

FAQ sur les priorités d'analyse

Publié: 2025-02-13

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

- [Comment fonctionnent les priorités d'analyse intelligentes ?](#)
- [Quel est l'ordre de priorité des priorités d'analyse ?](#)
- [Comment la capacité de l'équipement est-elle déterminée pour les niveaux d'analyse ?](#)
- [Où puis-je trouver mon utilisation actuelle ?](#)
- [Comment savoir quels appareils figurent sur la liste de surveillance ?](#)
- [Comment ajouter plusieurs appareils à la liste de surveillance ?](#)
- [Quel est le niveau d'analyse des appareils personnalisés ?](#)
- [Quel niveau d'analyse prend en charge les métriques personnalisées ?](#)
- [Quel niveau d'analyse prend en charge les déclencheurs ?](#)
- [Comment déterminer le niveau d'analyse d'un équipement ?](#)
- [Mes appareils reçoivent-ils toujours des observations logicielles s'ils sont en cours d'analyse standard ?](#)
- [Que se passe-t-il lorsqu'un équipement prioritaire devient inactif ?](#)

Comment fonctionnent les priorités d'analyse intelligentes ?

Le système ExtraHop priorise automatiquement les nouveaux appareils et les périphériques d'infrastructure critiques, tels que les serveurs Windows, pour une Analyse avancée.

Si un équipement a déjà été classé par ordre de priorité pour l'Analyse avancée par le système, il n'est pas nécessaire de l'ajouter manuellement à un groupe d'analyse ou à une liste de surveillance prioritaires. Nous vous recommandons de prendre en compte la priorisation définie par le système.

Les priorités configurées par l'utilisateur ont priorité sur les priorités d'analyse intelligentes appliquées par le système.

Quel est l'ordre de priorité des priorités d'analyse ?

La liste de surveillance, les groupes d'équipements configurés pour l'Analyse avancée, puis les règles intelligentes ExtraHop sont hiérarchisés jusqu'à ce que la capacité d'Analyse avancée soit pleine.

Ensuite, les groupes d'équipements configurés pour l'analyse standard, puis les règles intelligentes ExtraHop sont hiérarchisés jusqu'à ce que la capacité d'analyse standard soit pleine. Enfin, tous les appareils restants sont classés par ordre de priorité.

Comment la capacité de l'équipement est-elle déterminée pour les niveaux d'analyse ?

Le nombre d'appareils bénéficiant de niveaux d'analyse plus élevés 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 recevoir une Analyse standard ou une 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.

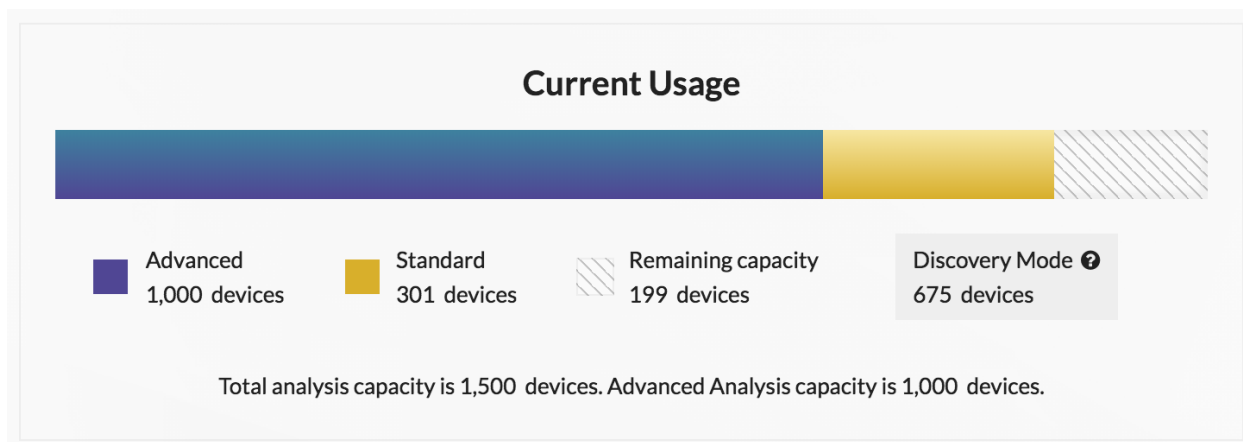
Par exemple, la capacité d'analyse totale d'un EDA 9200 est de 50 000 appareils actifs simultanément. Jusqu'à 8 000 de ces appareils actifs peuvent faire l'objet d'une Analyse avancée. Contactez votre représentant ExtraHop pour plus d'informations sur la capacité d'analyse de chaque abonnement ExtraHop.

