

Alertes FAQ

Publié: 2023-09-19

Voici quelques réponses aux questions fréquemment posées sur les alertes.

- [Où puis-je trouver les alertes générées par le système ExtraHop ?](#)
- [Puis-je ajouter un texte personnalisé aux notifications par courrier électronique ?](#)
- [Comment puis-je savoir quelles alertes sont affectées à une source ?](#)
- [Comment les mesures sont-elles calculées pour les configurations d'alerte affectées à un groupe de dispositifs ?](#)
- [Comment les tendances sont-elles calculées ?](#)

Où puis-je trouver les alertes générées par le système ExtraHop ?

La [page Alertes](#) fournit un accès rapide à toutes les alertes, mais il existe des indicateurs et des liens vers les alertes dans l'ensemble du système ExtraHop.

- Sur un tableau de bord, vous pouvez [ajouter un widget Alertes](#) qui affiche jusqu'à 40 alertes récentes.
- Sur la page Vue d'ensemble d'un appareil, d'un groupe d'appareils ou d'une application, vous pouvez afficher un graphique d'alertes.
- Sur une carte d'activité, la [couleur d'un dispositif](#) correspond à l'état d'alerte le plus grave pour toutes les alertes attribuées au dispositif.
- Sur une carte géographique, la [couleur d'un point de données](#) correspond à l'alerte la plus grave pour toutes les alertes qui suivent la même mesure.

Puis-je ajouter un texte personnalisé aux notifications par courrier électronique ?

Il n'y a pas de champ de texte pour les messages personnalisés dans les notifications par courrier électronique. Toutefois, des informations peuvent être ajoutées au champ **Description** dans les paramètres de l'alerte, et ce texte apparaît dans l'e-mail. Par exemple, le texte pourrait indiquer à votre équipe de prendre des mesures, telles que le redémarrage des appareils, lorsqu'elle reçoit des courriels pour des alertes spécifiques.

En outre, le champ **Description** prend en charge le Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Lorsqu'ils sont placés avant ou autour d'un texte, certains caractères non alphabétiques spécifient le style HTML à appliquer au texte. Par exemple, placez des doubles astérisques (**) avant et après le texte que vous souhaitez afficher en gras. Le tableau suivant présente les formats Markdown courants qui sont pris en charge dans la zone de texte.

Format	Description du format	Exemple de format
Titres	Placez un signe numérique (#) avant votre texte pour formater les titres. Le niveau de l'en-tête est déterminé par le nombre de signes numériques.	####Example H4 heading
Listes non ordonnées	Placez un astérisque (*) devant votre texte.	* First example * Second example
Listes ordonnées	Placez un seul chiffre et un point (1.) avant votre texte.	1. First example 2. Second example
Gras	Placez un double astérisque avant et après votre texte.	**bold text**
Italique	Placez un trait de soulignement avant et après votre texte.	<u>italicized text</u>

Format	Description du format	Exemple de format
Hyperliens	Placez le texte du lien entre parenthèses avant l'URL entre parenthèses. Ou tapez votre URL. Les liens vers des sites Web externes s'ouvrent dans un nouvel onglet du navigateur. Les liens à l'intérieur du système ExtraHop, tels que les tableaux de bord, s'ouvrent dans l'onglet actuel du navigateur.	[Visit our home page](https://www.extrahop.com) https://www.extrahop.com
Guillemets	Placez un crochet à angle droit et un espace avant votre texte.	On the ExtraHop website: > Access the live demo and review case studies.
Police monospace	Placez une coche (`) avant et après votre texte.	`example code block`
Emojis	L'ajout d'emojis dans la syntaxe Markdown n'est pas pris en charge ; cependant, vous pouvez copier et coller une image d'emoji Unicode http://unicode.org/emoji/charts/full-emoji-list.html dans la zone de texte .	

Comment puis-je savoir quelles alertes sont affectées à une source ?

Vous pouvez trouver les affectations d'alertes à partir de la page Présentation d'une source.

- Dans la page Présentation d'un dispositif, cliquez sur **Modifier les affectations**.
- Dans la page Présentation d'un groupe de dispositifs, cliquez sur **Affectations** dans le coin supérieur droit.
- Dans la page Présentation d'une application ou d'un réseau, cliquez sur **Alertes** dans le coin supérieur droit.

Une fenêtre contenant les informations suivantes sur l'affectation des alertes s'affiche :

- Configurations d'alerte directement affectées à la source.
- Configurations d'alerte attribuées par l'intermédiaire d'un groupe de dispositifs.
- Configurations d'alerte affectées globalement à la source.
- État de la configuration d'alerte.

Dans la fenêtre contenant les informations sur les alertes, vous pouvez supprimer une affectation d'alerte de la source en cliquant sur l'icône de suppression (X) située à côté du nom de l'alerte. Si l'alerte a été affectée globalement à toutes les applications ou à tous les dispositifs, vous ne pouvez pas supprimer l'affectation d'une source individuelle.

Comment les mesures sont-elles calculées pour les configurations d'alerte affectées à un groupe de dispositifs ?

Si vous assignez une alerte à un groupe de dispositifs, cela équivaut à assigner l'alerte à chaque dispositif du groupe. Si vous souhaitez agréger les mesures pour tous les membres d'un groupe, vous pouvez créer une application qui consolide les dispositifs en une seule source de mesures, puis assigner l'alerte à cette application.

Comment les tendances sont-elles calculées ?

Le système ExtraHop calcule les tendances en examinant les données historiques et en établissant une base de référence. Les alertes basées sur les tendances sont bien adaptées aux mesures pour lesquelles il est difficile de définir des seuils significatifs, comme les erreurs.

Les alertes basées sur les tendances sont générées lorsqu'une mesure est en dehors de la tendance normale apprise par le système. Dans la plupart des cas, les données historiques sont disponibles et les alertes de tendance sont actives dès qu'elles sont activées. Cependant, si vous configurez une alerte de tendance qui nécessite plus de données historiques que votre appliance n'en possède actuellement, l'appliance calcule la tendance avec les données disponibles.

Pourquoi une alerte n'apparaît-elle pas dans le tableau Alertes ?

Si vous avez ajouté une alerte à partir d'une console, vous devez vous connecter à ce système pour voir et configurer l'alerte.