

FAQ sur les priorités d'analyse

Publié: 2023-09-19

Voici quelques réponses aux questions fréquemment posées sur les priorités d'analyse.

- [Comment la capacité des appareils est-elle déterminée pour les niveaux d'analyse ?](#)
- [Où puis-je trouver mon utilisation actuelle ?](#)
- [Comment puis-je savoir quels appareils figurent sur la liste de surveillance ?](#)
- [Comment ajouter plusieurs appareils à la liste de surveillance ?](#)
- [Quel niveau d'analyse les dispositifs personnalisés reçoivent-ils ?](#)
- [Quel niveau d'analyse prend en charge les mesures personnalisées ?](#)
- [Quel niveau d'analyse prend en charge les déclencheurs ?](#)
- [Comment déterminer le niveau d'analyse d'un appareil ?](#)
- [Que se passe-t-il lorsqu'un dispositif prioritaire devient inactif ?](#)

Comment la capacité des appareils est-elle déterminée pour les niveaux d'analyse ?

Le nombre d'appareils pouvant bénéficier des niveaux d'analyse supérieurs varie en fonction de votre abonnement et de votre licence ExtraHop.

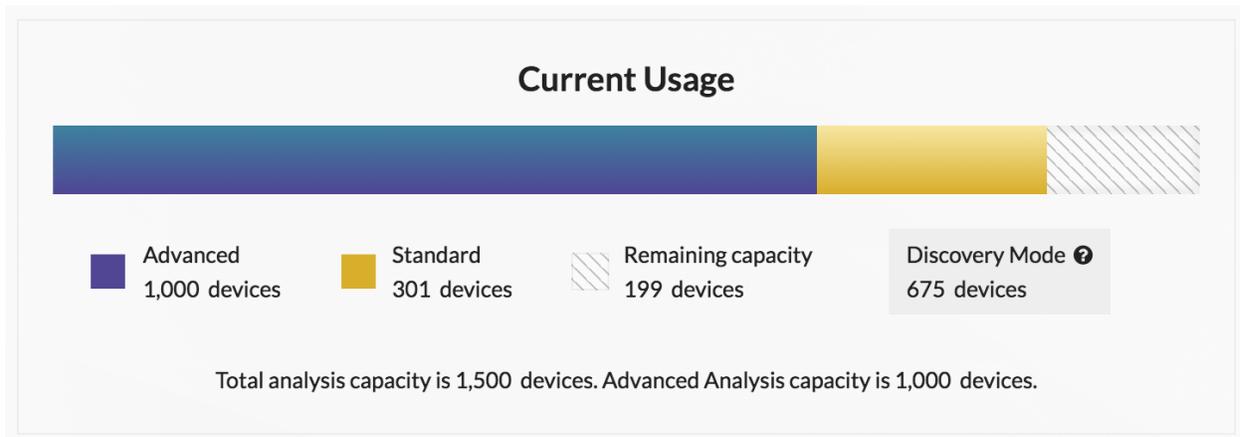
- Votre abonnement détermine la capacité d'analyse totale, c'est-à-dire le nombre d'appareils pouvant bénéficier de l'analyse standard ou de l'analyse avancée.
- Votre licence détermine la part de cette capacité totale disponible pour l'analyse avancée, qui est le niveau d'analyse le plus élevé.

Par exemple, la capacité d'analyse totale d'un EDA 9200 est de 50 000 appareils actifs simultanément. Jusqu'à 8 000 de ces appareils actifs peuvent être en analyse avancée. Contactez votre représentant ExtraHop pour plus d'informations sur la capacité d'analyse de chaque abonnement ExtraHop.

Où puis-je trouver mon utilisation actuelle ?

La page Priorités d'analyse affiche un graphique qui permet d'évaluer en un coup d'œil le nombre de dispositifs bénéficiant d'une analyse à chaque niveau par rapport à la capacité d'analyse restante. Cliquez sur l'icône Paramètres du système ⚙️, puis sur **Priorités d'analyse**.