Où puis-je trouver mon utilisation actuelle ?


La page Priorités d'analyse affiche un graphique qui montre en un coup d'œil une évaluation du nombre d'appareils faisant l'objet d'une analyse à chaque niveau par rapport à la capacité d'analyse restante.

Cliquez sur l'icône Paramètres système  puis cliquez sur **Priorités d'analyse**.

Les capacités totales autorisées sont affichées sous le graphique à barres.



Comment savoir quels appareils figurent sur la liste de surveillance ?

Connectez-vous au système ExtraHop via <https://<extrahop-hostname-or-IP-address>>, cliquez sur Paramètres du système , puis cliquez sur **Priorités d'analyse**. 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 **Actifs** puis cliquez sur **Appareils** dans le volet de gauche. Recherchez des appareils sur la page de liste des appareils, puis cochez la case à côté de chaque appareil que vous souhaitez ajouter à la liste de surveillance. Cliquez ensuite sur **Ajouter à la liste de suivi** dans le coin supérieur droit de la page.

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

Quel est le niveau d'analyse des appareils personnalisés ?

[Appareils personnalisés](#) peut recevoir n'importe quel niveau d'analyse. Tu peux [créer un groupe d'équipements](#) avec tous vos appareils personnalisés et donnez la priorité à ce groupe pour une analyse avancée ou standard. Ou tu peux [ajouter un équipement personnalisé à la liste de surveillance](#).

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

[Métriques personnalisées](#) ne sont disponibles que dans Analyse avancée. Si vous souhaitez consulter des statistiques personnalisées pour un équipement spécifique, donnez la priorité à un groupe contenant l'équipement ou ajoutez-le à la liste de surveillance.

Quel niveau d'analyse prend en charge les déclencheurs ?

UNE [déclencheur](#) s'exécutera pour tout équipement auquel il est affecté, quel que soit le niveau d'analyse. Le niveau d'analyse d'un équipement n'a aucune incidence sur le moment où le déclencheur est exécuté. Toutefois, si un déclencheur attribué à un équipement collecte des mesures personnalisées, vous devez donner la priorité à l'équipement pour l'Analyse avancée avant de pouvoir consulter les données métriques personnalisées.

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

Trouvez un équipement [🔗](#) puis cliquez sur le nom de l'équipement pour ouvrir [Page de présentation de l'appareil](#) [🔗](#). Le niveau d'analyse est affiché dans la section des propriétés de l'équipement.

Dans la liste des appareils, cliquez sur la colonne Niveau d'analyse pour trier les appareils par niveau.

[Extraire la liste des équipements via l' API REST](#) [🔗](#) et ajoutez une option pour filtrer par niveau d'analyse. Des privilèges d'écriture complets sont requis pour exécuter des commandes via l'API REST.

Mes appareils reçoivent-ils toujours des observations logicielles s'ils sont en cours d' analyse standard ?

Oui, des observations logicielles peuvent être créées pour les appareils aux niveaux Découverte, Standard ou Analyse avancée. Les observations logicielles aident le système à hiérarchiser automatiquement les appareils critiques, mais les appareils inactifs pendant 30 jours perdront leur priorité basée sur les observations logicielles.

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

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

Si un équipement est inactif pour un protocole spécifique et qu'il fait partie d'un groupe d'équipements prioritaire, il peut rester en analyse avancée ou standard pendant 96 heures au maximum. Par exemple, un groupe d'équipements de serveurs TLS est classé par priorité pour l'Analyse avancée. Un serveur qui reçoit généralement des requêtes TLS est inclus dans ce groupe. Si le serveur n'a pas envoyé ou reçu de données TLS au cours des 30 dernières minutes, mais continue d'envoyer et de recevoir des données via d'autres protocoles, le serveur reste en Analyse avancée en tant que membre du groupe d'équipements TLS Servers. Si le serveur est toujours inactif via le protocole TLS après 96 heures, cela signifie qu'il n'est plus membre du groupe des serveurs TLS et peut ne plus recevoir l' Analyse avancée.

Les appareils de la liste de surveillance sont toujours en Analyse avancée. Un équipement inactif figurant sur la liste de surveillance continue de consommer de l'espace dans votre capacité d'Analyse avancée, même s'il est inactif.

Les appareils qui font partie d'un groupe d'équipements ne consomment pas votre capacité d'Analyse avancée ou d'Analyse standard une fois qu'ils sont devenus inactifs. Lorsque l'équipement redevient actif, il reçoit une Analyse avancée ou une Analyse standard en fonction de la priorité configurée pour cet équipement.