou annuler au rapport.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`GET /reports/{id}/emailgroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`DELETE /reports/{id}/emailgroups/{group-id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`group-id:` ***Numéro***
L'identifiant unique du groupe de messagerie.

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.

Détails de l'opération

`GET /runningconfig/saved`

Il n'existe aucun paramètre pour cette opération.

`POST /runningconfig/save`

Il n'existe aucun paramètre pour cette opération.

`GET /runningconfig`

Spécifiez les paramètres suivants.

`section:` ***Corde***
(Facultatif) (Facultatif) Section spécifique du fichier de configuration en cours d'exécution que vous souhaitez récupérer.

`PUT /runningconfig`

Spécifiez les paramètres suivants.

`body:` ***Corde***
(Facultatif) Le fichier de configuration en cours d'exécution.

Logiciel

Vous pouvez consulter la liste des logiciels que le système ExtraHop a observés sur votre réseau.

Fonctionnement	Descriptif
GET /logiciel	Récupérez le logiciel observé par le système ExtraHop.
GET /software/ {id}	Récupérez les logiciels observés par le système ExtraHop par identifiant.

Détails de l'opération

`GET /software`

Spécifiez les paramètres suivants.

`software_type:` ***Corde***
(Facultatif) Type de logiciel.

`name:` ***Corde***
(Facultatif) Le nom du logiciel.

`version:` ***Corde***
(Facultatif) Version du logiciel.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

`GET /software/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique du logiciel.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

Clé de déchiffrement TLS

Cette ressource vous permet d'ajouter une clé de déchiffrement pour votre trafic réseau.

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

opération	Descriptif
GET /ssldecryptkeys	Récupérez toutes les clés de déchiffrement TLS.
Clés de déchiffrement POST /ssl	Créez une nouvelle clé de déchiffrement TLS.
SUPPRIMER /ssldecryptkeys/ {id}	Supprimez une clé TLS du système ExtraHop.
GET /ssldecryptkeys/ {id}	Récupérez un PEM TLS et des métadonnées.
PATCH /ssldecryptkeys/ {id}	Mettez à jour une clé de déchiffrement TLS existante.
GET /ssldecryptkeys/ {id} /protocols	Tout récupérer protocoles attribué à une clé de déchiffrement TLS.
POST /ssldecryptkeys/ {id} /protocoles	Créez un nouveau protocole pour une clé de déchiffrement TLS.
SUPPRIMER /ssldecryptkeys/ {id} /protocols/ {protocol}	Supprimez un protocole d'une clé de déchiffrement TLS.

Détails de l'opération

`GET /ssldecryptkeys`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cert_pem": "string",
    "enabled": true,
    "id": "string",
    "name": "string"
}
```

`POST /ssldecryptkeys`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Définissez les valeurs de propriété spécifiées sur la nouvelle clé de déchiffrement SSL.

`enabled:` ***Booléen***

Indiquez si cette clé de déchiffrement SSL est active.

`name:` ***Corde***

Nom convivial de la clé de déchiffrement SSL.

`certificate:` ***Corde***

Le certificat SSL associé à cette clé de déchiffrement.

`private_key:` ***Corde***

La clé privée SSL qui déchiffre le trafic.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "certificate": "string",
    "enabled": true,
    "name": "string",
    "private_key": "string"
```

```
}
```

`PATCH /ssldecryptkeys/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour de propriétés spécifiées à la clé de déchiffrement SSL.

`id:` ***Corde***
Représentation hexadécimale du hachage SHA-1 de la clé de déchiffrement SSL. La chaîne ne doit pas inclure de délimiteurs.

`GET /ssldecryptkeys/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Représentation hexadécimale du hachage SHA-1 de la clé de déchiffrement SSL. La chaîne ne doit pas inclure de délimiteurs.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "cert_pem": "string",
    "enabled": true,
    "id": "string",
    "name": "string"
}
```

`DELETE /ssldecryptkeys/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Représentation hexadécimale du hachage SHA-1 de la clé de déchiffrement SSL. La chaîne ne doit pas inclure de délimiteurs.

`GET /ssldecryptkeys/{id}/protocols`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Représentation hexadécimale du hachage SHA-1 de la clé de déchiffrement SSL. La chaîne ne doit pas inclure de délimiteurs.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "port": 0,
    "protocol": "string"
}
```

`POST /ssldecryptkeys/{id}/protocols`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Le corps du protocole.

`protocol:` ***Corde***

Le nom du protocole, en minuscules.

`port:` ***Numéro***

Port dans lequel écouter le trafic.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "port": 0,
    "protocol": "string"
}
```

`id:` ***Corde***

Identifiant unique de la clé de déchiffrement SSL.

`DELETE /ssldecryptkeys/{id}/protocols/{protocol}`

Spécifiez les paramètres suivants.

`protocol:` ***Corde***

Le nom du protocole, en minuscules.

`id:` ***Corde***

Représentation hexadécimale du hachage SHA-1 de la clé de déchiffrement SSL. La chaîne ne doit pas inclure de délimiteurs.

`port:` ***Numéro***

(Facultatif) Supprimez uniquement les protocoles assignés sur ce port.

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.

Détails de l'opération

`GET /supportpacks/queue/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du pack de support en cours d'exécution.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "created_time": 0,
    "filename": "string",
    "size": "string"
}
```

`GET /supportpacks/{filename}`

Spécifiez les paramètres suivants.

`filename:` ***Corde***
Nom du pack de support à télécharger.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "created_time": 0,
    "filename": "string",
    "size": "string"
}
```

`POST /supportpacks/execute`

`GET /supportpacks`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "created_time": 0,
    "filename": "string",
    "size": "string"
}
```

`POST /supportpacks`

Spécifiez les paramètres suivants.

`file:` ***Nom du fichier***
Nom du fichier du pack de support.

Tag

Les balises d'appareil vous permettent d'associer un équipement ou un groupe d'appareils en fonction de certaines caractéristiques.

Par exemple, vous pouvez étiqueter tous vos HTTP serveurs ou balisez tous les appareils qui se trouvent dans un sous-réseau commun. Pour plus d'informations, voir Marquer un équipement via l'API REST.

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

Fonctionnement	Descriptif
OBTENIR /tags	Récupérez tous les tags.
POSTER /tags	Créez un nouveau tag.

Fonctionnement	Descriptif
SUPPRIMER /tags/ {id}	Supprimez un tag spécifique.
OBTENEZ /tags/ {id}	Récupérez un tag spécifique.
PATCH /tags/ {id}	Appliquez les mises à jour à une balise spécifique.
GET /tags/ {id} /appareils	Récupérez tous les appareils associés à une étiquette spécifique.
POST /tags/ {id} /appareils	Attribuez et annulez l'attribution d'une balise spécifique aux appareils.
SUPPRIMER /tags/ {id} /devices/ {child-id}	Annuler l'attribution à un équipement d'une balise spécifique.
POST /tags/ {id} /appareils/ {child id}	Attribuez un tag spécifique à un équipement.

Détails de l'opération

`GET /tags`

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "id": 0,
    "mod_time": 0,
    "name": "string"
}
```

`POST /tags`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées à la nouvelle balise.

`name:` ***Corde***

La valeur de chaîne de la balise.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "name": "string"
}
```

`GET /tags/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la balise.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "id": 0,
    "mod_time": 0,
    "name": "string"
```

```
}
```

`DELETE /tags/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de la balise.

`PATCH /tags/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour des valeurs de propriété spécifiées à la balise.

`id:` ***Numéro***
Identifiant unique de la balise.

`GET /tags/{id}/devices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de la balise.

`POST /tags/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Listes d'identifiants uniques que l'équipement doit attribuer ou non.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
Identifiant unique de la balise.

`POST /tags/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'équipement.

`id:` ***Numéro***
l'identifiant unique du tag.

```
DELETE /tags/{id}/devices/{child-id}
```

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique de l'équipement.

`id:` ***Numéro***
Identifiant unique de la balise.

Collecte des menaces

La ressource Threat Collection vous permet de télécharger gratuitement et à des fins commerciales collections de menaces proposé par la communauté de sécurité à votre système RevealX.

Important: Les téléchargements de fichiers STIX sont désormais obsolètes et la date de suppression est prévue pour mars 2025.

- Vous devez télécharger des collections de menaces individuellement vers votre appliance Command ou RevealX 360, et vers tous les appareils connectés capteurs.
- Les collections de menaces personnalisées doivent être formatées dans STIX (Structured Threat Information Expression) sous forme de fichiers TAR.GZ. RevealX prend actuellement en charge les versions 1.0 à 1.2 de STIX.
- Le nombre maximum d'observables qu'une collecte des menaces peut contenir dépend de votre plate-forme et de votre licence. Contactez votre représentant ExtraHop pour plus d'informations.

Note: Cette rubrique s'applique uniquement à ExtraHop RevealX Premium et Ultra.

Pour plus d'informations sur le téléchargement de fichiers STIX via le système ExtraHop, voir Téléchargez des fichiers STIX via l'API REST.

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

opération	Descriptif
GET /ThreatCollections	Récupérez toutes les collections de menaces.
Collections POST et menaces	Créez une nouvelle collecte des menaces.
SUPPRIMER /threatcollections/ {id}	Supprimez une collecte des menaces.
PUT /threatcollections/ {id}	Téléchargez une nouvelle collecte des menaces. ExtraHop prend actuellement en charge les versions 1.0 à 1.2 de STIX. **Note:** Si une collecte des menaces portant le même nom existe déjà sur le système ExtraHop, la collecte des menaces existante est remplacée.
GET /threatcollections/ {id} /observables	Récupérez le nombre d'observables STIX chargés à partir d'une collecte des menaces, tels que l' adresse IP, le nom d'hôte ou l'URI.

Détails de l'opération

```
GET /threatcollections
```

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "id": 0,
    "last_updated": 0,
    "name": "string",
    "observables": 0,
    "user_key": "string"
}
```

`POST /threatcollections`

Spécifiez les paramètres suivants.

