9.8
Guide de l'API REST du capteur IDS

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

Publié: 2024-09-26

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

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.

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"
}
```

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.
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"
}
```

Nuage

Cette ressource vous permet de connecter votre site capteurs à RevealX 360 Pour plus d' informations, consultez Connectez-vous à RevealX 360 à partir de capteurs autogérés.

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"
}
```

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.
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.

opération	Descriptif
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.

Les valeurs suivantes sont valides :

- `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.

Les valeurs suivantes sont valides :

- `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***

Type de participant.

Les valeurs suivantes sont valides :

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

`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 ».

`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***

Type de participant.

Les valeurs suivantes sont valides :

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

`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 ».

`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 le 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"
    },
    "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"
    }
}
```

`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***

Type de participant.

Les valeurs suivantes sont valides :

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

`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 ».

`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***

Type de participant.

Les valeurs suivantes sont valides :

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

`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 ».

`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 le 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"
    },
    "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"
    }
}
```

`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"
        }
    ]
}
```

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.

Fonctionnement	Descriptif
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.

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.

opération	Descriptif
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.
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.

opération	Descriptif
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 Mettez 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`
- `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"
}
```

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.
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/`

opération	Descriptif
	`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"]
}
```

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.

opération	Descriptif
	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.

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.
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.

Fonctionnement	Descriptif
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.

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 à un moment donné 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 de l'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 incorporés 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. La valeur spécifiée est interprétée comme une durée dans le futur. 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. Si une valeur non nulle est spécifiée, la réponse inclut un identifiant de curseur accepté par POST /records/cursor/. Ce paramètre n'est pas pris en charge pour les magasins d'enregistrement tiers.

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.

`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,
    "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'opérande 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`

Unité de temps	Suffixe d'unité
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"]
}
```

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.

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.

Fonctionnement	Descriptif
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.
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.

- 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.
- Vous pouvez télécharger directement des collections de menaces sur les systèmes RevealX 360 pour une gestion autonome capteurs. Contactez le support ExtraHop pour télécharger une collecte des menaces vers ExtraHop Managed capteurs.
- 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.

opération	Descriptif
	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.

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.