Les capacités totales sous licence sont affichées sous le graphique ; les appareils en mode découverte ne sont pas pris en compte dans votre capacité totale.



Comment puis-je savoir quels appareils figurent sur la liste de surveillance ?

Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`, cliquez sur l'icône System Settings  puis sur **Analysis Priorities**. En haut de la page, cliquez sur **Afficher la liste de surveillance**.

Comment ajouter plusieurs appareils à la liste de surveillance ?

Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`. En haut de la page, cliquez sur **Assets**, puis sur **Devices** dans le volet de gauche. Recherchez des dispositifs sur la page de liste des dispositifs, puis cochez la case en regard de chaque dispositif que vous souhaitez ajouter à la liste de surveillance. Cliquez ensuite sur **Ajouter à la liste de surveillance** dans le coin supérieur droit de la page.

Pour plus d'informations, voir [Ajouter un appareil à la liste de surveillance](#).

Quel niveau d'analyse les dispositifs personnalisés reçoivent-ils ?

Les [dispositifs personnalisés](#) peuvent faire l'objet de n'importe quel niveau d'analyse. Vous pouvez [créer un groupe de](#) dispositifs avec tous vos dispositifs personnalisés et donner la priorité à ce groupe pour une analyse avancée ou standard. Vous pouvez également [ajouter un appareil personnalisé individuel à la liste de surveillance](#).

Quel niveau d'analyse prend en charge les mesures personnalisées ?

Les [mesures personnalisées](#) ne sont disponibles que dans l'analyse avancée. Si vous souhaitez voir les mesures personnalisées pour un appareil spécifique, donnez la priorité à un groupe contenant l'appareil ou ajoutez l'appareil à la liste de surveillance.

Quel niveau d'analyse prend en charge les déclencheurs ?

Un [déclencheur](#) s'exécute pour tout appareil auquel il est affecté, quel que soit le niveau d'analyse. Le niveau d'analyse d'un appareil n'affecte pas le moment où le déclencheur s'exécute. Toutefois, si un déclencheur affecté à un périphérique collecte des mesures personnalisées, vous devez donner la priorité à l'analyse avancée du périphérique avant de pouvoir afficher les données des mesures personnalisées.

Comment déterminer le niveau d'analyse d'un appareil ?

[Trouver un périphérique](#) Cliquez sur l'icône de l'appareil, puis sur son nom pour ouvrir la [page Présentation de l'appareil](#). Le niveau d'analyse est affiché dans la section des propriétés du dispositif.

Dans une liste de dispositifs, cliquez sur la colonne Niveau d'analyse pour trier les dispositifs par niveau.

[Extrayez la liste des appareils via l'API REST](#) et ajoutez une option de filtrage par niveau d'analyse. Des droits d'écriture complets sont requis pour exécuter des commandes via l'API REST.

Que se passe-t-il lorsqu'un dispositif prioritaire devient inactif ?

Un dispositif peut devenir inactif au fil du temps s'il n'a pas envoyé ou reçu de données au cours des 30 dernières minutes.

Un appareil inactif qui figure sur la liste de surveillance ou qui fait partie d'un groupe d'appareils ne consomme pas votre capacité d'analyse avancée ou standard. Lorsque l'appareil redevient actif, il reçoit une analyse avancée ou standard en fonction de la priorité configurée.

Si un périphérique est inactif pour un protocole spécifique et qu'il fait partie d'un groupe de périphériques prioritaires, il peut rester en analyse avancée ou standard pendant 96 heures maximum. Par exemple, un groupe de dispositifs Serveurs SSL est prioritaire pour l'analyse avancée. Un serveur qui reçoit généralement des requêtes SSL est inclus dans ce groupe. Si le serveur n'a pas envoyé ou reçu de données SSL au cours des 30 dernières minutes, mais qu'il continue d'envoyer et de recevoir des données via

d'autres protocoles, il reste en analyse avancée en tant que membre du groupe de dispositifs Serveurs SSL. Si le serveur est toujours inactif sur le protocole SSL après 96 heures, il n'est plus membre du groupe Serveurs SSL et peut cesser de recevoir l'analyse avancée.