`user_key:` ***Corde***
(Facultatif) Identifiant fourni par l'utilisateur pour la collecte des menaces. Si ce paramètre n'est pas spécifié, le nom de la collecte des menaces est défini pour cette valeur, sans espaces ni ponctuation.

`name:` ***Corde***
Nom de la collecte des menaces.

`file:` ***Nom du fichier***
Le nom de fichier de la collecte des menaces.

`PUT /threatcollections/~{userKey}`

Spécifiez les paramètres suivants.

`userKey:` ***Corde***
Identifiant fourni par l'utilisateur pour la collecte des menaces.

`name:` ***Corde***
(Facultatif) Nom de la collecte des menaces.

`file:` ***Nom du fichier***
(Facultatif) Nom du fichier pour la collecte des menaces.

`DELETE /threatcollections/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique pour la collecte des menaces.

`GET /threatcollections/{id}/observables`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique pour la collecte des menaces.

Gâchette

Les déclencheurs sont des scripts personnalisés qui exécutent une action lors d'un événement prédéfini.

Par exemple, vous pouvez créer un déclencheur pour enregistrer une métrique personnalisée chaque fois qu'un HTTP une requête se produit ou classe le trafic pour un serveur particulier en tant que serveur d'applications. Pour plus d'informations, consultez le Référence de l'API Trigger. Pour des notes de mise en œuvre supplémentaires concernant les options avancées, voir Options de déclencheur avancées.

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

opération	Descriptif
GET /triggers	Récupérez tous les déclencheurs.
POST /déclencheurs	Créez un nouveau déclencheur.
POST/déclencheurs/données externes	Envoie des données à l'API Trigger en exécutant l'événement EXTERNAL_DATA. Vous pouvez accéder aux données via ExternalData classe de déclencheur. **Note:** Cette opération n'est pas disponible pour les appliances Command ou RevealX 360.
SUPPRIMER /triggers/ {id}	Supprimez un identifiant spécifique.
GET /triggers/ {id}	Récupérez un déclencheur spécifique par identifiant unique.
PATCH /triggers/ {id}	Mettez à jour un déclencheur existant.
GET /triggers/ {id} /devicegroups	Récupérez tout groupes d'équipements qui sont affectés à un déclencheur spécifique.
POST /triggers/ {id} /devicegroups	Attribuez et annulez l'attribution d'un déclencheur spécifique à des groupes d'équipements.
SUPPRIMER /triggers/ {id} /devicegroups/ {child-id}	Annulez l'attribution d'un groupe dveloppements à un déclencheur spécifique.
POST /triggers/ {id} /devicegroups/ {childid}	Assignez un groupe dproximatif d'équipements à un déclencheur spécifique.
GET /triggers/ {id} /appareils	Récupérez tous les appareils affectés à un déclencheur spécifique.
POST /triggers/ {id} /appareils	Attribuez et annulez l'attribution d'un déclencheur spécifique aux appareils.
SUPPRIMER /triggers/ {id} /devices/ {child-id}	Annulez l'attribution d'un équipement à un déclencheur spécifique.
POST /triggers/ {id} /devices/ {childid}	Assignez un équipement à un déclencheur spécifique.

Détails de l'opération

`GET /triggers`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
```

```
    ],
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`DELETE /triggers/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`POST /triggers/externaldata`

Spécifiez les paramètres suivants.

`body:` ***Objet***
L'objet contenant les données à envoyer aux déclencheurs via l'événement EXTERNAL_DATA.

`type:` ***Corde***
Identifiant de chaîne qui décrit les données contenues dans le paramètre body. Par exemple, vous pouvez spécifier « phantom-data » pour les données envoyées depuis la plateforme Phantom SOAR.

`body:` ***Objet***
Les données à envoyer aux déclencheurs via l'événement EXTERNAL_DATA. Ces données sont accessibles dans le déclencheur à l'aide de la propriété « ExternalData.body ».

Spécifiez le paramètre body au format JSON suivant.

```
{
    "body": {},
    "type": "string"
}
```

`POST /triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les valeurs des propriétés du nouveau déclencheur.

`name:` ***Corde***
Le nom convivial du déclencheur.

`description:` ***Corde***
(Facultatif) Description facultative du déclencheur.

`author:` ***Corde***
Le nom du créateur du déclencheur.

`script:` ***Corde***
Le contenu JavaScript du déclencheur.

`event:` ***Corde***
(Facultatif) Obsolète. Remplacé par le champ des événements.

`events:` ***Tableau de cordes***

La liste des événements sur lesquels le déclencheur s'exécute, exprimée sous forme de tableau JSON.

`disabled:` ***Booléen***

Indique si le déclencheur peut être exécuté.

`debug:` ***Booléen***

Indique si les instructions de débogage sont imprimées pour le déclencheur.

`apply_all:` ***Booléen***

Indique si le déclencheur s'applique à toutes les ressources pertinentes.

`hints:` ***Objet***

Options basées sur les événements déclencheurs sélectionnés. Pour plus d'informations sur l'objet hints, consultez Guide de l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
    "hints": {},
    "name": "string",
    "script": "string"
}
```

`PATCH /triggers/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La valeur de la propriété est mise à jour pour le déclencheur.

`id:` ***Numéro***

Identifiant unique du déclencheur.

`GET /triggers/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du déclencheur.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
```

```
    ],
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`GET /triggers/{id}/devicegroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`POST /triggers/{id}/devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Liste d'identifiants uniques pour les groupes d'équipements affectés et non attribués à un déclencheur.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
Identifiant unique du déclencheur.

`POST /triggers/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`DELETE /triggers/{id}/devicegroups/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`GET /triggers/{id}/devices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`POST /triggers/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Liste d'identifiants uniques pour les appareils qui sont attribués et non affectés à un déclencheur.

`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer

`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

`id:` ***Numéro***
Identifiant unique du déclencheur.

`POST /triggers/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique de l'équipement.

`id:` ***Numéro***
Identifiant unique du déclencheur.

`DELETE /triggers/{id}/devices/{child-id}`

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique de l'équipement.

`id:` ***Numéro***
Identifiant unique du déclencheur.

Options de déclencheur avancées

Les options de déclenchement avancées sont des options de configuration que vous pouvez définir en fonction des événements système associés au déclencheur. Par exemple, vous pouvez configurer le nombre d' octets de charge utile sur lesquels mettre en mémoire tampon HTTP demander des événements.

Les options avancées sont contenues dans le `hints` objet de la ressource déclencheur, comme indiqué dans l'exemple suivant :

