ExtraHop 9.8
Guide de l'API REST RevealX 360

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

Guide de l'API REST RevealX 360

L'API REST RevealX 360 vous permet d'automatiser les tâches de configuration et de récupérer des métriques, des paquets et des détections depuis RevealX 360. Vous pouvez envoyer des requêtes à l'API via une interface REST (Representational State Transfer), accessible via des URI de ressources et des méthodes HTTP standard.

Avant de pouvoir envoyer une demande d'API REST à RevealX 360, vous devez activer le système pour accéder à l' API REST et générer des informations dcessaires d'identification. Ensuite, vous devez récupérer un jeton d'accès temporaire en envoyant l'ID et le secret de vos informations dectueuses de l'API REST à RevealX 360. Enfin, incluez le jeton d'accès dans l'en-tête de votre demande d'authentification. Les informations dcessations d'identification de l'API REST n'expirent pas automatiquement et doivent être supprimées manuellement avant de devenir invalides.

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

Activer l'API REST pour RevealX 360

Avant de pouvoir envoyer des demandes d'API REST à RevealX 360, vous devez activer l'accès à l'API REST .

Avant de commencer

- Vous devez disposer des privilèges d'administration du système et des accès.

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Accès à l'API**.
4. Dans le Gérer l'accès aux API section, cliquez sur **Activer**.

   Si vous désactivez puis réactivez l'API REST, celle-ci risque de ne pas être disponible pendant environ 15 minutes en raison de la propagation du DNS, même si la section Status indique que l'accès est activé. Nous vous recommandons de ne pas désactiver et réactiver souvent l'API REST.

Création d'informations d'identification pour l'API REST

RevealX 360 authentifie les requêtes d'API REST à l'aide du protocole OpenID Connect (OIDC). L'OIDC demande aux utilisateurs de fournir des jetons d'accès temporaires lorsqu'ils font une demande à l'API. Avant de pouvoir générer des jetons d'accès, vous devez créer des informations d'identification de l'API REST, également appelées informations d'identification du client.

Note: Les informations dcessations d'identification de l'API REST n'expirent pas automatiquement. Les informations dcessaires d'identification créées par un utilisateur ne sont pas supprimées lorsque celui-ci est retiré du système. Les informations dcessaires d'identification restent valides jusqu'à leur suppression. Tout administrateur peut supprimer toutes les informations d'identification, quel que soit l'utilisateur qui les a créées.

L'API REST RevealX 360 ne prend pas en charge le partage de ressources d'origine croisée (CORS).

Avant de commencer

- Vous devez disposer des privilèges d'administration du système et des accès.

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Accès à l'API**.
4. Cliquez **Créer des informations d'identification**.
5. Dans le **Nom** dans ce champ, saisissez un nom pour les informations dcessations d'identification.
6. Dans le **Privilèges** champ, spécifiez un niveau de privilège pour les informations dproximatives.

   Le niveau de privilège détermine les actions qui peuvent être effectuées avec les informations d'identification. N'accordez pas plus de privilèges que nécessaire aux informations d'identification de l'API REST, car cela peut créer un risque de sécurité. Par exemple, les applications qui récupèrent uniquement des métriques ne doivent pas se voir attribuer d'informations dcessitant d'octroyer des privilèges administratifs. Pour plus d'informations sur chaque niveau de privilège, consultez Privilèges utilisateur.

   Note: Les privilèges d'administration du système et des accès sont similaires aux privilèges d'écriture complets et autorisent l'obtention d'informations d'identification pour connecter des capteurs autogérés et des appliances Trace à RevealX 360.
7. Dans le **Accès aux paquets** champ, spécifiez si vous pouvez récupérer les paquets et les clés de session avec les informations dproximatives.
8. Cliquez **Enregistrer**.
   Le Copier les informations d'identification de l'API REST le volet apparaît.
9. En dessous IDENTIFIANT, cliquez **Copier dans le presse-papiers** et enregistrez l'identifiant sur votre ordinateur local.
10. En dessous Secret, cliquez **Copier dans le presse-papiers** et enregistrez le secret sur votre machine locale.

    Important: Le secret ne peut pas être consulté ou récupéré ultérieurement.
11. Cliquez **Terminé**.

Générer un jeton d'API REST

Un jeton d'accès à l'API temporaire doit être inclus dans toutes les demandes d'API REST adressées à RevealX 360 . Après avoir créé les informations d'identification de l'API REST, vous pouvez écrire des scripts qui génèrent des jetons d'accès API temporaires à l'aide de ces informations. Les scripts peuvent ensuite authentifier les demandes d'API REST adressées à RevealX 360 à l'aide des jetons. Les jetons sont valides pendant 10 minutes après avoir été générés.

La demande de jeton HTTPS doit répondre aux exigences suivantes :

- Le jeton est envoyé dans une requête POST au point de terminaison du jeton d'API, qui est affiché sur Accès à l'API page ci-dessous Point de terminaison API dans RevealX 360.
- Incluez les en-têtes suivants :
  - `Authorization: Basic <auth>`

    Où `<auth>` est une chaîne codée en base64 contenant l'identifiant et le secret, joints par deux points.
  - `Content-Type: application/x-www-form-urlencoded`
- Incluez la charge utile suivante :

```
grant_type=client_credentials
```

Note: Les jetons d'accès à l'API temporaires créés par les exemples de scripts ne sont valides que pendant 10 minutes. Si l'exécution d'un script prend plus de 10 minutes, il doit générer un nouveau jeton toutes les 10 minutes pour s'assurer qu'il n'envoie pas de jeton expiré. Si un script envoie un jeton expiré, le système répond avec un code d'erreur HTTP 401 et le message d'erreur suivant :

```
The incoming token has expired
```

Prochaines étapes
Après avoir généré un jeton, vous pouvez l'inclure en tant que jeton porteur dans l'en-tête d'autorisation HTTP pour authentifier les demandes. Par exemple, si votre jeton est »`abcdefghijklmnop0123456789`«, incluez la chaîne suivante dans l' en-tête :

```
"Authorization": "Bearer abcdefghijklmnop0123456789"
```

Récupérez et exécutez l'exemple de script Python

Le référentiel GitHub ExtraHop contient un exemple de script Python qui génère un jeton d'accès à l'API temporaire, puis authentifie deux demandes simples avec le jeton qui récupère des appareils et des groupes d'appareils depuis RevealX 360.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `py_rx360_auth/py_rx360_auth.py` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `py_rx360_auth.py` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :

   • **HÔTE:** Le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché dans RevealX 360 Accès à l'API page ci-dessous Point de terminaison API. Le nom d'hôte n'inclut pas `/oauth2/token`.

   • **IDENTIFIANT:** L'ID des informations d'identification de l'API REST.

   • **SECRET:** Le secret des informations d'identification de l'API REST.

Exécutez la commande suivante :

```
python3 py_rx360_auth.py
```

Exemple de Bash et cURL

Le référentiel GitHub ExtraHop contient un exemple de script Bash qui génère un jeton d' API REST à l'aide de la commande cURL, puis authentifie deux requêtes simples avec le jeton qui récupèrent des appareils et des groupes d'appareils à partir de l'API REST RevealX 360.

Avant de commencer

- L'outil cURL doit être installé sur votre machine.
- L'analyseur jq doit être installé sur votre machine. Pour plus d'informations, voir https://stedolan.github.io/jq/.

1. Accédez au Référentiel GitHub d'exemples de code ExtraHop et téléchargez le `bash_rx360_auth/bash_rx360_auth.sh` fichier sur votre machine locale.
2. Dans un éditeur de texte, ouvrez `bash_rx360_auth.sh` archivez et remplacez les variables de configuration suivantes par des informations provenant de votre environnement :

   • **HÔTE:** Le nom d'hôte de l'API RevealX 360. Ce nom d'hôte est affiché dans RevealX 360 Accès à l'API page ci-dessous Point de terminaison API. Le nom d'hôte n'inclut pas `/oauth2/token`.

   • **IDENTIFIANT:** L'ID des informations d'identification de l'API REST.

   • **SECRET:** Le secret des informations d'identification de l'API REST.
3. Exécutez la commande suivante :

```
./bash_auth.sh
```

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://<revealx-360-hostname-or-ip-address>/api/v1/explore/
```

1. Connectez-vous à RevealX 360.
2. Cliquez sur l'icône Paramètres système en haut à droite de la page, puis cliquez sur **Toute l'administration**.
3. Cliquez **Accès à l'API**.
4. Sur le Accès à l'API page, cliquez **Ouvrez l'explorateur d' API REST ExtraHop**.

   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 RevealX 360

Vous pouvez effectuer des opérations sur les ressources suivantes via l'API REST RevealX 360. Vous pouvez également consulter des informations plus détaillées sur ces ressources, telles que HTTP méthodes, paramètres de requête et propriétés des objets.

Note: Les points de terminaison de l'API sont situés à `<host>/api/v1/<endpoint>`, où `host` est le nom d'hôte de l'API RevealX 360. Par exemple, si le nom d'hôte de l'API est `https://example.com`, le point de terminaison des cartes d'activité serait l'URL suivante :

```
https://example.com/api/v1/activitymaps
```

Vous pouvez obtenir le nom d'hôte à partir du point de terminaison du jeton d'API en supprimant `/oauth2/token` à partir de la chaîne de point de terminaison, qui apparaît sur la page d'accès à l'API RevealX 360 sous Point de terminaison API.

Carte des activités

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

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

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

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

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

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

Fonctionnement	Descriptif
PATCH /activitymaps/ {id} /partage	Mettez à jour les utilisateurs et leurs autorisations de partage pour une carte dactivitiés spécifique.
PUT /activitymaps/ {id} /partage	Remplacez les utilisateurs et leurs autorisations de partage pour une carte dactivitiés spécifique.

Détails de l'opération

`POST /activitymaps`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de la carte dactivities.

`name:` ***Corde***

Nom convivial de la carte dactivités.

`short_code:` ***Corde***

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

`description:` ***Corde***

Description de la carte dactivitiés.

`weighting:` ***Corde***

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

`mode:` ***Corde***

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

`show_alert_status:` ***Booléen***

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

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

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

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

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

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

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

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

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

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

`protocol:` ***Corde***

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

`role:` ***Corde***

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

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

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

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

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

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

`object_type:` ***Corde***

Type de source métrique.

Les valeurs suivantes sont valides :

- `device`
- `device_group`

`object_id:` ***Numéro***

Identifiant unique de l'objet source.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "mode": "string",
    "name": "string",
    "short_code": "string",
    "show_alert_status": true,
    "walks": {
        "origins": {
            "object_type": "string",
            "object_id": 0
        },
        "steps": {
            "relationships": {
                "protocol": "string",
                "role": "string"
            },
            "peer_in": {
                "object_type": "string",
                "object_id": 0
            },
            "peer_not_in": {
                "object_type": "string",
                "object_id": 0
            }
        }
    },
    "weighting": "string"
}
```

`POST /activitymaps/query`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de la requête topologique.

`from:` ***Numéro***

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

`until:` ***Numéro***

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

`weighting:` ***Corde***

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

Les valeurs suivantes sont valides :

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

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

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

Les valeurs suivantes sont valides :

- `protocols`

- `appearances`

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

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

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

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

`object_type:` ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

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

`object_id:` ***Numéro***

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

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

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

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

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

`role:` ***Corde***

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

Les valeurs suivantes sont valides :

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

`protocol:` ***Corde***

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

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

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

`object_type:` ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

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

`object_id:` ***Numéro***

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

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

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

`object_type:` ***Corde***

Type d'objet source.