```
"hints": {
"flowClientPortMin": null,
"flowClientBytes": 16384,
```

```
"flowClientPortMax": null,
"flowServerBytes": 16384,
"flowPayloadTurn": true,
"flowServerPortMin": 135,
"flowServerPortMax": 49155
}
```

Le tableau suivant décrit les options avancées disponibles et les événements applicables :

Option	Descriptif	Évènements applicables
`"snaplen": number`	Spécifie le nombre d'octets à capturer par paquet, jusqu'à un maximum de 65535. La capture commence par le premier octet du paquet. Spécifiez cette option uniquement si le script du déclencheur capture des paquets. Une valeur de `0` configure le déclencheur pour capturer le nombre maximum d'octets pour chaque paquet.	Tous les événements sauf : • ALERT_RECORD_COMMIT • METRIC_CYCLE_BEGIN • METRIC_CYCLE_END • FLOW_REPORT • NOUVELLE_APPLICATION • NOUVEL_APPAREIL • EXPIRATION DE SESSION
`"payloadBytes": number`	Spécifie le nombre minimal d'octets de charge utile à mettre en mémoire tampon.	• REQUÊTE_CIFS • CIFS_RESPONSE • REQUÊTE_HTTP • HTTP_RESPONSE • ICA_TICK
`"clipboardBytes": number`	Spécifie le nombre d'octets à mettre en mémoire tampon lors d'un transfert dans le presse-papiers Citrix.	• ICA_TICK
`"cycle": [30sec, 5min, 1hr, 24hr]`	Spécifie la durée du cycle métrique, exprimée en secondes.	• METRIC_CYCLE_BEGIN • METRIC_CYCLE_END • METRIC_RECORD_COMMIT
`"metricTypes": string`	Spécifie le type de métrique par le nom brut de la métrique, tel que extrahop.device.http_server.	• ALERT_RECORD_COMMIT • METRIC_RECORD_COMMIT
`"flowPayloadTurn": boolean`	Active la capture de paquets à chaque tour de flux. L'analyse par tour analyse en permanence la communication entre deux points de terminaison pour extraire un seul point de données de charge utile du flux. Si cette option est activée, toutes les valeurs spécifiées pour `flowClientString` et `flowServerString` les options sont ignorées.	• CHARGE UTILE SSL_ • TCP_PAYLOAD

Option	Descriptif	Évènements applicables
`"flowClientPortMin": number`	Spécifie le numéro de port minimal du client plage de ports. Les valeurs valides sont `0` pour `65535`. Une valeur de `0` spécifie la correspondance de n'importe quel port.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD
`"flowClientPortMax": number`	Spécifie le numéro de port maximal du client plage de ports. Les valeurs valides sont `0` pour `65535`. Toute valeur spécifiée pour cette option est ignorée si la valeur de `flowClientPortMin` l'option est `0`.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD
`"flowClientBytes": number`	Spécifie le nombre de client octets dans la mémoire tampon. La valeur de cette option ne peut pas être définie sur `0` si la valeur de `flowServerBytes` l'option est également définie sur `0`.	• CHARGE UTILE SSL_ • TCP_PAYLOAD
`"flowClientString": string`	Spécifie la chaîne de format de client données à traiter. Toute valeur spécifiée pour cette option est ignorée si `flowPayloadTurn` l'option est activée.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD
`"flowServerPortMin": number`	Spécifie le numéro de port minimal de la plage de ports du serveur. Les valeurs valides sont `0` au `65535`. Une valeur de `0` spécifie la correspondance de n'importe quel port.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD
`"flowServerPortMax": number`	Spécifie le numéro de port maximal de la plage de ports du serveur. Les valeurs valides sont `0` pour `65535`. Toute valeur spécifiée pour cette option est ignorée si la valeur de `flowServerPortMin` l'option est `0`.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD

Option	Descriptif	Évènements applicables
`"flowServerBytes": number`	Spécifie le nombre d'octets du serveur à mettre en mémoire tampon. La valeur de cette option ne peut pas être définie sur `0` si la valeur du `flowClientBytes` l'option est également définie sur `0`.	• CHARGE UTILE SSL_ • TCP_PAYLOAD
`"flowServerString": string`	Spécifie la chaîne de format des données du serveur à traiter. Renvoie le paquet entier en cas de correspondance d'une chaîne. Toute valeur spécifiée pour cette option est ignorée si `flowPayloadTurn` l'option est activée.	• CHARGE UTILE SSL_ • TCP_PAYLOAD • UDP_PAYLOAD
`"flowUdpAll": boolean`	Permet la capture de tous les datagrammes UDP.	• UDP_PAYLOAD
`"fireClassifyOnExpiration": boolean`	Permet d'exécuter l'événement à son expiration afin d'accumuler des métriques pour les flux qui n'ont pas été classés avant leur expiration.	• FLOW_CLASSIFY

Utilisateur

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

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

opération	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 d'un utilisateur spécifique.
GET /users/ {nom d'utilisateur} /apikeys/ {keyid}	Récupérez des informations sur une clé d'API et un utilisateur spécifiques.
SUPPRIMER /users/ {username} /lock	Déverrouillez un compte utilisateur spécifique.
GET /users/ {nom d'utilisateur} /lock	Récupérez l'état de verrouillage d'un compte utilisateur spécifique.

Détails de l'opération

`GET /users`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "date_joined": "string",
    "effective_roles": {},
    "eh_account_team": true,
    "enabled": true,
    "granted_roles": {},
    "last_ui_login_time": "string",
    "name": "string",
    "type": "string",
    "username": "string"
}
```

`POST /users`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres du compte utilisateur.

`enabled:` ***Booléen***

(Facultatif) Indique si l'utilisateur peut se connecter au système ExtraHop.

`name:` ***Corde***

Le nom convivial de l'utilisateur.

`username:` ***Corde***

Le nom de connexion de l'utilisateur.

`password:` ***Corde***

Le mot de passe de l'utilisateur. Les mots de passe doivent répondre aux exigences configurées dans les paramètres d'administration.

`granted_roles:` ***Objet***

(Facultatif) Les privilèges de l'utilisateur. Les niveaux d'autorisation pris en charge sont décrits dans Guide de l'API REST.

`create_apikey:` ***Booléen***

(Facultatif) Générez et renvoyez une nouvelle clé API pour l'utilisateur créé.

`type:` ***Corde***

(Facultatif) La méthode dauthentification utilisée par cet utilisateur pour se connecter.

Les valeurs suivantes sont valides :

- `local`
- `remote`

`eh_account_team:` ***Booléen***

Indique un utilisateur de l'équipe ExtraHop Account qui accède au système ExtraHop via ExtraHop Cloud Services.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "create_apikey": true,
```

```
    "eh_account_team": true,
    "enabled": true,
    "granted_roles": {},
    "name": "string",
    "password": "string",
    "type": "string",
    "username": "string"
}
```

`GET /users/{username}`

Spécifiez les paramètres suivants.

`username:` ***Corde***

Le nom de l'utilisateur.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "date_joined": "string",
    "effective_roles": {},
    "eh_account_team": true,
    "enabled": true,
    "granted_roles": {},
    "last_ui_login_time": "string",
    "name": "string",
    "type": "string",
    "username": "string"
}
```

`PATCH /users/{username}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres du compte utilisateur.

`enabled:` ***Booléen***

(Facultatif) Indique si l'utilisateur peut se connecter au système ExtraHop.

`name:` ***Corde***

(Facultatif) Le nom convivial de l'utilisateur.

`password:` ***Corde***

(Facultatif) Le mot de passe de l'utilisateur. Les mots de passe doivent répondre aux exigences configurées dans les paramètres d'administration.

`granted_roles:` ***Objet***

(Facultatif) Les privilèges de l'utilisateur. Les niveaux d'autorisation pris en charge sont décrits dans Guide de l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "enabled": true,
    "granted_roles": {},
    "name": "string",
    "password": "string"
}
```

`username:` ***Corde***
Le nom de l'utilisateur.

`DELETE /users/{username}`

Spécifiez les paramètres suivants.

`username:` ***Corde***
Le nom de l'utilisateur.

`dest_user:` ***Corde***
(Facultatif) L'utilisateur auquel les personnalisations sont transférées. Si ce paramètre est spécifié, tous les tableaux de bord, collections et cartes d'activité appartenant à l'utilisateur supprimé sont transférés à cet utilisateur.

`GET /users/{username}/lock`

Spécifiez les paramètres suivants.

`username:` ***Corde***
Le nom de connexion de l'utilisateur.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "is_locked": true,
    "lockout_expiration": 0
}
```

`DELETE /users/{username}/lock`

Spécifiez les paramètres suivants.

`username:` ***Corde***
Le nom de connexion de l'utilisateur.

`GET /users/{username}/apikeys`

Spécifiez les paramètres suivants.

`username:` ***Corde***
Le nom de l'utilisateur.

`GET /users/{username}/apikeys/{keyid}`

Spécifiez les paramètres suivants.

`keyid:` ***Corde***
L'ID de la clé API.
`username:` ***Corde***
Le nom de l'utilisateur.

Groupe d'utilisateurs

La ressource des groupes d'utilisateurs vous permet de gérer et de mettre à jour des groupes d'utilisateurs et leurs associations de partage de tableaux de bord.

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

Fonctionnement	Descriptif
GET /groupes d'utilisateurs	Récupérez tous les groupes d'utilisateurs.
POST/groupes d'utilisateurs	Créez un nouveau groupe d'utilisateurs.
POST /groupes d'utilisateurs/rafraîchir	Interrogez le LDAP pour connaître les adhésions les plus récentes pour tous les groupes d'utilisateurs distants.
SUPPRIMER /usergroups/ {id}	Supprimez un groupe d'utilisateurs spécifique.
OBTENEZ /usergroups/ {id}	Récupérez un groupe d'utilisateurs spécifique.
PATCH /usergroups/ {id}	Mettez à jour un groupe d'utilisateurs spécifique.
SUPPRIMER /usergroups/ {id} /associations	Supprimez toutes les associations de partage de tableau de bord avec un groupe d'utilisateurs spécifique.
GET /usergroups/ {id} /membres	Récupérez tous les membres d'un groupe d'utilisateurs spécifique.
PATCH /usergroups/ {id} /membres	Attribuez ou annulez l'attribution d'utilisateurs à un groupe d'utilisateurs.
PUT /usergroups/ {id} /membres	Remplacez les attributions de groupes d'utilisateurs.
POST /usergroups/ {id} /rafraîchir	Interrogez LDAP pour connaître l'appartenance la plus récente à un groupe d'utilisateurs distants spécifique.