Les valeurs suivantes sont valides :

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

`object_id:` ***Numéro***

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

Spécifiez le paramètre body au format JSON suivant.

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

`GET /activitymaps`

Il n'existe aucun paramètre pour cette opération.

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

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

`GET /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

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

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

`POST /activitymaps/{id}/query`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

`body:` ***Objet***

Les propriétés de la requête topologique.

`from:` ***Numéro***

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

`until:` ***Numéro***

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

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

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

Les valeurs suivantes sont valides :

- `protocols`
- `appearances`

Spécifiez le paramètre body au format JSON suivant.

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

`DELETE /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

`PATCH /activitymaps/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

`body:` ***Objet***

Les propriétés de la carte dactivités à mettre à jour.

`GET /activitymaps/{id}/sharing`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

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

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

`PUT /activitymaps/{id}/sharing`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les utilisateurs et leurs niveaux d'autorisation.

`id:` ***Numéro***

Identifiant unique de la carte dactivités.

```
PATCH /activitymaps/{id}/sharing
```

Spécifiez les paramètres suivants.

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

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

Alerte

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

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

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

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

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

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

Détails de l'opération

`GET /alerts`

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

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
```

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

`POST /alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées à la nouvelle alerte.

`description:` ***Corde***

Description facultative de l'alerte.

`notify_snmp:` ***Booléen***

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

`field_op:` ***Corde***

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

Les valeurs suivantes sont valides :

- `/`
- `null`

`stat_name:` ***Corde***

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

`disabled:` ***Booléen***

(Facultatif) Indique si l'alerte est désactivée.

`operator:` ***Corde***

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

Les valeurs suivantes sont valides :

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

`operand:` ***Corde***

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

`field_name:` ***Corde***

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

`name:` ***Corde***

Le nom unique et convivial de l'alerte.

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

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

`apply_all:` ***Booléen***

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

`severity:` ***Numéro***

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

Les valeurs suivantes sont valides :

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

`author:` ***Corde***

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

`param:` ***Objet***

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

`interval_length:` ***Numéro***

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

Les valeurs suivantes sont valides :

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

`param2:` ***Objet***

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

`units:` ***Corde***

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

Les valeurs suivantes sont valides :

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

`field_name2:` ***Corde***

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

`refire_interval:` ***Numéro***

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

Les valeurs suivantes sont valides :

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

`type:` ***Corde***

Type d'alerte.

Les valeurs suivantes sont valides :

- `threshold`

`object_type:` ***Corde***

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

Les valeurs suivantes sont valides :

- `application`
- `device`

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

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

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

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

Spécifiez le paramètre body au format JSON suivant.

```
{
    "apply_all": true,
    "author": "string",
    "categories": [
        "string"
    ],
    "cc": [],
    "description": "string",
    "disabled": true,
    "field_name": "string",
    "field_name2": "string",
```

```
    "field_op": "string",
    "interval_length": 0,
    "name": "string",
    "notify_snmp": true,
    "object_type": "string",
    "operand": "string",
    "operator": "string",
    "param": {},
    "param2": {},
    "protocols": [
        "string"
    ],
    "refire_interval": 0,
    "severity": 0,
    "stat_name": "string",
    "type": "string",
    "units": "string"
}
```

`GET /alerts/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

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

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

`DELETE /alerts/{id}`

Spécifiez les paramètres suivants.

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

`PATCH /alerts/{id}`

Spécifiez les paramètres suivants.

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

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

`GET /alerts/{id}/stats`

Spécifiez les paramètres suivants.

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

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

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

`GET /alerts/{id}/devicegroups`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/devicegroups`

Spécifiez les paramètres suivants.

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

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

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

`GET /alerts/{id}/emailgroups`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/emailgroups`

Spécifiez les paramètres suivants.

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

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

Spécifiez les paramètres suivants.

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

`GET /alerts/{id}/exclusionintervals`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/exclusionintervals`

Spécifiez les paramètres suivants.

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

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

`GET /alerts/{id}/devices`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/devices`

Spécifiez les paramètres suivants.

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

`GET /alerts/{id}/networks`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/networks`

Spécifiez les paramètres suivants.

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

`GET /alerts/{id}/applications`

Spécifiez les paramètres suivants.

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

`POST /alerts/{id}/applications`

Spécifiez les paramètres suivants.

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

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

L'identifiant unique de l'alerte.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'application.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'application.

`id:` ***Numéro***

L'identifiant unique de l'alerte.

Priorité d'analyse

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

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

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

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

opération	Descriptif
GET /analysispriority/config/ {sensor_id}	Récupérez les règles de priorité d'analyse pour un objet spécifique sonde.
PUT /analysispriority/config/ {sensor_id}	Remplacer les règles de priorité d'analyse pour un objet spécifique sonde.
GET /analysispriority/{sensor_id} /manager	Récupérez le système configuré pour gérer les règles de priorité d'analyse pour le sonde.

opération	Descriptif
PATCH /priorité d'analyse/{sensor_id} /gestionnaire	Mettre à jour le système qui gère les règles de priorité d'analyse pour un domaine spécifique sonde.

Détails de l'opération

`GET /analysispriority/{appliance_id}/manager`

Spécifiez les paramètres suivants.

`appliance_id:` ***Numéro***

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

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

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

`GET /analysispriority/config/{appliance_id}`

Spécifiez les paramètres suivants.

`appliance_id:` ***Numéro***

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

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

```
{
    "advanced_rules": [],
    "autofill_advanced": true,
    "autofill_standard": true,
    "is_in_effect": true,
    "standard_rules": []
}
```

`PUT /analysispriority/config/{appliance_id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Propriétés des règles d'analyse des priorités.

`autofill_advanced:` ***Booléen***

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

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

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

`type:` ***Corde***

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

Les valeurs suivantes sont valides :

- `device_group`

`object_id:` ***Numéro***

Identifiant unique du groupe.

`description:` ***Corde***

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

`autofill_standard:` ***Booléen***

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

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

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

`type:` ***Corde***

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

Les valeurs suivantes sont valides :

- `device_group`

`object_id:` ***Numéro***

Identifiant unique du groupe.

`description:` ***Corde***

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

Spécifiez le paramètre body au format JSON suivant.

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

`appliance_id:` ***Numéro***

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

`PATCH /analysispriority/{appliance_id}/manager`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

`manager:` ***Numéro***

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

Spécifiez le paramètre body au format JSON suivant.

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

```
}
```

`appliance_id:` ***Numéro***

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

Appareil

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

Vous pouvez récupérer des informations sur les appareils ExtraHop connectés à l'appareil local et établir de nouvelles connexions avec des appareils ExtraHop distants.

Note: Vous ne pouvez établir une connexion qu'à une appliance ExtraHop distante dont la licence est identique à celle de l'appliance ExtraHop locale.

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

Fonctionnement	Descriptif
GET /appareils	Récupérez tous les appareils ExtraHop distants connectés à l'appareil local.
OBTENEZ /appliances/ {id}	Récupérez une appliance ExtraHop distante spécifique connectée à l'appliance locale.
GET /appareils/firmware/next	Récupérez les versions du microprogramme vers lesquelles les systèmes ExtraHop distants peuvent être mis à niveau.
POST /appareils/firmware/mise à niveau	Mettez à jour le microprogramme sur les systèmes ExtraHop distants connectés au système local. Les images du firmware sont téléchargées depuis ExtraHop Cloud Services.

Détails de l'opération

`GET /appliances`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "add_time": 0,
    "advanced_analysis_capacity": 0,
    "analysis_levels_managed": true,
    "connection_type": "string",
    "data_access": true,
    "display_name": "string",
    "fingerprint": "string",
    "firmware_version": "string",
    "hostname": "string",
    "id": 0,
    "license_platform": "string",
    "license_status": "string",
    "licensed_features": {},
    "licensed_modules": [
        "string"
    ],
    "managed_by_local": true,
```

```
    "manages_local": true,
    "nickname": "string",
    "platform": "string",
    "status_message": "string",
    "sync_time": 0,
    "total_capacity": 0,
    "uuid": "string"
}
```

`GET /appliances/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Spécifiez l'identifiant unique de l'appliance. Spécifiez 0 pour sélectionner l'appliance locale.

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

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

`GET /appliances/{ids_id}/association`

Spécifiez les paramètres suivants.

`ids_id:` ***Numéro***

Spécifiez l'ID de la sonde IDS.

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

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

`POST /appliances/{ids_id}/association`

Spécifiez les paramètres suivants.

`ids_id:` ***Numéro***

Spécifiez l'ID de la sonde IDS.

`body:` ***Objet***

Spécifiez l'ID de la sonde réseau dveloppe analyse de paquets.

`associated_sensor_id:` ***Numéro***

L'ID de la sonde réseau dveloppe l'analyse de paquets.

Spécifiez le paramètre body au format JSON suivant.

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

`GET /appliances/firmware/next`

Spécifiez les paramètres suivants.

`ids:` ***Corde***

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

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

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

`POST /appliances/firmware/upgrade`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les options de mise à niveau du microprogramme.

`version:` ***Corde***

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

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

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

Spécifiez le paramètre body au format JSON suivant.

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

Demande

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

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

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

Détails de l'opération

`GET /applications/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique de l'application.

`include_criteria:` ***Booléen***

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

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

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

`POST /applications`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les propriétés de l'application.

`node_id:` ***Numéro***

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

`discovery_id:` ***Corde***

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

`display_name:` ***Corde***

Nom convivial de l'application.

`description:` ***Corde***

(Facultatif) Description facultative de l'application.

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

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

`protocol_default:` ***Corde***

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

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

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

`type:` ***Corde***

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

`id:` ***Numéro***

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

`protocols:` ***Objet***

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

Spécifiez le paramètre body au format JSON suivant.

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

```
    "display_name": "string",
    "node_id": 0
}
```

`PATCH /applications/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

`id:` ***Numéro***

Identifiant unique de l'application.

`GET /applications`

Spécifiez les paramètres suivants.

`active_from:` ***Numéro***

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

`active_until:` ***Numéro***

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

`limit:` ***Numéro***

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

`offset:` ***Numéro***

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

`search_type:` ***Corde***

Type d'objet à rechercher.

Les valeurs suivantes sont valides :

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

`value:` ***Corde***

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

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

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

```
}
```

`GET /applications/{id}/activity`

Spécifiez les paramètres suivants.

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

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

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

`GET /applications/{id}/alerts`

Spécifiez les paramètres suivants.

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

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

`POST /applications/{id}/alerts`

Spécifiez les paramètres suivants.

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

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

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

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

Spécifiez les paramètres suivants.

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

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

```
GET /applications/{id}/dashboards
```

Spécifiez les paramètres suivants.

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

Journal d'audit

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

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

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

Détails de l'opération

```
GET /auditlog
```

Spécifiez les paramètres suivants.

`limit:` ***Numéro***
(Facultatif) Nombre maximal de messages de journal à renvoyer.

`offset:` ***Numéro***
(Facultatif) Nombre de messages de journal à ignorer dans les résultats. Renvoie les messages du journal à partir de la valeur de décalage.

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

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

Bundle

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

Vous pouvez créer un bundle, puis transférer ces configurations vers un autre système ExtraHop, ou enregistrer le bundle en tant que sauvegarde. Les packs peuvent également être téléchargés sur Offres groupées de solutions ExtraHop et appliquées via l'API REST. Pour plus d'informations, voir Lots.

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

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

Détails de l'opération

`GET /bundles`

Il n'existe aucun paramètre pour cette opération.

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

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

`POST /bundles`

Spécifiez les paramètres suivants.

`body:` ***Corde***

Une exportation de bundle au format JSON.

`name:` ***Corde***

Le nom convivial du bundle.

`description:` ***Corde***

(Facultatif) Description facultative du bundle.

Spécifiez le paramètre body au format JSON suivant.

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

```
}
```

`GET /bundles/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du bundle.

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

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

`DELETE /bundles/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du bundle.

`POST /bundles/{id}/apply`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du bundle.

`body:` ***Objet***
Les options de configuration pour appliquer le bundle.

`policy:` ***Corde***
Indique si les objets en conflit doivent être remplacés ou ignorés.

Les valeurs suivantes sont valides :

- `overwrite`
- `skip`

`include_assignments:` ***Booléen***
Indique si les assignations d'objets doivent être restaurées avec le bundle.

`node_ids:` ***Tableau de nombres***
Une liste d'identifiants uniques pour les capteurs sur lesquels appliquer le bundle. Ce champ n'est valide que sur une console.

Spécifiez le paramètre body au format JSON suivant.

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

Tableaux de bord

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

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

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

Détails de l'opération

`GET /dashboards`

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

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

`GET /dashboards/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du tableau de bord.

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

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

`DELETE /dashboards/{id}`

Spécifiez les paramètres suivants.

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

`PATCH /dashboards/{id}`

Spécifiez les paramètres suivants.

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

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

`GET /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

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

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

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

`PUT /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

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

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

`PATCH /dashboards/{id}/sharing`

Spécifiez les paramètres suivants.

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

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

`GET /dashboards/{id}/reports`

Spécifiez les paramètres suivants.

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

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"
        }
    ]
}
```

Catégories de détection

Le champ des catégories est un tableau renvoyé dans les réponses pour `GET /detections` et `POST /detections/search` opérations. Le tableau suivant répertorie les entrées valides du tableau :

Valeur	Catégorie
`sec`	Sûreté
`sec.action`	Actions par rapport à l'objectif
`sec.attack`	Attaque
`sec.botnet`	botnet
`sec.caution`	Mise en garde

Valeur	Catégorie
`sec.command`	Commandement et contrôle
`sec.cryptomining`	Cryptominage
`sec.dos`	Déni de service
`sec.exfil`	Exfiltration
`sec.exploit`	Exploitation
`sec.hardening`	Durcissement
`sec.lateral`	Mouvement latéral
`sec.ransomware`	Un ransomware
`sec.recon`	Reconnaissance
`perf`	Rendement
`perf.auth`	Autorisation et contrôle d'accès
`perf.db`	Base de données
`perf.network`	Infrastructure réseau
`perf.service`	Dégradation du service
`perf.storage`	Rangement
`perf.virtual`	Virtualisation des ordinateurs de bureau et des applications
`perf.web`	Application Web

Groupe d'appareils

Groupes d'appareils peut être statique ou dynamique.

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

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

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

Fonctionnement	Descriptif
GET /devicegroups	Récupérez tous les groupes d'équipements actifs au cours d'une période donnée.
POST/groupes d'appareils	Créez un nouveau groupe d'équipements.
SUPPRIMER /devicegroups/ {id}	Supprimez un groupe déquipements.
OBTENEZ /devicegroups/ {id}	Récupérez un groupe déquipements spécifique.
PATCH /devicegroups/ {id}	Mettez à jour un groupe d'équipements spécifique.
GET /devicegroups/ {id} /alertes	Tout récupérer alertes qui sont affectés à un groupe d'équipements spécifique.

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

Détails de l'opération

```
GET /devicegroups
```

Spécifiez les paramètres suivants.

`since:` ***Numéro***

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

`all:` ***Booléen***

(Facultatif) Obsolète. Remplacé par le paramètre type.

`name:` ***Corde***

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

`type:` ***Corde***

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

Les valeurs suivantes sont valides :

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

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

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

`GET /devicegroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

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

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

`POST /devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Appliquez les valeurs de propriété spécifiées au nouveau groupe dcesséquipements.

`description:` ***Corde***

Description facultative du groupe dO'équipements.

`name:` ***Corde***

Le nom convivial du groupe dcesséquipements.

`include_custom_devices:` ***Booléen***

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

`dynamic:` ***Booléen***

(Facultatif) Indique si le groupe dafficheurs est dynamique.

`field:` ***Corde***

Obsolète. Remplacé par le paramètre de filtre.

Les valeurs suivantes sont valides :

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

`value:` ***Objet***

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

`filter:` ***Objet***

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

`field:` ***Corde***

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

Les valeurs suivantes sont valides :

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

- instance_name
- instance_type
- cloud_account
- vpc_id
- subnet_id
- is_active
- network_locality_type
- network_locality_id
- id

`operator:` ***Corde***

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

Les valeurs suivantes sont valides :

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

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

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

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

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

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

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

Spécifiez le paramètre body au format JSON suivant.

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

```
    },
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`DELETE /devicegroups/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`PATCH /devicegroups/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

`description:` ***Corde***

Description facultative du groupe dO'équipements.

`name:` ***Corde***

Le nom convivial du groupe dcesséquipements.

`include_custom_devices:` ***Booléen***

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

`field:` ***Corde***

Obsolète. Remplacé par le paramètre de filtre.

Les valeurs suivantes sont valides :

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

`value:` ***Objet***

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

`filter:` ***Objet***

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

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

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

Spécifiez le paramètre body au format JSON suivant.

```
{
    "description": "string",
    "editors": [],
```

```
    "field": "string",
    "filter": {},
    "include_custom_devices": true,
    "name": "string",
    "value": "string"
}
```

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`direct_assignments_only:` ***Booléen***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/triggers`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`direct_assignments_only:` ***Booléen***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique d'un équipement.

`id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique d'un équipement.

`id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

`POST /devicegroups/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***
La liste des identifiants uniques pour les appareils attribués et non attribués au groupe dcesséquipements.

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

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

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

`GET /devicegroups/{id}/devices`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du groupe dcesséquipements.

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

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

`limit:` ***Numéro***

(Facultatif) Limitez le nombre d'appareils retournés.

`offset:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

Appareil

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

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

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

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

Détails de l'opération

`GET /devices`

Spécifiez les paramètres suivants.

`active_from:` ***Numéro***

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

`active_until:` ***Numéro***

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

`limit:` ***Numéro***

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

`offset:` ***Numéro***

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

`search_type:` ***Corde***

Indique le champ dans lequel effectuer la recherche.

Les valeurs suivantes sont valides :

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

`value:` ***Corde***

(Facultatif) Spécifie les critères de recherche.

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

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

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


`POST /devices/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les critères relatifs à l'équipement.

`active_from:` ***Numéro***

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

`active_until:` ***Numéro***

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

`limit:` ***Numéro***

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

`offset:` ***Numéro***

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

`filter:` ***Objet***

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

`field:` ***Corde***

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

Les valeurs suivantes sont valides :

- name
- discovery_id
- ipaddr
- macaddr
- vendor
- tag
- activity
- node
- vlan
- discover_time
- role
- dns_name
- dhcp_name
- netbios_name
- cdp_name
- custom_name
- software
- model
- is_critical
- instance_id
- instance_name
- instance_type
- cloud_account
- vpc_id
- subnet_id
- is_active
- analysis
- network_locality_type
- network_locality_id
- id

operator: ***Corde***

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

Les valeurs suivantes sont valides :

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

- `in`
- `not_in`

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

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

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

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

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

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

Les valeurs suivantes sont valides :

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

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

Spécifiez le paramètre body au format JSON suivant.

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

`GET /devices/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

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

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

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

`PATCH /devices/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

`id:` ***Numéro***

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

`GET /devices/{id}/activity`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

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

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

`GET /devices/{id}/ipaddrs`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`from:` ***Numéro***

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

`until:` ***Numéro***

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

`GET /devices/{id}/dnsnames`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`from:` ***Numéro***

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

`until:` ***Numéro***

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

`GET /devices/{id}/triggers`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`direct_assignments_only:` ***Booléen***

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

`POST /devices/{id}/triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du déclencheur.

`id:` ***Numéro***

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

`GET /devices/{id}/dashboards`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`GET /devices/{id}/devicegroups`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique de l'équipement.

`active_from:` ***Numéro***

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

`active_until:` ***Numéro***

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

`POST /devices/{id}/devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

Identifiant unique du groupe dcesséquipements.

`id:` ***Numéro***

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

`GET /devices/{id}/tags`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`POST /devices/{id}/tags`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de la balise.

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de la balise.

`id:` ***Numéro***

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

`GET /devices/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`direct_assignments_only:` ***Booléen***

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

`POST /devices/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***

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

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

Identifiants des ressources à attribuer

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

Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'alerte.

`id:` ***Numéro***

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

`GET /devices/{id}/software`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

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

`from:` ***Numéro***

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

`until:` ***Numéro***

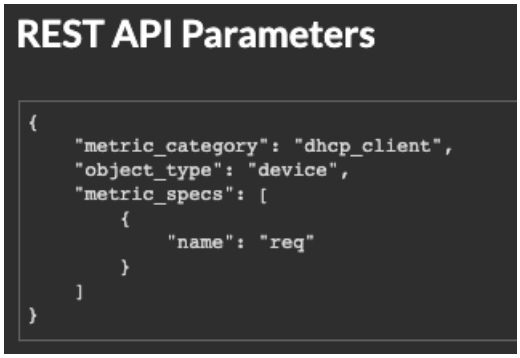
(Facultatif) Renvoie le logiciel observé sur l'équipement avant la date spécifiée, exprimée en millisecondes depuis l'époque.

Valeurs d'opérandes pour la recherche d'équipements

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

`activity`

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



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

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

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

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

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

analyse

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

standard
: Appareils en Analyse standard.

avancé
: Appareils en Analyse avancée.

découverte
: Appareils en mode de découverte.

l2_exempté
: Appareils dans L2 Parent Analysis.

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

`discover_time`

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

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

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

`discovery_id`

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

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

identifiant

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

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

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

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

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

est_actif

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

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

`ipaddr`

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

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

`node`

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

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

`macaddr`

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

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

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

`model`

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

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

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

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

`name`

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

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

identifiant_localité_réseau

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

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

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

`role`

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

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

`software`

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

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

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

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

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

`software_type`

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

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

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

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

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

`tag`

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

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

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

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

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

vlan

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

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

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

Pour certains `field` valeurs, la chaîne peut être en syntaxe regex. Spécifiez le `operand` valeur en tant qu'objet ayant un `value` paramètre avec la syntaxe regex que vous souhaitez faire correspondre et un

`is_regex` paramètre défini sur `true`. L'exemple suivant renvoie les résultats pour tous les noms DNS qui se terminent par `com`.

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

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

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

Unités de temps prises en charge

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

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

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

Unité de temps	Suffixe d'unité
Année	`y`
Mois	`M`
Semaine	`w`

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

Intervalles d'exclusion

Un intervalle d'exclusion peut être créé pour définir une période de suppression d'un alerte.

Par exemple, si vous ne souhaitez pas être informé des alertes en dehors des heures de bureau ou le week-end, un intervalle d' exclusion peut créer une règle pour supprimer l'alerte pendant cette période. Pour plus d' informations, voir Alertes.

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

Fonctionnement	Descriptif
GET /intervalles d'exclusion	Récupérez tous les intervalles d'exclusion.
Intervalles POST /exclusion	Créez un nouvel intervalle d'exclusion.
SUPPRIMER /exclusioninterval/{id}	Supprimez un intervalle d'exclusion spécifique.
OBTENEZ /exclusioninterval/{id}	Récupérez un intervalle d'exclusion spécifique.
PATCH /exclusionintervals/ {id}	Appliquez les mises à jour à un intervalle d'exclusion spécifique.