Détails de l'opération

`GET /usergroups`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "display_name": "string",
    "enabled": true,
    "id": "string",
    "is_remote": true,
    "last_sync_time": 0,
    "name": "string",
    "rights": []
}
```

`POST /usergroups`

Spécifiez les paramètres suivants.

`body` : ***Objet***

Les propriétés du groupe d'utilisateurs.

`name` : ***Corde***

Le nom du groupe d'utilisateurs.

`enabled:` ***Booléen***

Indique si le groupe d'utilisateurs est activé.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "enabled": true,
    "name": "string"
}
```

`PATCH /usergroups/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La valeur de la propriété est mise à jour pour le groupe d'utilisateurs spécifique.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

`GET /usergroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "display_name": "string",
    "enabled": true,
    "id": "string",
    "is_remote": true,
    "last_sync_time": 0,
    "name": "string",
    "rights": []
}
```

`DELETE /usergroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

`DELETE /usergroups/{id}/associations`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

`GET /usergroups/{id}/members`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "users": {}
}
```

`POST /usergroups/refresh`

Il n'existe aucun paramètre pour cette opération.

`POST /usergroups/{id}/refresh`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique du groupe d'utilisateurs.

`PATCH /usergroups/{id}/members`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique du groupe d'utilisateurs.

`body:` ***Corde***
Objet qui spécifie les utilisateurs à affecter ou à annuler. Chaque clé doit être un nom d'utilisateur et chaque valeur doit être « membre » ou nulle. Par exemple, {"Alice » : « member », « Bob » : null} assigne Alice au groupe et retire Bob du groupe.

`PUT /usergroups/{id}/members`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique du groupe d'utilisateurs.

`body:` ***Corde***
Objet qui spécifie quels utilisateurs sont affectés au groupe. Chaque clé doit être un nom d'utilisateur et chaque valeur doit être « membre ». Par exemple, {"Alice » : « member », « Bob » : « member"} désigne Alice et Bob comme seuls membres du groupe.

VLAN

Les réseaux locaux virtuels sont des groupements logiques de trafic ou de périphériques sur le réseau.

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

Fonctionnement	Descriptif
GET /vlan	Récupérez tous les VLAN
OBTENEZ /vlans/ {id}	Récupérez un VLAN spécifique.
PATCH /vlans/ {id}	Mettez à jour un VLAN spécifique.

Détails de l'opération

`GET /vlans`

Il n'existe aucun paramètre pour cette opération.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`GET /vlans/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du VLAN.

Si la demande aboutit, le système ExtraHop renvoie un objet au format suivant.

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`PATCH /vlans/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour des valeurs de propriété spécifiées au VLAN.

`id:` ***Numéro***
Identifiant unique du VLAN.

Liste de surveillance

Pour garantir qu'un actif, tel qu'un serveur important, une base de données ou un ordinateur portable, bénéficie de la garantie Analyse avancée, vous pouvez ajouter cet équipement à la liste de surveillance.

Conseil: Si vous souhaitez ajouter plusieurs appareils à la liste de surveillance, pensez à créer un groupe d' appareils, puis à donner la priorité à ce groupe pour Analyse avancée.

Voici quelques considérations importantes concernant la liste de surveillance :

- La liste de surveillance s'applique uniquement à l'Analyse avancée.
- La liste de surveillance peut contenir autant d'appareils que le permet la capacité d'Analyse avancée, qui est déterminée par votre licence.

- Un équipement reste sur la liste de surveillance, qu'il soit inactif ou actif. Un équipement doit être actif pour que le système ExtraHop collecte les métriques d'Analyse avancée.

Pour plus d'informations sur l'Analyse avancée, voir Niveaux d'analyse.

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

Opération	Descriptif
SUPPRIMER /watchlist/device/ {id}	Supprimer un équipement de la liste de surveillance.
POST /watchlist/device/ {id}	Ajoutez un équipement à la liste de surveillance.
GET /watchliste/appareils	Récupérez tous les appareils figurant dans la liste de surveillance.
POST/liste de surveillance/appareils	Ajoutez ou supprimez des appareils de la liste de surveillance.

Détails de l'opération

`GET /watchlist/devices`

Il n'existe aucun paramètre pour cette opération.

`POST /watchlist/device/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de l'équipement.

`DELETE /watchlist/device/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de l'équipement.

`POST /watchlist/devices`

Spécifiez les paramètres suivants.

`assignments:` ***Objet***
Liste des appareils à ajouter ou à supprimer de la liste de surveillance.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre d'assignation au format JSON suivant.

```
{
    "assign": [],
    "unassign": []
}
```

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
- Extraire 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 RevealX 360 . Pour exécuter ce script avec RevealX 360, vous devez le modifier 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 TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `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}"
```

Modifier le propriétaire d'un tableau de bord via l'API REST

Les tableaux de bord appartiennent à l'utilisateur connecté qui les a créés. Si un utilisateur ne fait plus partie de votre entreprise, il se peut que vous deviez changer le propriétaire du tableau de bord pour le maintenir à jour.

Pour transférer la propriété d'un tableau de bord, vous avez besoin de l'ID du tableau de bord et du nom d'utilisateur du propriétaire du tableau de bord. Vous pouvez uniquement consulter le nom d'utilisateur du propriétaire d'un tableau de bord via l'API REST.

Avant de commencer

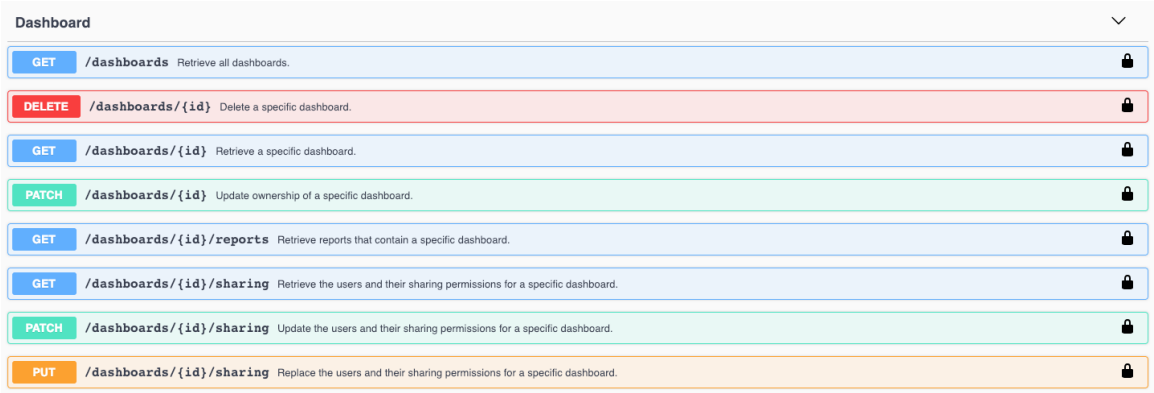
- Pour les capteurs et la console ExtraHop, vous devez disposer d'une clé API valide avec administration du système et des accès privilèges ou supérieur. (Voir Générer une clé API).
- Pour RevealX 360, vous devez disposer d'informations d'identification d'API REST valides auprès de l'administration du système et des accès privilèges ou supérieur. (Voir Création d'informations d'identification pour l'API REST).
- Familiarisez-vous avec les Guide de l'API REST ExtraHop pour savoir comment naviguer dans l'explorateur d'API REST ExtraHop.

Récupérez les identifiants du tableau de bord

1. Dans un navigateur, accédez à l'explorateur d'API REST.

L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.

2. Entrez les informations dcessitude d'identification de votre API REST.
   - Pour les capteurs et la console ExtraHop, cliquez sur **Entrez la clé API** puis collez ou saisissez votre clé API dans **Clé API** champ.
   - Pour RevealX 360, cliquez sur **Entrez les identifiants de l'API** puis collez ou saisissez l'ID et le code secret de vos informations diciatives d'API dans le **IDENTIFIANT** et **Secret** champs.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **Tableau de bord** pour afficher les opérations du tableau de bord.



5. Cliquez **GET /tableaux de bord**.
6. Cliquez **Essayez-le** puis cliquez sur **Envoyer la demande** pour envoyer la demande à votre sonde ou à votre console.
7. Recherchez les tableaux de bord à l'aide du nom du tableau de bord ou du compte utilisateur répertorié dans `"owner"` champ. Si votre liste de tableaux de bord est longue, vous pouvez appuyer sur Ctrl+f et rechercher le corps de la réponse.
   Pour notre exemple, nous voulons modifier le `"LDAP Server Health"` tableau de bord créé par le compte utilisateur pour `"marksmith"`:

```
{
    "id": 1876,
    "comment": null,
    "mod_time": 1507576983922,
    "author": "Mark Smith",
    "name": "LDAP Server Health",
    "owner": "marksmith",
    "built-in": false,
    "short_code": "MpXgk",
    "rights": [
      "transfer",
      "view",
      "edit",
      "share",
      "delete"
    ]
}
```

8. Notez le numéro dans `"id"` champ pour chaque tableau de bord que vous souhaitez modifier.

Changer le propriétaire du tableau de bord

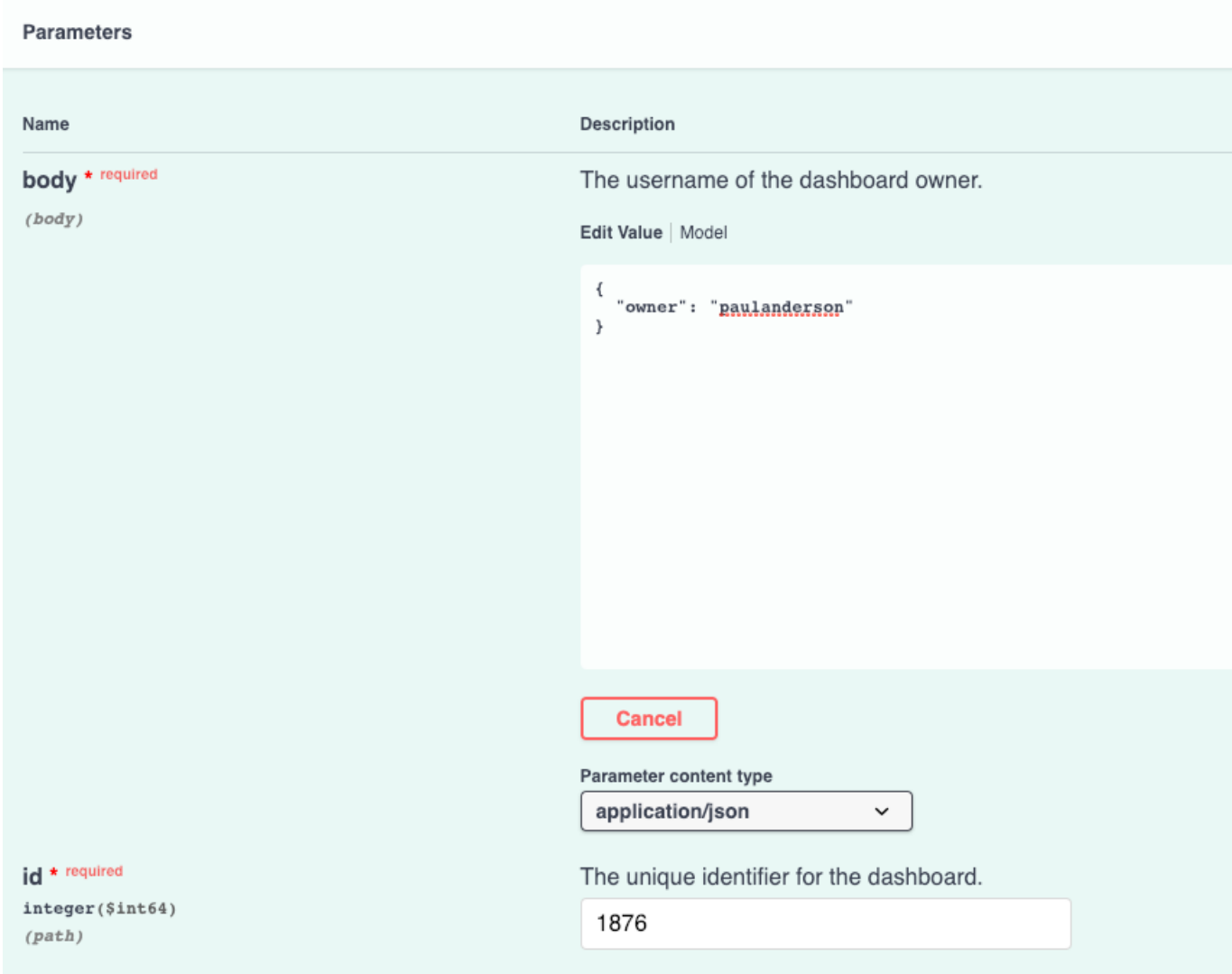
1. Faites défiler la page des opérations du tableau de bord vers le bas jusqu'à la section /dashboards/ {id}.
2. Cliquez **PATCH /tableaux de bords/ {id}**.
3. Cliquez **Essayez-le**.

Le schéma JSON est automatiquement ajouté à la zone de texte du paramètre du corps.

4. Dans la zone de texte du corps de texte, dans le `"owner"` champ, remplacez `string` avec le nom d'utilisateur du nouveau propriétaire.
5. Dans le **identifiant** champ, saisissez le numéro que vous avez noté précédemment pour le tableau de bord.

   Pour notre exemple, cette valeur est `1876`. (Vous ne pouvez modifier qu' un seul tableau de bord à la fois via l'explorateur d'API REST.)

   Dans la figure suivante, nous avons ajouté le JSON `"string"` pour le `"owner"` paramètre du corps zone de texte du paramètre, modifiée `"string"` à `"paulanderson"`, et saisi `"1876"` dans le identifiant champ.



6. Cliquez **Envoyer la demande** pour envoyer la demande à votre sonde ou à votre console.
   En dessous Réponse du serveur, le Code affichages de colonnes `204` si l' opération est réussie. Vous pouvez cliquer **GET /tableaux de bord** à nouveau pour vérifier que `"owner"` le champ a changé. Notez que vous ne pouvez modifier que le propriétaire du tableau de bord. Vous ne pouvez pas modifier le nom du tableau de bord ni les champs d'auteur via l'API REST.

   Le tableau de bord est désormais disponible sous **Mes tableaux de bord** dans le système ExtraHop pour le nouvel utilisateur. En tant que nouveau propriétaire, vous pouvez désormais vous connecter à votre système ExtraHop et modifier d'autres propriétés du tableau de bord, telles que le nom ou l'auteur du tableau de bord.

Conseil: Après avoir cliqué **Envoyer la demande**, l' explorateur d'API REST fournit des scripts pour les opérations dans Curl, Python 2.7 ou Ruby.

Exemple de script Python

Le référentiel GitHub d'ExtraHop contient un exemple de script Python qui recherche tous les tableaux de bord appartenant à un compte utilisateur sur un sonde ou console puis remplace le propriétaire de tous ces tableaux de bord par un autre compte utilisateur.

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 RevealX 360 . Pour exécuter ce script avec RevealX 360, vous devez le modifier 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.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `change_dashboard_owner/change_dashboard_owner.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `change_dashboard_owner.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
   - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console.
   - **CLÉ_API:** La clé d'API.
   - **ACTUEL:** Le nom d'utilisateur du propriétaire actuel du tableau de bord.
   - **NOUVEAU:** Le nom d'utilisateur du nouveau propriétaire du tableau de bord.
3. Exécutez la commande suivante :

```
python3 change_dashboard_owner.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `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)
```

Extraire la liste des équipements via l'API REST

L'API REST ExtraHop vous permet d'extraire la liste des appareils découverts par sonde ou console. En extrayant la liste à l'aide d'un script d'API REST, vous pouvez exporter la liste dans un format lisible par des applications tierces, comme une base de données de gestion des configurations (CMDB). Dans cette rubrique, nous montrons les méthodes permettant d'extraire une liste à la fois par le biais de la commande cURL et d'un script Python.

Avant de commencer

- Pour les capteurs et la console ExtraHop, vous devez disposer d'une clé API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir Générer une clé API).
- Pour RevealX 360, vous devez disposer d'informations d'identification d'API REST valides pour apporter des modifications via l' API REST et suivre les procédures ci-dessous. (Voir Création d'informations d'identification pour l'API REST).

Récupérez la liste des équipements à l'aide de la commande cURL

La liste des appareils inclut toutes les métadonnées de l'équipement, telles que les adresses MAC et les identifiants des appareils. Cependant, vous pouvez filtrer la liste des appareils à l'aide d'un analyseur JSON

pour extraire les informations spécifiques que vous souhaitez exporter. Dans cet exemple, la liste des équipements est récupérée puis filtrée avec l'analyseur jq pour extraire uniquement le nom d'affichage de chaque appareil.

Note: La procédure suivante n'est pas compatible avec l'API REST RevealX 360. Pour récupérer la liste des équipements depuis RevealX 360, voir Récupérez la liste des équipements depuis RevealX 360 à l'aide de la commande cURL.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- L'analyseur jq doit être installé sur votre machine. Pour plus d'informations, voir https://stedolan.github.io/jq/.

Ouvrez une application de terminal et exécutez la commande suivante, où `YOUR_KEY` est l'API de votre compte utilisateur, `HOSTNAME` est le nom d'hôte de votre sonde ou console, et `MAX_DEVICES` est un nombre suffisamment élevé pour être supérieur au nombre total de périphériques découverts par votre système :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --header
 "accept: application/json" --header "Authorization: ExtraHop
 apikey=YOUR_KEY" --header "Content-Type: application/json" -d
 "{ \"active_from\": 1, \"active_until\": 0, \"limit\": MAX_DEVICES}" |
 jq -r '.[] | .display_name'
```

Note: Si la commande ne renvoie aucun résultat, assurez-vous que un certificat fiable a été ajouté à votre système ExtraHop. Vous pouvez également ajouter `--insecure` option permettant de récupérer la liste des équipements à partir d'un système ExtraHop sans certificat fiable ; cependant, cette méthode n'est pas sécurisée et n'est pas recommandée.