Détails de l'opération

`GET /exclusionintervals`

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

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
```

```
    "id": 0,
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`POST /exclusionintervals`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Définissez les valeurs de propriétés spécifiées sur le nouvel intervalle d'exclusion.

`name:` ***Corde***

Nom convivial de l'intervalle d'exclusion.

`author:` ***Corde***

(Facultatif) Le nom du créateur de l'intervalle d'exclusion.

`description:` ***Corde***

(Facultatif) Description facultative de l'intervalle d'exclusion.

`interval_type:` ***Corde***

La fenêtre temporelle pendant laquelle l'intervalle d'exclusion a été évalué.

Les valeurs suivantes sont valides :

- `onetime`
- `weekly`
- `daily`

`start:` ***Numéro***

Début de la plage de temps de l'intervalle d'exclusion, exprimé en secondes. Cette valeur est relative à l'époque pour les exclusions ponctuelles, par rapport à minuit pour les exclusions quotidiennes et par rapport au lundi à minuit pour les exclusions hebdomadaires.

`end:` ***Numéro***

Fin de la plage de temps de l'intervalle d'exclusion, exprimée en secondes. Cette valeur est relative à l'époque pour les exclusions ponctuelles, par rapport à minuit pour les exclusions quotidiennes et par rapport au lundi à minuit pour les exclusions hebdomadaires.

`alert_apply_all:` ***Booléen***

Indique si cet intervalle d'exclusion doit être appliqué à toutes les alertes.

`trend_apply_all:` ***Booléen***

Indique si cet intervalle d'exclusion doit être appliqué à toutes les tendances.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "interval_type": "string",
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`GET /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.

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

```
{
    "alert_apply_all": true,
    "author": "string",
    "description": "string",
    "end": 0,
    "id": 0,
    "interval_type": "string",
    "mod_time": 0,
    "name": "string",
    "start": 0,
    "trend_apply_all": true
}
```

`DELETE /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.

`PATCH /exclusionintervals/{id}`

Spécifiez les paramètres suivants.

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

`id:` ***Numéro***
Identifiant unique de l'intervalle d'exclusion.

Enquêtes

Les enquêtes vous permettent d'ajouter et de visualiser plusieurs détections sur une seule chronologie et une seule carte. Pour plus d'informations, voir Enquêtes.

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

opération	Descriptif
GET /enquêtes	Récupérez toutes les enquêtes.
POST /enquêtes	Créez une investigation.
POST /enquêtes/recherche	Recherchez des enquêtes.
SUPPRIMER /investigations/ {id}	Supprimer une investigation spécifique.
GET /investigations/ {id}	Récupérez une investigation spécifique.
PATCH /investigations/ {id}	Mettez à jour une enquête.

Détails de l'opération

`GET /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique pour l'investigation.

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

```
{
    "assessment": "string",
    "assignee": "string",
    "created_by": "string",
    "creation_time": 0,
    "description": "string",
    "detections": [
        "string"
    ],
    "end_time": 0,
    "id": 0,
    "investigation_types": [
        "string"
    ],
    "is_user_created": true,
    "last_interaction_by": "string",
    "name": "string",
    "notes": "string",
    "start_time": 0,
    "status": "string",
    "update_time": 0,
    "url": "string"
}
```

`GET /investigations`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "assessment": "string",
    "assignee": "string",
    "created_by": "string",
    "creation_time": 0,
    "description": "string",
    "detections": [
        "string"
    ],
    "end_time": 0,
    "id": 0,
    "investigation_types": [
        "string"
    ],
    "is_user_created": true,
    "last_interaction_by": "string",
    "name": "string",
    "notes": "string",
    "start_time": 0,
    "status": "string",
    "update_time": 0,
```

```
    "url": "string"
}
```

`POST /investigations/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de l'enquête.

`update_time:` ***Numéro***

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

`creation_time:` ***Numéro***

Renvoie les enquêtes créées après la date spécifiée, exprimée en millisecondes depuis l'époque.

`is_user_created:` ***Booléen***

(Facultatif) Renvoie uniquement les enquêtes créées manuellement par un utilisateur.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "creation_time": 0,
    "is_user_created": true,
    "update_time": 0
}
```

`PATCH /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'ID de l'investigation à mettre à jour.

`body:` ***Objet***

Les champs d'investigation à mettre à jour.

`name:` ***Corde***

(Facultatif) Le nom de l'enquête.

`status:` ***Corde***

(Facultatif) L'état de l'enquête.

Les valeurs suivantes sont valides :

- `open`
- `in_progress`
- `closed`

`notes:` ***Corde***

(Facultatif) Remarques facultatives concernant l'enquête.

`event_ids:` ***Tableau de nombres***

(Facultatif) La liste des identifiants pour les détections dans le cadre de l'investigation. Si vous spécifiez ce champ, la nouvelle liste d'identifiants remplace la liste existante.

`assignee:` ***Corde***

(Facultatif) Le nom d'utilisateur de la personne chargée de l'enquête.

`assessment:` ***Corde***

(Facultatif) L'évaluation de l'enquête.

Les valeurs suivantes sont valides :

- `malicious_true_positive`
- `benign_true_positive`
- `false_positive`
- `undecided`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "event_ids": [],
    "name": "string",
    "notes": "string",
    "status": "string"
}
```

`POST /investigations`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les domaines de la nouvelle enquête.

`name:` ***Corde***

Le nom de l'enquête.

`status:` ***Corde***

(Facultatif) L'état de l'enquête.

Les valeurs suivantes sont valides :

- `open`
- `in_progress`
- `closed`

`notes:` ***Corde***

(Facultatif) Remarques facultatives concernant l'enquête.

`event_ids:` ***Tableau de nombres***

(Facultatif) La liste des identifiants pour les détections dans le cadre de l'investigation.

`assignee:` ***Corde***

(Facultatif) Le nom d'utilisateur de la personne chargée de l'enquête.

`assessment:` ***Corde***

(Facultatif) L'évaluation de l'enquête.

Les valeurs suivantes sont valides :

- `malicious_true_positive`
- `benign_true_positive`
- `false_positive`
- `undecided`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "assessment": "string",
    "assignee": "string",
    "event_ids": [],
    "name": "string",
```

```
    "notes": "string",
    "status": "string"
}
```

`DELETE /investigations/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'ID de l'investigation à supprimer.

Métriques

Des informations métriques sont collectées sur chaque objet identifié par le système ExtraHop.

Notez que les métriques sont récupérées via la méthode POST, qui crée une requête pour collecter les informations demandées via l'API. Pour plus d'informations, voir Extraire des métriques via l'API REST.

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

opération	Descriptif
POST /métriques	Récupère les métriques pour chaque objet spécifié.
GET /metrics/next/ {xid}	Si vous demandez des statistiques à un console avec le `POST /metrics`, `POST /metrics/total`, ou `POST /metrics/totalbyobject` opération, et vous spécifiez des objets qui ont été observés par plusieurs capteurs, la réponse contient le `xid` champ, plutôt que des données métriques. Vous pouvez récupérer des données métriques en spécifiant `xid` champ dans le `GET /metrics/next/{xid}` opération, qui renvoie des métriques provenant de l'un des capteurs connectés à la console. Répéter le `GET /metrics/next/{xid}` opération pour renvoyer des métriques provenant de capteurs supplémentaires. Une fois toutes les métriques récupérées, l'opération renvoie la valeur null. Si les métriques ne sont pas encore disponibles à partir de la sonde, la chaîne `again` est renvoyé. Patientez quelques secondes, puis réessayez. **Note:** La réponse peut contenir un `xid` champ, même si vous n'avez demandé que des métriques concernant un seul groupe d'équipements, car les groupes d'équipements peuvent contenir des appareils provenant de plusieurs capteurs.
POST /métriques/total	Récupère les totaux métriques combinés pour tous les objets spécifiés.
POST /métriques/total par objet	Récupère les totaux métriques pour chaque objet spécifié.

Par exemple, le corps de requête suivant extrait les réponses HTTP envoyées par deux appareils au cours des 30 dernières minutes.

```
{
  "cycle": "auto",
  "from": -1800000,
  "metric_category": "http_server",
  "metric_specs": [
    {
      "name": "rsp"
    }
  ],
  "object_ids": [
    180, 177
  ],
  "object_type": "device",
  "until": 0
}
```

Pour `POST /metrics` opération, l'exemple de corps de requête précédent renvoie le nombre de réponses HTTP survenues au cours de chaque intervalle de temps, étiqueté avec l'heure de chaque événement et l'ID de l'équipement qui a envoyé les réponses, comme dans l'exemple de réponse suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659320000,
  "from": 1709657520000,
  "until": 1709659320000,
  "stats": [
    {
      "oid": 177,
      "time": 1709657520000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 177,
      "time": 1709657550000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 180,
      "time": 1709657520000,
      "duration": 30000,
      "values": [
        4
      ]
    },
    {
      "oid": 180,
      "time": 1709657550000,
      "duration": 30000,
      "values": [
        4
      ]
    }
```

```
  ]
}
```

Pour `POST /metrics/totalbyobject` opération, le même exemple de corps de requête précédent récupère le total combiné pour chaque équipement sur toute la période, comme dans l'exemple de réponse suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659620000,
  "from": 1709657820000,
  "until": 1709659620000,
  "stats": [
    {
      "oid": 180,
      "time": 1709659620000,
      "duration": 1830000,
      "values": [
        8
      ]
    },
    {
      "oid": 177,
      "time": 1709659620000,
      "duration": 1830000,
      "values": [
        8
      ]
    }
  ]
}
```

Pour `POST /metrics/total` opération, le même exemple de corps de requête précédent récupère le total combiné des deux appareils sur toute la période, comme dans l'exemple de réponse suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1709659830000,
  "from": 1709658030000,
  "until": 1709659830000,
  "stats": [
    {
      "oid": -1,
      "time": 1709659830000,
      "duration": 1830000,
      "values": [
        16
      ]
    }
  ]
}
```

Notez que le comportement du `/metrics/total` et `/metrics/totalbyobject` les points de terminaison dépendent du type de métrique. Pour les mesures de comptage, le `values` Le champ contient la somme totale des valeurs sur l'intervalle de temps spécifié, comme indiqué dans l'exemple ci-dessus. Toutefois, pour les métriques des ensembles de données, le `values` Le champ contient une liste de valeurs et la fréquence à laquelle ces valeurs sont apparues. Par exemple, une requête concernant les temps

de traitement du serveur avec le `POST /metrics/total` L'opération renvoie une réponse similaire à l'exemple suivant :

```
{
  "cycle": "30sec",
  "node_id": 0,
  "clock": 1494541440000,
  "from": 1494539640000,
  "until": 1494541440000,
  "stats": [
    {
      "oid": -1,
      "time": 1494541380000,
      "duration": 1800000,
      "values": [
        [
          {
            "value": 2.271,
            "freq": 5
          },
          {
            "value": 48.903,
            "freq": 1
          }
        ]
      ]
    }
  ]
}
```

S'il existe plus de 1 000 valeurs d'ensemble de données distinctes au cours de la période spécifiée, les valeurs similaires sont consolidées pour réduire la réponse à 1 000 valeurs. Par exemple, s'il y a moins de 1 000 valeurs, la réponse peut contenir les entrées suivantes :

```
{
  "value": 2.571,
  "freq": 4
},
{
  "value": 2.912,
  "freq": 2
}
```

Toutefois, si la réponse contient plus de 1 000 valeurs, ces entrées peuvent être consolidées dans l'entrée suivante :

```
{
  "value": 2.571,
  "freq": 6
}
```

Si le `calc_type` Le champ est spécifié et la réponse contient plus de 1 000 valeurs, le percentile ou la moyenne est calculé en fonction de l'ensemble de données consolidé.

Détails de l'opération

`POST /metrics`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

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

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent

également être des expressions régulières délimitées par des barres obliques (« / GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`POST /metrics/total`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

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

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`

- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent également être des expressions régulières délimitées par des barres obliques (« /GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

`POST /metrics/totalbyobject`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Description de la demande métrique.

`from:` ***Numéro***

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

`until:` ***Numéro***

L'horodateur de fin de la demande. Renvoie uniquement les statistiques collectées avant cette date. Suit les mêmes directives relatives aux valeurs temporelles que le paramètre from.

`cycle:` ***Corde***

Période d'agrégation des métriques.

Les valeurs suivantes sont valides :

- `auto`
- `1sec`
- `30sec`
- `5min`
- `1hr`
- `24hr`

`object_type:` ***Corde***

Indique le type d'objet des identificateurs uniques spécifiés dans la propriété object_ids.

Les valeurs suivantes sont valides :

- `network`
- `device`
- `application`
- `vlan`
- `device_group`
- `system`

`object_ids:` ***Tableau de nombres***

La liste des valeurs numériques qui représentent des identificateurs uniques. Les identifiants uniques peuvent être récupérés via les ressources /networks, /devices, /applications, /vlans, /devicegroups, /activitygroups et /appliances. Pour les mesures de santé du système, spécifiez l'ID de la sonde ou de la console et définissez le paramètre object_type sur « système ».

`metric_category:` ***Corde***

Groupe de mesures pouvant faire l'objet d'une recherche dans le catalogue de métriques.

`metric_specs:` ***Tableau d'objets***

Tableau d'objets de spécification métrique.

`name:` ***Corde***

Le nom du champ pour la métrique. Lors du filtrage dans le catalogue de métriques sur une metric_category, chaque résultat est un nom potentiel de metric_spec. Lorsqu'un résultat est sélectionné dans le catalogue, la valeur du champ « Métrique » est une option valide pour ce champ.

`key1:` ***Corde***

(Facultatif) Filtrez les mesures détaillées. Les métriques détaillées répartissent les données par clés, qui sont des chaînes ou des adresses IP. Par exemple, la métrique « Requêtes HTTP par méthode » accepte la valeur key1 de « GET ». Les clés peuvent également être des expressions régulières délimitées par des barres obliques (« /GET/ »).

`key2:` ***Corde***

(Facultatif) Activez un filtrage supplémentaire sur les mesures détaillées.

`calc_type:` ***Corde***

(Facultatif) Type de calcul à effectuer.

Les valeurs suivantes sont valides :

- `mean`
- `percentiles`

`percentiles:` ***Tableau de nombres***

(Facultatif) La liste des percentiles, triée par ordre croissant, qui doit être renvoyée. Ce paramètre n'est obligatoire que si le paramètre calc_type est défini sur « percentiles ». Si le paramètre calc_type est défini sur mean, la propriété percentiles ne peut pas être définie.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cycle": "string",
    "from": 0,
    "metric_category": "string",
    "metric_specs": {
        "name": "string",
        "key1": "string",
        "key2": "string",
        "calc_type": "string",
        "percentiles": []
    },
    "object_ids": [],
    "object_type": "string",
    "until": 0
}
```

```
GET /metrics/next/{xid}
```

Spécifiez les paramètres suivants.

`xid:` ***Numéro***
Identifiant unique renvoyé par une requête métrique.

Unités de temps prises en charge

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

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

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

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

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

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

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

```
{
    "from": "-2h",
    "until": "-1h",
```

```
    "types": ["~http"]
}
```

Entrée de localité sur le réseau

Vous pouvez gérer une liste qui indique la localité des adresses IP sur le réseau.

Par exemple, vous pouvez créer une entrée dans la liste des localités du réseau qui indique qu'une adresse IP ou un bloc CIDR est interne ou externe.

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

Fonctionnement	Descriptif
GET/networklocalities	Récupérez toutes les entrées de localité du réseau.
POST/networklocalities	Créez une entrée de localité du réseau.
SUPPRIMER /networklocalities/ {id}	Supprimez une entrée de localité du réseau.
GET /networklocalities/ {id}	Récupérez une entrée de localité de réseau spécifique.
PATCH /networklocalities/ {id}	Appliquez les mises à jour à une entrée de localité du réseau spécifique.

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.

Réseau

Les réseaux sont corrélés à la carte d'interface réseau qui reçoit les entrées de tous les objets identifiés par le système ExtraHop.

Sur un console, chaque sonde connectée est identifiée comme une capture réseau. Pour plus d'informations, voir Réseaux.

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

Opération	Descriptif
GET /réseaux	Récupérez tous les réseaux.
GET /networks/ {id}	Récupérez un réseau spécifique par identifiant.
PATCH /networks/ {id}	Mettez à jour un réseau spécifique par identifiant.
GET /networks/ {id} /alertes	Tout récupérer alertes qui sont affectés à un réseau spécifique.
POST /networks/ {id} /alertes	Attribuez et annulez les alertes à un réseau spécifique.
SUPPRIMER /networks/ {id} /alerts/ {child-id}	Annuler l'attribution d'une alerte à un réseau spécifique.
POST /networks/ {id} /alerts/ {child id}	Attribuez une alerte à un réseau spécifique.
GET /networks/ {id} /vlan	Récupérez tous les VLAN assignés à un réseau spécifique.

Détails de l'opération

`GET /networks`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
```

```
    "name": "string",
    "node_id": 0
}
```

`PATCH /networks/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Mises à jour de la valeur des propriétés à appliquer au réseau.

`id:` ***Numéro***
Identifiant unique du réseau.

`GET /networks/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

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

```
{
    "appliance_uuid": "string",
    "description": "string",
    "id": 0,
    "idle": true,
    "mod_time": 0,
    "name": "string",
    "node_id": 0
}
```

`GET /networks/{id}/alerts`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

`direct_assignments_only:` ***Booléen***
(Facultatif) Limitez les résultats aux seules alertes directement attribuées au réseau.

`POST /networks/{id}/alerts`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Listes d'identifiants d'alerte à attribuer et/ou à annuler.

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

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

Spécifiez le paramètre body au format JSON suivant.

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

```
}
```

`id:` ***Numéro***
Identifiant unique du réseau.

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

`GET /networks/{id}/vlans`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du réseau.

Observations

Une observation associe l'adresse IP d'un équipement du système ExtraHop à une adresse IP extérieure à votre réseau. Par exemple, vous pouvez suivre l'activité d'un utilisateur VPN en associant l'adresse IP du client VPN sur votre réseau interne à l' adresse IP externe attribuée à l'utilisateur sur l'Internet public.

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

Fonctionnement	Descriptif
POST /observations/associatedipaddrs	Ajoutez une observation pour créer une association entre les adresses IP des équipements.

Détails de l'opération

`POST /observations/associatedipaddrs`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Les paramètres d'observation.
`observations:` ***Tableau d'objets***
Une série d'observations.
`ipaddr:` ***Corde***
L'adresse IP de l'équipement observée par la sonde ou la console.

`associated_ipaddr:` ***Corde***

L'adresse IP associée.

`timestamp:` ***Numéro***

Heure à laquelle l'observation a été créée par la source, exprimée en millisecondes depuis l'époque.

`source:` ***Corde***

La source des observations.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "observations": {
        "ipaddr": "string",
        "associated_ipaddr": "string",
        "timestamp": 0
    },
    "source": "string"
}
```

Recherche par paquets

Vous pouvez rechercher et télécharger des paquets stockés sur le système ExtraHop. Le téléchargé les paquets peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

Pour plus d'informations sur les paquets, voir Paquets.

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

Fonctionnement	Descriptif
GET /packets/search	Recherchez des paquets en spécifiant des paramètres dans une URL.
POST /paquets/search	Recherchez des paquets en spécifiant des paramètres dans une chaîne JSON.

Détails de l'opération

`GET /packets/search`

Spécifiez les paramètres suivants.

`output:` ***Corde***

(Facultatif) Format de sortie. * `pcap` - Un fichier PCAP qui contient des paquets. * `keylog_txt` - Un fichier texte keylog contenant des secrets pour le déchiffrement. * `pcapng` - Un fichier PCAPNG qui peut contenir à la fois des paquets et des secrets à déchiffrer. * `zip` - Un fichier ZIP qui contient à la fois un fichier texte PCAP et un keylog. * `extract` - Un fichier ZIP contenant des fichiers extraits de paquets correspondant à la requête. Cette option n'est valide que si vous disposez d'un accès complet au module NDR.

Les valeurs suivantes sont valides :

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`
- `extract`

`include_secrets:` ***Booléen***

(Facultatif) Spécifie s'il faut inclure des secrets dans le fichier PCAPNG. Cette option n'est valide que si la sortie est définie sur pcapng.

`decrypt_files:` ***Booléen***

(Facultatif) Spécifie s'il faut déchiffrer les fichiers extraits contenant des secrets stockés. Cette option n'est valide que si le paramètre « output » est « extract ».

`limit_bytes:` ***Corde***

(Facultatif) Le nombre maximum approximatif d'octets à renvoyer. Une fois que le système ExtraHop a trouvé des paquets correspondant à la taille spécifiée dans les critères de recherche, il arrête de rechercher des paquets supplémentaires. Cependant, étant donné que le système analyse plusieurs paquets à la fois, la taille totale des paquets renvoyés peut être supérieure à la taille spécifiée. L'unité par défaut est l'octet, mais vous pouvez spécifier d'autres unités avec un suffixe d'unité. La valeur par défaut est « 100 Mo ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 100 Mo », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`limit_search_duration:` ***Corde***

(Facultatif) Durée maximale approximative pour effectuer la recherche de paquets. Une fois le délai spécifié écoulé, le système ExtraHop arrête de rechercher des paquets supplémentaires. Cependant, le système va dépasser la durée spécifiée pour terminer l'analyse des paquets qui étaient recherchés avant l'expiration du délai, et le système analyse plusieurs paquets à la fois. Par conséquent, la recherche peut durer plus longtemps que la durée spécifiée. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. La valeur par défaut est « 5 m ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 5 m », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`always_return_body:` ***Booléen***

(Facultatif) Spécifie le comportement si la requête ne correspond à aucun paquet ou si les paquets correspondants à la requête ne contiennent aucun fichier. Si la valeur est vraie, le système renvoie un fichier vide et un code dquo 200. Si la valeur est fausse, le système renvoie un code dveloppement 204 mais ne renvoie pas de fichier.

`from:` ***Corde***

L'horodateur de début de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -10m pour commencer la recherche avec les paquets capturés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera avec les paquets capturés au moment de la recherche. Une valeur négative indique que la recherche se terminera par des paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -5m pour terminer la recherche avec les paquets capturés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`bpf:` ***Corde***

(Facultatif) La syntaxe du filtre de paquets de Berkeley (BPF) pour la recherche de paquets. Pour plus d'informations sur la syntaxe BPF, consultez Guide de l'API REST.

`ip1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`ip2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`POST /packets/search`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les paramètres de la recherche de paquets.

`output:` ***Corde***

(Facultatif) Format de sortie.

Les valeurs suivantes sont valides :

- `pcap`
- `keylog_txt`
- `pcapng`
- `zip`
- `extract`

`include_secrets:` ***Booléen***

(Facultatif) Indique s'il faut inclure ou non les secrets TLS avec les données des paquets dans les fichiers .pcapng. Valide uniquement si « output » est « pcapng ».