Conseil: Vous pouvez ajouter `select(.analysis == "LEVEL")` option pour filtrer les résultats par niveau d'analyse. Par exemple, la commande suivante limite les résultats afin d'inclure uniquement les appareils sélectionnés pour une analyse avancée :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit\":
 1000000000}" | jq -r '.[] | select(.analysis == "advanced")
 | .display_name'
```

Conseil: Vous pouvez ajouter `select(.critical == BOOLEAN)` option pour filtrer les résultats en fonction du champ critique. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils identifiés comme critiques par le système ExtraHop :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit
\": 1000000000}" | jq -r '.[] | select(.critical == true)
 | .display_name'
```

Conseil: Vous pouvez ajouter `select(.cloud_instance_name != null)` option pour filtrer les résultats en fonction du champ de nom de l'instance cloud. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils dotés d'un nom d'instance cloud :

```
curl -s -X POST "https://HOSTNAME/api/v1/devices/search" --
header "accept: application/json" --header "Authorization:
```

```
 ExtraHop apikey=YOUR_KEY" --header "Content-Type: application/
json" -d "{ \"active_from\": 1, \"active_until\": 0, \"limit
\": 1000000000}" | jq -r '.[] | select(.cloud_instance_name !=
 null) | .cloud_instance_name'
```

Récupérez la liste des équipements depuis RevealX 360 à l'aide de la commande cURL

La liste des appareils inclut toutes les métadonnées de l'équipement, telles que les adresses MAC et les identifiants des appareils. Cependant, vous pouvez filtrer la liste des appareils à l'aide d'un analyseur JSON pour extraire les informations spécifiques que vous souhaitez exporter. Dans cet exemple, la liste des équipements est récupérée puis filtrée avec l'analyseur jq pour extraire uniquement le nom d'affichage de chaque appareil.

Note: La procédure suivante est uniquement compatible avec l'API REST RevealX 360. Pour récupérer la liste des équipements à partir des capteurs et de la console ExtraHop, voir Récupérez la liste des équipements à l'aide de la commande cURL.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- L'analyseur jq doit être installé sur votre machine. Pour plus d'informations, voir https://stedolan.github.io/jq/.

1. Ouvrez une application de terminal et exécutez la commande suivante, où `REVEAL_X_360_REST_API` est le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché dans RevealX 360 sur l'accès à l'API page sous API Endpoint. Le nom d'hôte n'inclut pas `/oauth2/token`:

```
HOST="https://REVEAL_X_360_REST_API"
```

2. Exécutez la commande suivante, où `YOUR_ID` est l'ID des informations dcessatives d'identification de l'API REST :

```
ID="YOUR_ID"
```

3. Exécutez la commande suivante, où `YOUR_SECRET` est le secret des informations dcessaires d'identification de l'API REST :

```
SECRET="YOUR_SECRET"
```

4. Exécutez la commande suivante :

```
AUTH=$(printf "$ID:$SECRET" | base64 --wrap=0)
```

5. Exécutez la commande suivante :

```
ACCESS_TOKEN=$(curl -s \
    -H "Authorization: Basic ${AUTH}" \
    -H "Content-Type: application/x-www-form-urlencoded" \
    --request POST \
     ${HOST}/oauth2/token \
    -d "grant_type=client_credentials" \
    | jq -r '.access_token')
```

6. Exécutez la commande suivante, où `MAX_DEVICES` est un nombre suffisamment élevé pour être supérieur au nombre total de périphériques découverts par votre système :

```
curl -s -X GET -H "Authorization: Bearer ${ACCESS_TOKEN}"  "$HOST/api/
v1/devices?active_from=1&active_until=0&limit=MAX_DEVICES" | jq -r '.[]
 | .display_name'
```

Conseil Vous pouvez ajouter `select(.analysis == "LEVEL")` option pour filtrer les résultats par niveau d'analyse. Par exemple, la commande suivante limite les résultats afin d' inclure uniquement les appareils sélectionnés pour une analyse avancée :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000" | jq -r '.[] |
 select(.analysis == "advanced") | .display_name'
```

Conseil Vous pouvez ajouter `select(.critical == BOOLEAN)` option pour filtrer les résultats en fonction du champ critique. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils identifiés comme critiques par le système ExtraHop :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000"  | jq -r '.[] |
 select(.critical == true) | .display_name'
```

Conseil Vous pouvez ajouter `select(.cloud_instance_name != null)` option pour filtrer les résultats en fonction du champ de nom de l'instance cloud. Par exemple, la commande suivante limite les résultats pour inclure uniquement les appareils dotés d'un nom d'instance cloud :

```
curl -s -X GET -H "Authorization: Bearer
 ${ACCESS_TOKEN}"  "$HOST/api/v1/devices?
active_from=1&active_until=0&limit=10000000000"  | jq -r '.[] |
 select(.cloud_instance_name != null) | .cloud_instance_name'
```

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui extrait la liste des équipements, y compris toutes les métadonnées de l'équipement, et écrit la liste dans un fichier CSV situé dans le même répertoire que le script.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `extract_device_list/extract_device_list.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez le `extract_device_list.py` archivez et remplacez les variables de configuration par des informations provenant de votre environnement.
   - Pour les capteurs et la console ExtraHop, spécifiez les variables de configuration suivantes :
     - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde ou de la console ExtraHop.
     - **CLÉ_API:** La clé API.
     - **FICHIER_CSV:** Fichier contenant la liste des groupes d'équipements.
     - **NOM DE FICHIER:** Le fichier dans lequel la sortie sera écrite
     - **LIMITE:** Le nombre maximum d'appareils à récupérer avec chaque requête GET
     - **SAVEL2:** Récupère les appareils parents L2. Cette variable n'est valide que si vous avez activé le système ExtraHop pour détecter les appareils par adresse IP.
     - **AVANCÉ_UNIQUEMENT:** Récupère uniquement les appareils qui font actuellement l'objet d'une analyse avancée
     - **HAUTE_VALEUR_UNIQUEMENT:** Récupère uniquement les appareils considérés comme ayant une valeur élevée
   - Pour RevealX 360, spécifiez les variables de configuration suivantes :

• **HÔTE:** Le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché sur la page d'accès à l' API RevealX 360 sous API Endpoint. Le nom d'hôte n'inclut pas le `/oauth2/token`.

• **IDENTIFIANT:** L'ID des informations d'identification de l'API REST RevealX 360.

• **SECRET:** Le secret des informations d'identification de l'API REST RevealX 360.

• **FICHIER_CSV:** Fichier contenant la liste des groupes d'équipements.

• **NOM DE FICHIER:** Le fichier dans lequel la sortie sera écrite

• **LIMITE:** Le nombre maximum d'appareils à récupérer avec chaque requête GET

• **SAVEL2:** Récupère les appareils parents L2. Cette variable n'est valide que si vous avez activé le système ExtraHop pour détecter les appareils par adresse IP.

• **AVANCÉ_UNIQUEMENT:** Récupère uniquement les appareils qui font actuellement l'objet d'une analyse avancée

• **HAUTE_VALEUR_UNIQUEMENT:** Récupère uniquement les appareils considérés comme ayant une valeur élevée

3. Exécutez la commande suivante :

```
python3 extract_device_list.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `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)
```

Créez un certificat TLS fiable via l'API REST

Par défaut, capteurs et consoles inclure un certificat TLS auto-signé. Vous pouvez toutefois améliorer la sécurité et les performances de votre système en ajoutant un certificat sécurisé signé par une autorité de certification (CA). Vous pouvez créer la demande de signature de certificat à envoyer à votre autorité de certification via l'API REST ExtraHop . Après avoir reçu le certificat signé, vous pouvez également l'ajouter à votre sonde ou console via l'API REST.

Avant de commencer

- Vous devez vous connecter au sonde ou console avec un compte qui possède privilèges d'administration du système et des accès pour générer une clé API.
- Vous devez disposer d'une clé API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir Générer une clé API).
- Familiarisez-vous avec les Guide de l'API REST ExtraHop pour savoir comment naviguer dans l'explorateur d'API REST ExtraHop.

Note: Vous pouvez également exécuter les procédures décrites dans cette rubrique via les paramètres d'administration. Pour plus d'informations, consultez les rubriques suivantes :

- Créez une demande de signature de certificat depuis votre système ExtraHop
- Certificat TLS

Création d'une demande de signature de certificat TLS

Pour créer un certificat TLS signé, vous devez envoyer une demande de signature de certificat à une autorité de certification de confiance.