`decrypt_files:` ***Booléen***

(Facultatif) Spécifie s'il faut déchiffrer les fichiers extraits contenant des secrets stockés. Cette option n'est valide que si le paramètre « output » est « extract ».

`limit_bytes:` ***Corde***

(Facultatif) Le nombre maximum approximatif d'octets à renvoyer. Une fois que le système ExtraHop a trouvé des paquets correspondant à la taille spécifiée dans les critères de recherche, il arrête de rechercher des paquets supplémentaires. Cependant, étant donné que le système analyse plusieurs paquets à la fois, la taille totale des paquets renvoyés peut être supérieure à la taille spécifiée. L'unité par défaut est l'octet, mais vous pouvez spécifier d'autres unités avec un suffixe d'unité. La valeur par défaut est « 100 Mo ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 100 Mo », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`limit_search_duration:` ***Corde***

(Facultatif) Durée maximale approximative pour effectuer la recherche de paquets. Une fois le délai spécifié écoulé, le système ExtraHop arrête de rechercher des paquets supplémentaires. Cependant, le système va dépasser la durée spécifiée pour terminer l'analyse des paquets qui étaient recherchés avant l'expiration du délai, et le système analyse plusieurs paquets à la fois. Par conséquent, la recherche peut durer plus longtemps que la durée spécifiée. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. La valeur par défaut est « 5 m ». **Remarque** : Si la sortie est « extraire », il existe une valeur maximale pour ce champ. Le maximum par défaut est « 5 m », mais le maximum peut être modifié dans la configuration en cours. Si la sortie n'est pas « extraire », il n'y a pas de valeur maximale.

`always_return_body:` ***Booléen***

(Facultatif) Spécifie le comportement si la requête ne correspond à aucun paquet ou si les paquets correspondants à la requête ne contiennent aucun fichier. Si la valeur est vraie, le système renvoie un fichier vide et un code dquo 200. Si la valeur est fausse, le système renvoie un code dveloppement 204 mais ne renvoie pas de fichier.

`from:` ***Corde***

L'horodateur de début de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -10m pour commencer la recherche avec les paquets capturés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de la plage de temps que la recherche inclura, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera avec les paquets capturés au moment de la recherche. Une valeur négative indique que la recherche se terminera par des paquets capturés à un moment donné dans le passé. Par exemple, spécifiez -5m pour terminer la recherche avec les paquets capturés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`bpf:` ***Corde***

(Facultatif) La syntaxe du filtre de paquets de Berkeley (BPF) pour la recherche de paquets. Pour plus d'informations sur la syntaxe BPF, voir Filtrer les paquets avec la syntaxe du filtre de paquets de Berkeley.

`ip1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port1:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

`ip2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés ou reçus par l'adresse IP spécifiée.

`port2:` ***Corde***

(Facultatif) Renvoie les paquets envoyés depuis ou reçus sur le port spécifié.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "always_return_body": true,
    "bpf": "string",
    "decrypt_files": true,
    "from": "string",
    "include_secrets": true,
    "ip1": "string",
    "ip2": "string",
    "limit_bytes": "string",
    "limit_search_duration": "string",
    "output": "string",
    "port1": "string",
    "port2": "string",
    "until": "string"
}
```

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.

Avant de commencer
Vous pouvez accéder à cette ressource d'API REST uniquement si votre système RevealX 360 dispose d'un espace de stockage des enregistrements basé sur le cloud avec Premium Investigation.

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

opération	Descriptif
`GET /records/cursor/{cursor}`	Obsolète. Remplacé par `POST /records/cursor`.
`POST /records/cursor`	Récupère les enregistrements en commençant par un curseur spécifié.
`POST /records/search`	Effectuez une requête dans le journal d'enregistrement.

Détails de l'opération

```
POST /records/search
```

Spécifiez les paramètres suivants.

`body:` ***Objet***
Requête du journal d'enregistrement.

`from:` ***Numéro***
L'horodateur de début de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Une valeur négative indique que la recherche débutera avec les enregistrements créés dans le passé. Par exemple, spécifiez -600 000 ms pour commencer la recherche avec les enregistrements créés 10 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

`until:` ***Numéro***

L'horodateur de fin de la plage de temps recherchée par la requête, exprimé en millisecondes depuis l'époque. Une valeur 0 indique que la recherche se terminera par les enregistrements créés au moment de la demande. Une valeur négative indique que la recherche se terminera par des enregistrements créés dans le passé. Par exemple, spécifiez -300 000 ms pour terminer la recherche avec les enregistrements créés 5 minutes avant l'heure de la demande. Les valeurs négatives peuvent être spécifiées avec une unité de temps autre que les millisecondes, telle que les secondes ou les heures. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge.

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

(Facultatif) Tableau d'un ou de plusieurs formats d'enregistrement. La requête renvoie uniquement les enregistrements correspondant aux formats spécifiés. Si aucune valeur n'est spécifiée, la requête renvoie des enregistrements de n'importe quel type. Les valeurs valides pour ce champ sont affichées dans le champ Type d'enregistrement de la page Formats d'enregistrement. Par exemple : « ~cifs ».

`limit:` ***Numéro***

Le nombre maximum d'enregistrements renvoyés par la requête. La valeur maximale ne peut pas dépasser 10 000. La valeur par défaut est 100.

`offset:` ***Numéro***

Le nombre d'enregistrements à ignorer dans les résultats de la requête. La requête renverra des enregistrements à partir de la valeur de décalage. Ce paramètre est souvent associé aux paramètres de limite et de tri. La valeur par défaut est 0. Pour les magasins d'enregistrements ExtraHop, la valeur maximale est de 10 000 ; pour récupérer les enregistrements renvoyés après les 10 000 premiers, consultez POST /records/cursor/. Pour les magasins de disques tiers, il n'y a pas de valeur maximale.

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

Liste d'un ou de plusieurs objets de tri qui spécifient les priorités de tri. Les enregistrements renvoyés sont triés dans l'ordre dans lequel les objets sont répertoriés. Les paramètres sont définis dans la section sort_item ci-dessous. Si aucune valeur sort_item n'est fournie, les enregistrements sont triés par horodateur dans l'ordre décroissant.

`field:` ***Corde***

Le nom du champ qui a renvoyé les enregistrements est trié par.

`direction:` ***Corde***

L'ordre dans lequel les enregistrements renvoyés sont triés. L'ordre par défaut est décroissant. Une fois tous les autres critères de tri appliqués, ou si aucun critère de tri n'a été spécifié, l'ordre par défaut est décroissant par horodateur.

Les valeurs suivantes sont valides :

- `asc`
- `desc`

`filter:` ***Objet***

L'objet contenant les paramètres qui spécifient les critères de filtre. Les paramètres sont définis dans la section des filtres ci-dessous. Si aucune valeur de filtre n'est fournie, la requête renvoie tous les enregistrements correspondant à l'intervalle de temps et à tout format d'enregistrement spécifié.

`field:` ***Corde***

Le nom du champ de l'enregistrement à filtrer. La requête compare le contenu du paramètre de champ à la valeur du paramètre d'opérande. Si le nom de champ spécifié est « .any », l'union de toutes les valeurs de champ sera recherchée. Si le nom de champ spécifié est « .ipaddr » ou « .port », les rôles client, serveur, expéditeur et destinataire

sont inclus dans la recherche. Les noms des champs sont situés dans des formats d'enregistrement qui peuvent être visualisés dans le système ExtraHop.

`operator:` ***Corde***

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

Les valeurs suivantes sont valides :

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

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

La valeur à laquelle la requête tente de faire correspondre. La requête compare la valeur de l'opérande au contenu du paramètre de champ et applique la méthode de comparaison spécifiée par le paramètre de l'opérateur. Vous pouvez spécifier explicitement le type de données d'opérande comme décrit dans le Guide de l'API REST.

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

Liste d'un ou de plusieurs objets filtrants au sein d'un même objet filtrant. Les objets de filtre peuvent être intégrés de manière récursive. Seuls les opérateurs « et », « ou » et « non » sont autorisés pour ce paramètre.

`context_ttl:` ***Numéro***

Durée pendant laquelle le contexte de recherche reste actif. L'unité par défaut est la milliseconde, mais d'autres unités peuvent être spécifiées avec un suffixe d'unité. Consultez les Guide de l'API REST pour les unités de temps et les suffixes pris en charge. Dans RevealX Enterprise, ce champ n'est valide que si les enregistrements sont stockés sur un espace de stockage des enregistrements ExtraHop (tel qu'un EXA 5300) ou sur CrowdStrike LogScale. Dans RevealX 360, ce champ n'est valide que pour les systèmes dotés d'un espace de stockage des enregistrements basé sur le cloud avec Premium Investigation. Dans RevealX Enterprise avec CrowdStrike LogScale et RevealX 360 avec Premium Investigation, ce champ n'est pas valide si les champs de tri ou de décalage sont spécifiés.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "context_ttl": 0,
    "filter": {
        "field": "string",
        "operator": "string",
        "operand": "string",
```

```
        "rules": []
    },
    "from": 0,
    "limit": 0,
    "offset": 0,
    "sort": {
        "field": "string",
        "direction": "string"
    },
    "types": [],
    "until": 0
}
```

`POST /records/cursor`

Spécifiez les paramètres suivants.

`body:` ***Objet***

L'ID du curseur qui indique la page suivante de résultats de la requête.

`cursor:` ***Corde***

Identifiant unique du curseur qui indique la page de résultats suivante de la requête.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cursor": "string"
}
```

`context_ttl:` ***Numéro***

(Facultatif) Durée pendant laquelle le contexte de recherche reste actif, exprimée en millisecondes. Une fois la durée spécifiée écoulée, le curseur devient invalide et vous ne pouvez plus récupérer d'enregistrements supplémentaires à partir de la recherche. Spécifiez ce paramètre pour étendre le contexte de recherche spécifié précédemment.

`GET /records/cursor/{cursor}`

Spécifiez les paramètres suivants.

`cursor:` ***Corde***

L'ID du curseur.

`context_ttl:` ***Numéro***

(Facultatif) Durée pendant laquelle le contexte de recherche reste actif, exprimée en millisecondes.

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

```
{
    "cursor": "string",
    "from": 0,
    "lookback_exceeded": true,
    "lookback_truncated": true,
    "records": {},
    "total": 0,
    "until": 0,
    "warnings": {}
}
```

Valeurs des opérandes dans les requêtes d'enregistrement

Le `operand` champ dans le `POST /records/search` méthode spécifie la valeur à laquelle une requête d'enregistrement tente de correspondre. Vous pouvez spécifier la valeur uniquement ou à la fois le type de données et la valeur. Si vous spécifiez uniquement la valeur, la requête fera référence au format dac.enregistrement associé au `field` paramètre pour déterminer le type de données de la valeur.

Par exemple, si vous souhaitez rechercher une adresse IP, vous pouvez spécifier un type de données d'adresse IP, puis fournir l'adresse réelle comme valeur.

L'exemple suivant spécifie explicitement le type de données et la valeur de l' opérande :

```
{
    "from": -1000,
    "filter": {
        "field" : "senderAddr",
        "operator": "=",
        "operand" : { "type" : "ipaddr4", "value": "1.2.3.4" }
    }
}
```

L'exemple suivant indique uniquement la valeur de l' opérande :