1. Dans un navigateur, accédez à l'explorateur d'API REST.
   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le **Clé API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **ExtraHop** puis cliquez sur **Post/ExtraHop/SSLCert/Demande de signature**.
5. Cliquez **Essayez-le**.
   Le schéma JSON est automatiquement ajouté au Paramètres de demande de signature de certificat SSL zone de texte des paramètres.
6. Dans le Paramètres de demande de signature de certificat SSL zone de texte du paramètre, spécifiez les champs de demande de signature de certificat.
   a) Dans le `common_name` champ, remplacez `string` avec le nom de domaine complet de votre sonde ou console.
   b) Dans le `subject_alternative_names` champ, ajoutez un ou plusieurs noms de domaine ou adresses IP alternatifs pour votre sonde ou votre console.

      Note: Le `subject_alternative_names` le champ est obligatoire. Si votre système ne possède qu'un seul nom de domaine, dupliquez la valeur du `common_name` champ. Vous devez inclure au moins un nom alternatif du sujet dont le type est défini sur `dns`, mais d'autres noms alternatifs peuvent avoir le type défini sur `ip` ou `dns`.

   c) Optionnel : Dans le `email_address` champ, remplacez `string` avec l'adresse e-mail du propriétaire du certificat.
   d) Optionnel : Dans le `organization_name` champ, remplacez `string` avec le nom légal enregistré de votre organisation.
   e) Optionnel : Dans le `country_code` champ, remplacez `string` avec le code ISO à 2 caractères du pays dans lequel se trouve votre organisation.
   f) Optionnel : Dans le `state_or_province_name` champ, remplacez `string` avec le nom de l'État ou du siège de votre organisation.
   g) Optionnel : Dans le `locality_name` champ, remplacez `string` avec le nom de la ville dans laquelle se trouve votre organisation.
   h) Optionnel : Dans le `organizational_unit_name` champ, remplacez `string` avec le nom de votre département au sein de votre organisation.

   Le Valeur la section doit ressembler à l' exemple suivant :

```
{
  "subject": {
    "common_name": "example.com",
    "email_address": "admin@example.com",
    "organization_name": "Example",
    "country_code": "US"
  },
  "subject_alternative_names": [
    {
      "name": "www.example.com",
      "type": "dns"
    }
  ]
}
```

7. Cliquez **Envoyer la demande** pour créer la demande de signature.
   Dans le Réponse du serveur section, la Organe de réponse affiche la demande de signature dans `pem` champ.

Prochaines étapes
Envoyez la demande de signature à votre autorité de certification pour créer votre certificat TLS signé.

Important: La demande de signature contient des séquences d'échappement qui représentent des sauts de ligne (\n). Remplacez chaque instance de\npar un saut de ligne avant d'envoyer la demande à votre autorité de certification. Vous pouvez modifier la demande PEM manuellement dans un éditeur de texte ou automatiquement via un utilitaire d'analyse JSON, comme illustré dans l'exemple de commande suivant :

```
echo '<json_output>' | python -c 'import sys, json; print
 json.load(sys.stdin)["pem"]'
```

Remplacez le `<json_output>` variable avec la chaîne JSON complète renvoyée dans la section Response Body.

Ajoutez un certificat TLS fiable à votre sonde ou à votre console

Vous pouvez ajouter un certificat TLS signé par une autorité de certification de confiance à votre sonde ou sur console via l'explorateur d'API REST.

1. Dans un navigateur, accédez à l'explorateur d'API REST.

   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans **Clé API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **ExtraHop** puis cliquez sur **PUT/ExtraHop/SSLCert**.
5. Cliquez **Essayez-le**.
6. Dans le **Certificat et clé** dans le champ, collez le certificat TLS.

   Le certificat doit ressembler au texte suivant :

```
-----BEGIN CERTIFICATE-----
a0O8zvV4MlDhWX4e0VyvGAJx+9d4AqQB4Czy/P7z36CmHe2Y7PPdVSeWHNCQoJ0g
CnO42u2V9YKNFYRQejIJv8CxGVJKsdfV0iP0WnCvpZXkaBOYIrDvE5xn010WPUls
6qe3mCXsUK87i++mYuVDA1U0A5YVXRO2OOWIWy7P+MCU/cR/op3Jpekng2cxN4qD
FqGbtRpLdCuJ/xGWL1FFRHBg76+TbO+pxgZhiCtHYXfMKIaoPmDwsAqEtLbizz1W
mbMig9hs4QNcJ+aMNSnTZpkbeBR4a2nkGnQoYvnFOXV/nWzvfHmI4ydSH9g4I8qt
4ArqFepInvm70n07FYAKL6Mdd1i+7ieo9AqckltVzzKFzkakHm04214wtsYmle94
4HqIJ7p7NH5maXxttXMzHFlArbnjHWCl0gIv8lAu+IvLJ8aiGAb3zqveNz6ZAZ5j
PGAUsP+dVYV/8VjvqhkiP/1jWzUHwzpdlHbcD8qOkAF41fnbv+2EXqFJ096JSSiU
rqeJpgNuH3LbkT0KORAiLoGLMZKEKxF+3OpLVD7ox7NQh9pMdZlB8tcTbTmsvD8T
3L2tMVZssqYOANcidtd17t72VW4hzQURT1me5tGWxpN6od/q6B+FIvRq/7Vq0UE1
c2AG/om5UN/Vj3pUjXzq/B1IWUS9TicRcKdl5wrKEkPUGjK4w1R/87bj5HSn8nyd
lMCcOpLTokHj0B5+8O1ylNhVXNPlj3eY0n6OQOdClBqTDM0/4sB3XgeC/pjpleU3
3uot+wM/GoN/Dqb1LPt3BNpUQuCzSfmGSSOXiWELsEhz3ix/36a9eUWjfhmtPsW5
dne5Lf+G7cf+ebsRTb7R89GmgKzTpUl1KAzKINAebkT6WrWWljugpA0BcfANjS6o
mik4ZbY8d54UtA17evprr2+8UotIgVIrCbfLgA2DY8QOTCBYIFKJ3GZAedqRK9Sm
I2qdaB6QBczYNaVYSeCsBdHHw1+h7dBeqdUUwYKtmPW96/djj/6vJSXh9/UX/3c0
eqXG36w/lqJAYu8QtAydJsVC85IzqzikkX0f0KE315Doginpg59yix9dHD2sxLb1
X39BRpLkZ9nvW6ke2YHU/VKBVIxqSslukGoTUIcUtPJrtMQOwCi/EQQXbPK9a2pW
K51938h6OuLjNbDTFuxfhE4zITWHTgyAs2MNVR9+uDUiVJclX+CIPjhZzjyPqmD6
6uh8Sr3zndOMabqDquo69rMQyvclF0xOUMVgUw1Rb8Y=
-----END CERTIFICATE-----
```

Note: Si vous souhaitez que le certificat soit signé avec votre propre clé privée, vous pouvez inclure votre clé après le certificat TLS, en la séparant par un saut de ligne. Cependant, nous vous recommandons de ne pas spécifier votre propre clé ; par défaut, la sonde ou la console signera le certificat avec la clé privée du système.

7. Cliquez **Envoyer la demande** pour ajouter le certificat.

Créez des appareils personnalisés via l'API REST

Vous pouvez créer des appareils personnalisés via l'API REST qui suit le trafic réseau sur plusieurs adresses IP et ports. Par exemple, vous souhaiterez peut-être ajouter un équipement personnalisé pour chaque succursale. Si vous créez les appareils par le biais d'un script, vous pouvez lire la liste des appareils à partir d'un fichier CSV. Dans cette rubrique, nous allons présenter des méthodes pour l'API REST et pour l'explorateur d'API REST ExtraHop.

Avant de commencer

- Vous devez vous connecter au sonde avec un compte doté de privilèges d'administration du système et d'accès pour générer une clé d'API.
- Vous devez disposer d'une clé d'API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir Générer une clé API.)
- Familiarisez-vous avec le Guide de l' API REST ExtraHop pour apprendre à naviguer dans l'explorateur d'API REST d'ExtraHop.

Créez un équipement personnalisé via l'explorateur d'API REST

Vous pouvez créer un équipement personnalisé et l'associer à une liste d' adresses IP ou de blocs CIDR via **Appareils POST/personnalisés** opération.

1. Dans un navigateur, accédez à l'explorateur d'API REST.

   L'URL est le nom d'hôte ou l'adresse IP de votre sonde, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Appareil personnalisé**, puis cliquez sur **Appareils POST /personnalisés**.
3. Dans le champ corps, spécifiez les propriétés de l'équipement personnalisé que vous souhaitez créer.