```
{
    "from": -1000,
    "filter": {
        "field" : "senderAddr",
        "operator": "=",
        "operand" : "1.2.3.4"
    }
}
```

Vous pouvez spécifier explicitement les types de données suivants dans le `operand` champ :

- application
- booléen
- équipement

  Note: Vous devez spécifier l'ID de découverte de l'équipement dans le champ de valeur. Vous pouvez trouver l'identifiant de découverte d'un équipement via le `POST /devices/search` opération.
- filtre_appareil
- groupe_d'appareils
- interface de flux
- réseau de flux
- ipad dr4
- ipad dr6
- nombre
- localité_réseau
- objet
- chaîne

Le `operand` le champ prend en charge la notation CIDR lors du filtrage par adresse IP ; le `operator` le champ doit être défini sur « = » ou « ! = ».

Vous pouvez spécifier plusieurs filtres en incluant `rules` option, comme indiqué dans l' exemple suivant :

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

```
      {
        "field": "method",
        "operand": "SMB2_READ",
        "operator": "="
      },
      {
        "field": "reqL2Bytes",
        "operand": "100",
        "operator": ">"
      }
    ]
  },
  "types": [
    "~cifs"
  ],
    "from": "-30m"
}
```

Interrogez les enregistrements à l'aide d'un filtre de groupe déquipements

Pour filtrer les enregistrements par groupe déquipements dans l'API REST, vous devez envoyer un `POST` demande adressée au `/records/search` point de terminaison doté d'un filtre de requête d'enregistrement répondant aux critères suivants :

- Le `field` doit spécifier des périphériques, tels que `client`, `server`, `sender`, ou `receiver`.
- Le `operator` doit être soit `in` ou `not_in`.
- Le `operand type` doit être `device_group`.
- Le `operand value` doit être une représentation sous forme de chaîne de l'identifiant numérique du groupe déquipements. Vous pouvez récupérer les identifiants de groupes d'équipements en exécutant l'opération GET /devicegroup et en consultant le contenu du `id` champ dans la réponse.

Par exemple, la requête suivante recherche des enregistrements dans lesquels l' équipement client était membre d'un groupe déquipements avec un ID de 200 :

```
{
    "from": "-30m",
    "filter": {
        "field": "client",
        "operator": "in",
        "operand": {
            "type": "device_group",
            "value": "200"
        }
    }
}
```

Vous pouvez également filtrer les enregistrements en fonction de critères de groupe d'équipements sans créer de groupe de périphériques en spécifiant le type d'opérande comme `device_filter`. Par exemple, la requête suivante recherche les enregistrements dans lesquels l'équipement client exécute Windows 10 :

```
{
    "from": "-30m",
    "filter": {
        "field": "client",
        "operator": "in",
        "operand": {
            "type": "device_filter",
            "value": {
                "field": "software",
                "operand": "windows_10",
                "operator": "="
```

```
            }
        }
    }
}
```

Note: Valeurs d'opérande avec type `device_filter` pour la recherche d'enregistrements sont formatés de la même manière que les filtres de recherche d'équipements. Pour plus d'informations, voir Valeurs d'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`
Deuxième	`s`
Milliseconde	`ms`

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

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

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

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

Rapport

Un rapport est un fichier PDF d'un tableau de bord que vous pouvez planifier pour la livraison par e-mail à un ou plusieurs destinataires. Vous pouvez spécifier la fréquence à laquelle l'e-mail du rapport est envoyé et l'intervalle de temps pour les données du tableau de bord incluses dans le fichier PDF.

Important: Vous ne pouvez planifier des rapports qu'à partir d'une machine virtuelle ECA.

Voici quelques points importants à prendre en compte à propos des rapports de tableau de bord :

- Vous ne pouvez créer un rapport que pour les tableaux de bord dont vous êtes propriétaire ou qui ont été partagés avec vous. Votre capacité à créer un rapport dépend de vos privilèges d'utilisateur. Contactez votre administrateur ExtraHop pour obtenir de l'aide.
- Chaque rapport ne peut être lié qu'à un seul tableau de bord.
- Si vous avez créé un rapport pour un tableau de bord qui a ensuite été supprimé ou est devenu inaccessible, l'e-mail planifié continuera d'être envoyé aux destinataires. Toutefois, l'e-mail n'inclura pas le fichier PDF et informera les destinataires que le tableau de bord n'est pas disponible pour le propriétaire du rapport.

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

Fonctionnement	Descriptif
GET /rapports	Récupérez tous les rapports.
POST /rapports	Créez un rapport.

Fonctionnement	Descriptif
SUPPRIMER /reports/ {id}	Supprimez un rapport spécifique.
GET /rapports/ {id}	Récupérez un rapport spécifique.
PATCH /rapports/ {id}	Mettez à jour un rapport spécifique.
GET /reports/ {id} /contenu	Récupérez le contenu d'un rapport spécifique.
PUT /reports/ {id} /contenu	Remplacez le contenu d'un rapport spécifique.
GET /reports/ {id} /télécharger	Récupérez le PDF d'un rapport.
POST /reports/ {id} /file d'attente	Générez et envoyez immédiatement un rapport spécifique.

Détails de l'opération

`GET /reports`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`POST /reports`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Le contenu du rapport.

`name:` ***Corde***

Le nom du rapport.

`description:` ***Corde***

(Facultatif) Description du rapport.

`owner:` ***Corde***

Nom d'utilisateur du propriétaire du rapport.

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

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

`enabled:` ***Booléen***

(Facultatif) Indique si le rapport est activé.

`from:` ***Corde***

L'horodateur de début de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`until:` ***Corde***

(Facultatif) L'horodateur de fin de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`email_subject:` ***Corde***

(Facultatif) Le contenu de la ligne d'objet de l'e-mail de rapport.

`schedule:` ***Objet***

(Facultatif) Objet contenant les paramètres qui spécifient la plage horaire planifiée pour générer et envoyer le rapport. Les paramètres sont définis dans la section schedule_type ci-dessous.

`type:` ***Corde***

Type de calendrier de livraison du rapport.

Les valeurs suivantes sont valides :

- `hourly`
- `daily`
- `weekly`
- `monthly`

`at:` ***Tableau d'objets***

(Facultatif) La liste des objets qui spécifient les paramètres de diffusion du rapport. Les paramètres sont définis dans la section at_type ci-dessous.

`by_day:` ***Tableau de cordes***

(Facultatif) Les jours de la semaine où le rapport doit être envoyé.

Les valeurs suivantes sont valides :

- `mo`
- `tu`
- `we`
- `th`
- `fr`
- `sa`
- `su`

`on_day:` ***Numéro***

(Facultatif) Le jour du mois auquel le rapport sera exécuté.

`tz:` ***Corde***

(Facultatif) Fuseau horaire dans lequel envoyer le rapport.

`hour:` ***Numéro***

(Facultatif) Heure d'envoi du rapport.

`minute:` ***Numéro***

(Facultatif) La minute à laquelle le rapport doit être envoyé.

`interval:` ***Corde***

(Facultatif) L'intervalle peut être previous_week, previous_month ou rien.

Les valeurs suivantes sont valides :

- `previous_week`
- `previous_month`

`output:` ***Objet***

Objet contenant les paramètres qui spécifient le format de sortie du rapport. Les paramètres sont définis dans la section format_type ci-dessous.

`type:` ***Corde***

Format de sortie du rapport.

Les valeurs suivantes sont valides :

- `pdf`

`width:` ***Corde***

(Facultatif) Option de largeur pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `narrow`
- `medium`
- `wide`

`pagination:` ***Corde***

(Facultatif) Schéma de pagination pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `per_region`

`theme:` ***Corde***

(Facultatif) Thème d'affichage de la sortie du rapport.

Les valeurs suivantes sont valides :

- `light`
- `dark`
- `space`
- `contrast`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cc": [],
    "description": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "on_day": 0,
            "tz": "string",
            "hour": 0,
            "minute": 0
        },
        "interval": "string"
    },
```

```
    "until": "string"
}
```

`POST /reports/{id}/queue`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`PATCH /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`body:` ***Objet***
Le contenu du rapport.

`name:` ***Corde***
Le nom du rapport.

`description:` ***Corde***
(Facultatif) Description du rapport.

`owner:` ***Corde***
Nom d'utilisateur du propriétaire du rapport.

`cc:` ***Tableau de cordes***
La liste des adresses e-mail, non incluses dans un groupe d'e-mails, pour recevoir des rapports.

`enabled:` ***Booléen***
(Facultatif) Indique si le rapport est activé.

`from:` ***Corde***
L'horodateur de début de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`until:` ***Corde***
(Facultatif) L'horodateur de fin de l'intervalle de temps pour le contenu du rapport, par rapport à l'heure actuelle et exprimé en millisecondes.

`email_subject:` ***Corde***
(Facultatif) Le contenu de la ligne d'objet de l'e-mail de rapport.

`schedule:` ***Objet***
(Facultatif) Objet contenant les paramètres qui spécifient la plage horaire planifiée pour générer et envoyer le rapport. Les paramètres sont définis dans la section schedule_type ci-dessous.

`type:` ***Corde***
Type de calendrier de livraison du rapport.

Les valeurs suivantes sont valides :

- `hourly`
- `daily`
- `weekly`
- `monthly`

`at:` ***Tableau d'objets***

(Facultatif) La liste des objets qui spécifient les paramètres de diffusion du rapport. Les paramètres sont définis dans la section at_type ci-dessous.

`by_day:` ***Tableau de cordes***

(Facultatif) Les jours de la semaine où le rapport doit être envoyé.

Les valeurs suivantes sont valides :

- `mo`
- `tu`
- `we`
- `th`
- `fr`
- `sa`
- `su`

`on_day:` ***Numéro***

(Facultatif) Le jour du mois auquel le rapport sera exécuté.

`tz:` ***Corde***

(Facultatif) Fuseau horaire dans lequel envoyer le rapport.

`hour:` ***Numéro***

(Facultatif) Heure d'envoi du rapport.

`minute:` ***Numéro***

(Facultatif) La minute à laquelle le rapport doit être envoyé.

`interval:` ***Corde***

(Facultatif) L'intervalle peut être previous_week, previous_month ou rien.

Les valeurs suivantes sont valides :

- `previous_week`
- `previous_month`

`output:` ***Objet***

Objet contenant les paramètres qui spécifient le format de sortie du rapport. Les paramètres sont définis dans la section format_type ci-dessous.

`type:` ***Corde***

Format de sortie du rapport.

Les valeurs suivantes sont valides :

- `pdf`

`width:` ***Corde***

(Facultatif) Option de largeur pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `narrow`
- `medium`
- `wide`

`pagination:` ***Corde***

(Facultatif) Schéma de pagination pour la sortie du rapport.

Les valeurs suivantes sont valides :

- `per_region`

`theme:` ***Corde***

(Facultatif) Thème d'affichage de la sortie du rapport.

Les valeurs suivantes sont valides :

- `light`
- `dark`
- `space`
- `contrast`

Spécifiez le paramètre body au format JSON suivant.

```
{
    "cc": [],
    "description": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "name": "string",
    "output": {
        "type": "string",
        "width": "string",
        "pagination": "string",
        "theme": "string"
    },
    "owner": "string",
    "schedule": {
        "type": "string",
        "at": {
            "by_day": [],
            "on_day": 0,
            "tz": "string",
            "hour": 0,
            "minute": 0
        },
        "interval": "string"
    },
    "until": "string"
}
```

`GET /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

L'identifiant unique du rapport.

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

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
```

```
    "until": "string"
}
```

`GET /reports/{id}/download`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

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

```
{
    "cc": [],
    "description": "string",
    "email_message": "string",
    "email_subject": "string",
    "enabled": true,
    "from": "string",
    "id": 0,
    "include_links": "string",
    "name": "string",
    "output": {},
    "owner": "string",
    "schedule": {},
    "until": "string"
}
```

`DELETE /reports/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`GET /reports/{id}/contents`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

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

```
{
    "dashboard_id": 0,
    "params": {},
    "type": "string"
}
```

`PUT /reports/{id}/contents`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
L'identifiant unique du rapport.

`body:` ***Objet***
Le contenu du rapport.

Logiciel

Vous pouvez consulter la liste des logiciels que le système ExtraHop a observés sur votre réseau.

Fonctionnement	Descriptif
GET /logiciel	Récupérez le logiciel observé par le système ExtraHop.
GET /software/ {id}	Récupérez les logiciels observés par le système ExtraHop par identifiant.

Détails de l'opération

`GET /software`

Spécifiez les paramètres suivants.

`software_type:` ***Corde***
(Facultatif) Type de logiciel.

`name:` ***Corde***
(Facultatif) Le nom du logiciel.

`version:` ***Corde***
(Facultatif) Version du logiciel.

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

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

`GET /software/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique du logiciel.

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

```
{
    "description": "string",
    "id": "string",
    "name": "string",
    "software_type": "string",
    "version": "string"
}
```

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. **Note:** Si une collecte des menaces portant le même nom existe déjà sur le système ExtraHop, la collecte des menaces existante est remplacée.

opération	Descriptif
GET /threatcollections/ {id} /observables	Récupérez le nombre d'observables STIX chargés à partir d'une collecte des menaces, tels que l' adresse IP, le nom d'hôte ou l'URI.

Détails de l'opération

`GET /threatcollections`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "id": 0,
    "last_updated": 0,
    "name": "string",
    "observables": 0,
    "user_key": "string"
}
```

`POST /threatcollections`

Spécifiez les paramètres suivants.

`user_key:` ***Corde***
(Facultatif) Identifiant fourni par l'utilisateur pour la collecte des menaces. Si ce paramètre n'est pas spécifié, le nom de la collecte des menaces est défini pour cette valeur, sans espaces ni ponctuation.

`name:` ***Corde***
Nom de la collecte des menaces.

`file:` ***Nom du fichier***
Le nom de fichier de la collecte des menaces.

`PUT /threatcollections/~{userKey}`

Spécifiez les paramètres suivants.

`userKey:` ***Corde***
Identifiant fourni par l'utilisateur pour la collecte des menaces.

`name:` ***Corde***
(Facultatif) Nom de la collecte des menaces.

`file:` ***Nom du fichier***
(Facultatif) Nom du fichier pour la collecte des menaces.

`DELETE /threatcollections/{id}`

Spécifiez les paramètres suivants.

`id:` ***Corde***
Identifiant unique pour la collecte des menaces.

`GET /threatcollections/{id}/observables`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique pour la collecte des menaces.

Gâchette

Les déclencheurs sont des scripts personnalisés qui exécutent une action lors d'un événement prédéfini.

Par exemple, vous pouvez créer un déclencheur pour enregistrer une métrique personnalisée chaque fois qu'un HTTP une requête se produit ou classe le trafic pour un serveur particulier en tant que serveur d'applications. Pour plus d'informations, consultez le Référence de l'API Trigger. Pour des notes de mise en œuvre supplémentaires concernant les options avancées, voir Options de déclencheur avancées.

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

opération	Descriptif
GET /triggers	Récupérez tous les déclencheurs.
POST /déclencheurs	Créez un nouveau déclencheur.
POST/déclencheurs/données externes	Envoie des données à l'API Trigger en exécutant l'événement EXTERNAL_DATA. Vous pouvez accéder aux données via ExternalData classe de déclencheur. **Note:** Cette opération n'est pas disponible pour les appliances Command ou RevealX 360.
SUPPRIMER /triggers/ {id}	Supprimez un identifiant spécifique.
GET /triggers/ {id}	Récupérez un déclencheur spécifique par identifiant unique.
PATCH /triggers/ {id}	Mettez à jour un déclencheur existant.
GET /triggers/ {id} /devicegroups	Récupérez tout groupes d'équipements qui sont affectés à un déclencheur spécifique.
POST /triggers/ {id} /devicegroups	Attribuez et annulez l'attribution d'un déclencheur spécifique à des groupes d'équipements.
SUPPRIMER /triggers/ {id} /devicegroups/ {child-id}	Annulez l'attribution d'un groupe dveloppements à un déclencheur spécifique.
POST /triggers/ {id} /devicegroups/ {childid}	Assignez un groupe dproximatif d'équipements à un déclencheur spécifique.
GET /triggers/ {id} /appareils	Récupérez tous les appareils affectés à un déclencheur spécifique.
POST /triggers/ {id} /appareils	Attribuez et annulez l'attribution d'un déclencheur spécifique aux appareils.
SUPPRIMER /triggers/ {id} /devices/ {child-id}	Annulez l'attribution d'un équipement à un déclencheur spécifique.
POST /triggers/ {id} /devices/ {childid}	Assignez un équipement à un déclencheur spécifique.

Détails de l'opération

`GET /triggers`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`DELETE /triggers/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***

Identifiant unique du déclencheur.

`POST /triggers/externaldata`

Spécifiez les paramètres suivants.

`body:` ***Objet***

L'objet contenant les données à envoyer aux déclencheurs via l'événement EXTERNAL_DATA.

`type:` ***Corde***

Identifiant de chaîne qui décrit les données contenues dans le paramètre body. Par exemple, vous pouvez spécifier « phantom-data » pour les données envoyées depuis la plateforme Phantom SOAR.

`body:` ***Objet***

Les données à envoyer aux déclencheurs via l'événement EXTERNAL_DATA. Ces données sont accessibles dans le déclencheur à l'aide de la propriété « ExternalData.body ».

Spécifiez le paramètre body au format JSON suivant.

```
{
    "body": {},
    "type": "string"
}
```

`POST /triggers`

Spécifiez les paramètres suivants.

`body:` ***Objet***

Les valeurs des propriétés du nouveau déclencheur.

`name:` ***Corde***

Le nom convivial du déclencheur.

`description:` ***Corde***

(Facultatif) Description facultative du déclencheur.

`author:` ***Corde***

Le nom du créateur du déclencheur.

`script:` ***Corde***

Le contenu JavaScript du déclencheur.

`event:` ***Corde***

(Facultatif) Obsolète. Remplacé par le champ des événements.

`events:` ***Tableau de cordes***

La liste des événements sur lesquels le déclencheur s'exécute, exprimée sous forme de tableau JSON.

`disabled:` ***Booléen***

Indique si le déclencheur peut être exécuté.

`debug:` ***Booléen***

Indique si les instructions de débogage sont imprimées pour le déclencheur.

`apply_all:` ***Booléen***

Indique si le déclencheur s'applique à toutes les ressources pertinentes.

`hints:` ***Objet***

Options basées sur les événements déclencheurs sélectionnés. Pour plus d'informations sur l'objet hints, consultez Guide de l'API REST.

Spécifiez le paramètre body au format JSON suivant.

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
    "hints": {},
    "name": "string",
    "script": "string"
}
```

`PATCH /triggers/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***

La valeur de la propriété est mise à jour pour le déclencheur.

`id:` ***Numéro***

Identifiant unique du déclencheur.

`GET /triggers/{id}`

Spécifiez les paramètres suivants.

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

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

```
{
    "apply_all": true,
    "author": "string",
    "debug": true,
    "description": "string",
    "disabled": true,
    "event": "string",
    "events": [
        "string"
    ],
    "hints": {},
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "script": "string"
}
```

`GET /triggers/{id}/devicegroups`

Spécifiez les paramètres suivants.

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

`POST /triggers/{id}/devicegroups`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Liste d'identifiants uniques pour les groupes d'équipements affectés et non attribués à un déclencheur.

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

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

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

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

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

Spécifiez les paramètres suivants.

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

`GET /triggers/{id}/devices`

Spécifiez les paramètres suivants.

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

`POST /triggers/{id}/devices`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Liste d'identifiants uniques pour les appareils qui sont attribués et non affectés à un déclencheur.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre body au format JSON suivant.

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

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

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***
L'identifiant unique de l'équipement.
`id:` ***Numéro***
Identifiant unique du déclencheur.

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

Spécifiez les paramètres suivants.

`child-id:` ***Numéro***

L'identifiant unique de l'équipement.

`id:` ***Numéro***

Identifiant unique du déclencheur.

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.
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.

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***
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": {}
}
```

`PATCH /usergroups/{id}/members`

Spécifiez les paramètres suivants.

`id:` ***Corde***

Identifiant unique du groupe d'utilisateurs.

`body:` ***Corde***

Objet qui indique les utilisateurs à attribuer 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 indique 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"} assigne Alice et Bob comme seuls membres du groupe.

VLAN

Les réseaux locaux virtuels sont des groupements logiques de trafic ou de périphériques sur le réseau.

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

Fonctionnement	Descriptif
GET /vlan	Récupérez tous les VLAN
OBTENEZ /vlans/ {id}	Récupérez un VLAN spécifique.
PATCH /vlans/ {id}	Mettez à jour un VLAN spécifique.

Détails de l'opération

`GET /vlans`

Il n'existe aucun paramètre pour cette opération.

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

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
```

```
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`GET /vlans/{id}`

Spécifiez les paramètres suivants.

`id:` ***Numéro***
Identifiant unique du VLAN.

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

```
{
    "description": "string",
    "id": 0,
    "mod_time": 0,
    "name": "string",
    "network_id": 0,
    "node_id": 0,
    "vlanid": 0
}
```

`PATCH /vlans/{id}`

Spécifiez les paramètres suivants.

`body:` ***Objet***
Appliquez les mises à jour des valeurs de propriété spécifiées au VLAN.

`id:` ***Numéro***
Identifiant unique du VLAN.

Liste de surveillance

Pour garantir qu'un actif, tel qu'un serveur important, une base de données ou un ordinateur portable, bénéficie de la garantie Analyse avancée, vous pouvez ajouter cet équipement à la liste de surveillance.

Conseil: Si vous souhaitez ajouter plusieurs appareils à la liste de surveillance, pensez à créer un groupe d' appareils, puis à donner la priorité à ce groupe pour Analyse avancée.

Voici quelques considérations importantes concernant la liste de surveillance :

- La liste de surveillance s'applique uniquement à l'Analyse avancée.
- La liste de surveillance peut contenir autant d'appareils que le permet la capacité d'Analyse avancée, qui est déterminée par votre licence.
- Un équipement reste sur la liste de surveillance, qu'il soit inactif ou actif. Un équipement doit être actif pour que le système ExtraHop collecte les métriques d'Analyse avancée.

Pour plus d'informations sur l'Analyse avancée, voir Niveaux d'analyse.

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

Opération	Descriptif
SUPPRIMER /watchlist/device/ {id}	Supprimer un équipement de la liste de surveillance.
POST /watchlist/device/ {id}	Ajoutez un équipement à la liste de surveillance.

Opération	Descriptif
GET /watchliste/appareils	Récupérez tous les appareils figurant dans la liste de surveillance.
POST/liste de surveillance/appareils	Ajoutez ou supprimez des appareils de la liste de surveillance.

Détails de l'opération

`GET /watchlist/devices`

Il n'existe aucun paramètre pour cette opération.

`POST /watchlist/device/{id}`

Spécifiez les paramètres suivants.

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

`DELETE /watchlist/device/{id}`

Spécifiez les paramètres suivants.

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

`POST /watchlist/devices`

Spécifiez les paramètres suivants.

`assignments:` ***Objet***
Liste des appareils à ajouter ou à supprimer de la liste de surveillance.
`assign:` ***Tableau de nombres***
Identifiants des ressources à attribuer
`unassign:` ***Tableau de nombres***
Identifiants des ressources à annuler

Spécifiez le paramètre d'assignation au format JSON suivant.

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