   Par exemple, le corps suivant associe l'équipement personnalisé aux blocs d'adresse CIDR 192.168.0.0/26, 192.168.0.64/27, 192.168.0.96/30 et 192.168.0.100/32 :

```
{
  "description": "The location of our office in Washington",
  "name": "Seattle",
  "criteria": [
    {
      "ipaddr": "192.168.0.0/26"
    },
    {
      "ipaddr": "192.168.0.64/27"
    },
    {
      "ipaddr": "192.168.0.96/30"
    },
    {
      "ipaddr": "192.168.0.100/32"
    }
  ]
}
```

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub d'ExtraHop contient un exemple de script Python qui crée des appareils personnalisés en lisant les critères d'un fichier CSV.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `create_custom_devices/create_custom_devices.py` fichier sur votre machine locale.
2. Créez un fichier CSV avec des lignes contenant les colonnes suivantes dans l' ordre indiqué :

Nom	IDENTIFIANT	Descriptif	adresse IP ou bloc CIDR

Conseil: Le `create_custom_devices` le répertoire contient un exemple de fichier CSV nommé `device_list.csv`.

Le script n'accepte pas de ligne d'en-tête dans le fichier CSV. Le nombre de colonnes du tableau n'est pas limité ; chaque colonne située après les quatre premières indique une adresse IP supplémentaire pour l'équipement. Les quatre premières colonnes sont obligatoires pour chaque ligne.

3. Dans un éditeur de texte, ouvrez le `create_custom_devices.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :
   - **HÔTE:** L'adresse IP ou le nom d'hôte de la sonde.
   - **APIKEY:** La clé d'API.
   - **FICHIER_CSV:** Le chemin du fichier CSV par rapport à l'emplacement du fichier de script.
4. Exécutez la commande suivante :

```
python3 create_custom_devices.py
```

Note: Si le script renvoie un message d'erreur indiquant que la vérification du certificat TLS a échoué, assurez-vous que un certificat fiable a été ajouté à votre sonde ou à votre console. Vous pouvez également ajouter `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)
```

Création et attribution d'une étiquette d'équipement via l'API REST

Le script Python suivant crée une balise d'équipement, puis affecte cette balise à tous les périphériques d'un sous-réseau spécifié.

```
#!/usr/bin/env python

import httplib
import urllib
import json
import sys

# Configuration Options:
host = "{HOST}"
apikey = "{API KEY}"
tag_name = "MyTestTag"
subnet = "10.20.0.[0-9]+"
batch_limit = 100
headers = {'Accept': 'application/json',
           'Authorization': "ExtraHop apikey=%s" % apikey}
conn = httplib.HTTPSConnection(host)
  def execute_req(method, path, expected_code, failure_message, body=None):
"""
   Returns the body of a successful request,
   otherwise prints error and terminates
"""

conn.request(method, "/api/v1" + path, headers=headers, body=body)
resp = conn.getresponse()
if resp.status is not expected_code:
```

```
    print(failure_message)
    print(resp.read())
    sys.exit(1)
return resp

def execute_get(path, expected_code, failure_message):
    resp = execute_req("GET", path, expected_code, failure_message)
    return json.loads(resp.read())

def execute_create(path, body, expected_code, failure_message):
    """Returns ID of newly created resource"""
    resp = execute_req("POST", path, expected_code, failure_message, body)
    resp.read() # drain the response
    return int(resp.getheader("location").split("/")[-1])

# First, search for the specified tag, by name
resp = execute_get("/tags", 200, "Unable to retrieve tags from ExtraHop")
tags = [tag for tag in resp if tag["name"] == tag_name]

if not tags:
    # tag is not found, create it
    body = json.dumps({"name": tag_name})
    tag_id = execute_create('/tags', body, 201, "Unable to create tag")
else:
    tag_id = tags[0]["id"]

query_params = {'limit': batch_limit,
                'search_type': 'ip address',
                'value': subnet}
query_string = urllib.urlencode(query_params)

# Paginate device results, building up a list of all devices to assign
device_ids = []
offset = 0

while True:
    path = "/devices?" + query_string + ("&offset=%d" % offset)
    resp = execute_get(path, 200, "Unable to retrieve devices")
    if not resp:
        break

    device_ids += [device["id"] for device in resp]
    offset += batch_limit

# Perform the assignments
resp = execute_req("POST", "/tags/%d/devices" % tag_id,
                   204, "Unable to perform assignments",
                   body=json.dumps({"assign": device_ids}))
resp.read() # drain the response

# Check that assignments were successful
resp = execute_get("/tags/%d/devices" % tag_id,
                   200, "Unable to retrieve tag assignments")
assigned_device_ids = [device["id"] for device in resp]

successful = set(device_ids).issubset(set(assigned_device_ids))
if successful:
    print("%d devices assigned to tag" % len(device_ids))
else:
    print("Unable to assign all devices to tag")
```

Requête de métriques relatives à un équipement spécifique via l'API REST

Le script Python suivant demande des métriques à partir d'un HTTP client appareil avec l'ID 9363 et imprime la réponse.

```
import httplib

headers = {'Content-Type': 'application/json',
       'Accept': 'application/json',
       'Authorization': 'ExtraHop apikey={API KEY}'
body = r"""{
  "cycle": "auto",
  "from": -1800000,
  "until": 0,
  "metric_category": "http_client",
  "metric_specs": [
    {
       "name": "req"
    }
   ],
   "object_ids": [
      9363
   ],
   "object_type": "device"
}"""
conn = httplib.HTTPSConnection('{HOST}')
conn.request('POST', '/api/v1/metrics', headers=headers, body=body)
resp = conn.getresponse()
print resp.status, resp.reason
print resp.read()
```

La réponse suivante indique les entrées relatives à l'équipement portant l'ID 9363 :

```
{
 "date": "Thu, 19 Nov 2015 23:20:07 GMT",
 "via": "1.1 localhost",
 "server": "Apache",
 "vary": "Accept-Encoding",
 "content-type": "application/json; charset=utf-8",
 "cache-control": "private, max-age=0",
 "connection": "Keep-Alive",
 "content-encoding": "gzip",
 "keep-alive": "timeout=45, max=44",
 "content-length": "277"
}

{
 "stats": [
   {
    "oid": 9363,
    "time": 1447973460000,
    "duration": 30000,
    "values": [
     2
    ]
   },
   {
    "oid": 9363,
    "time": 1447973490000,
    "duration": 30000,
    "values": [
     0
```

```
    ]
   },
   {
    "oid": 9363,
    "time": 1447973520000,
    "duration": 30000,
    "values": [
      1
     ]
    },
    {
     "oid": 9363,
     "time": 1447973550000,
     "duration": 30000,
     "values": [
       2
      ]
     }
```

Création, récupération et suppression d'un objet via l'API REST

Cet exemple montre comment créer et récupérer correctement des informations relatives à une étiquette d' équipement. Ensuite, une fois les balises de l'équipement supprimées, l'exemple montre comment une tentative de récupération d'informations échoue par la suite.

L'exemple suivant montre comment créer une balise d'équipement appelée my_test_tag.

```
curl -i -X POST --header "Content-Type: application/json" \
--header "Accept: application/json" \
--header "Authorization: ExtraHop apikey={API KEY}" \
-d "{
\"name\": \"my_test_tag\"
}" "https://{HOST}/api/v1/tags"
```

Le statut 201 est renvoyé en cas de succès avec les en-têtes de réponse suivants, qui indiquent que la balise a été créée, et fournissent l'emplacement de la balise de l'équipement et l'ID de /api/v1/tags/1.

```
{
 "date": "Wed, 18 Nov 2015 20:24:13 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=45, max=88",
 "content-length": "0"
}
```

Ensuite, l'ID (1) est ajouté à la requête GET suivante, qui renvoie un statut 200 en cas de réussite et la représentation JSON de la balise récupérée :

```
curl -i -X GET --header "Accept: application/json" \
--header "Authorization: ExtraHop apikey={API KEY}" \
"https://{HOST}/api/v1/tags/1"
{
 "mod_time": 1447878253953,
 "id": 1,
 "name": "my_test_tag"
}
```

Ensuite, l'exemple suivant montre une demande DELETE visant à supprimer la balise d'équipement du système, qui renvoie le statut 204 en cas de succès :

```
curl -i -X DELETE --header "Accept: application/json" \
--header "Authorization: ExtraHop apikey={API KEY}" \
"https://{HOST}/api/v1/tags/1"
```

Enfin, lorsqu'une autre requête GET est envoyée pour cette étiquette d'équipement supprimée, l'opération échoue et un statut 404 est renvoyé en cas d'échec, indiquant que la balise n'est plus disponible.

```
curl -i -X GET --header "Accept: application/json" \
--header "Authorization: ExtraHop apikey={API KEY}" \
"https://{HOST}/api/v1/tags/1"
```

Interroger le journal des enregistrements

Le corps de demande suivant interroge le journal des enregistrements pour en récupérer 100 HTTP les enregistrements dont la méthode est GET et le code dac.état est 404.

```
{
  "filter": {
    "operator": "and",
    "rules": [
        {
            "field": "method",
            "operand": "GET",
            "operator": "="
        },
        {
            "field": "statusCode",
            "operand": "404",
            "operator": "="
        }
   ]
 },
 "from": -900000,
 "limit": 100,
 "types": [
   "~http"
 ]
}
```