

Configurer une alerte de tendance

Publié: 2025-02-12

Configurez une alerte de tendance pour surveiller lorsqu'une métrique spécifique s'écarte des tendances normales. Les alertes de tendance sont utiles pour surveiller les tendances métriques, telles que les temps d'aller-retour anormalement élevés ou les serveurs de stockage enregistrant un trafic anormalement faible, ce qui peut indiquer l'échec d'une sauvegarde. Par exemple, vous pouvez configurer une alerte de tendance qui génère des alertes lorsqu'un pic (75e centile) du temps de traitement du serveur Web HTTP dure plus de 10 minutes et lorsque la valeur métrique du temps de traitement est 100 % supérieure à la tendance.

Avant de commencer

Tu dois avoir **privilèges d'écriture complets** ou supérieur.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système  puis cliquez sur **Alertes**.
3. Cliquez **Créez**.
4. Tapez un nom unique pour la configuration de l'alerte dans le **Nom** champ.
5. Dans le **Descriptif** champ, ajoutez des informations sur l'alerte.



Conseils Les descriptions d'alertes sont compatibles avec Markdown, une syntaxe de mise en forme simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le [FAQ sur les alertes](#).

6. Dans le **Type d'alerte** section, cliquez sur **Alerte de tendance**.
7. Dans le **Sources assignées** dans le champ, saisissez le nom d'un équipement, d'un groupe d'équipements ou d'une application, puis sélectionnez-le dans les résultats de recherche.
Pour rechercher un site, un réseau de flux ou une interface de flux, sélectionnez ce type de source dans le menu déroulant situé en haut des résultats de recherche.
8. Optionnel : Cliquez **Ajouter une source** pour attribuer l'alerte à plusieurs sources. Les sources multiples doivent être du même type, par exemple uniquement des appareils et des groupes d'appareils ou uniquement des applications.



Conseil Attribuez une alerte à un groupe d'équipements pour gérer efficacement les attributions à plusieurs appareils.

9. Dans le **Métrique surveillée** champ, saisissez le nom d'une métrique, puis sélectionnez-la dans les résultats de recherche.

La métrique doit être compatible avec les sources attribuées. Par exemple, si vous attribuez l'alerte à une application, vous ne pouvez pas sélectionner une métrique d'équipement métrique.

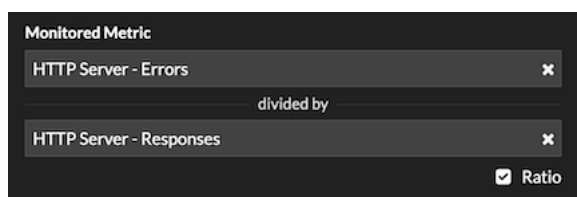
Si vous sélectionnez une métrique d'ensemble de données telle que le temps de traitement du serveur HTTP, vous devez spécifier l'une des méthodes d'agrégation de données suivantes :

Fusionner	Regroupez toutes les valeurs de l'ensemble de données métriques et appliquez le modèle de pondération des tendances à un sur-ensemble de données. Par exemple, un cumul agrégé de 30 secondes, ou cycle métrique, contient un seul jeu de données pour chaque intervalle de 30 secondes. Par conséquent, un intervalle de 30 minutes comporte 60 ensembles de données.
Moyenne	Regroupez la moyenne de chaque ensemble de données métriques.

Percentile	Agrégez le percentile de chaque jeu de données métriques en fonction de la valeur que vous spécifiez pour Percentile .
Écart type absolu	Regroupez le jeu de données métriques avec son écart-type en tant que constante.
Écart type relatif	Agréger l'ensemble de données métriques à son écart type par rapport à la moyenne.

10. Optionnel : Pour contrôler la valeur d'une métrique divisée par une métrique secondaire, cliquez sur **Ratio** puis sélectionnez une métrique secondaire.

Par exemple, divisez les erreurs de réponse HTTP par les réponses HTTP pour suivre l'évolution du pourcentage d'erreurs HTTP.



11. Dans la section Définition de la tendance, indiquez comment la tendance est calculée :

- a) Dans le menu déroulant Modèle de pondération des tendances, sélectionnez un modèle. Le modèle de pondération regroupe les valeurs métriques historiques pour calculer une tendance.

Moyenne	Calculez une tendance en faisant la moyenne de toutes les valeurs métriques, pondérées de manière égale.
Valeur minimale	Calculez une tendance à partir des mesures les plus faibles.
Valeur médiane	Calculez une tendance à partir des valeurs métriques historiques médianes.
Valeur maximale	Calculez une tendance à partir des indicateurs ayant la valeur la plus élevée.
Percentile	Calculez une tendance à partir du centile de chaque métrique en fonction de la valeur que vous spécifiez pour Valeur percentile .
Écart type absolu	Calculez une tendance en comparant l' écart type en tant que valeur constante à la tendance actuelle. À partir du Type de déviation menu déroulant, sélectionnez un type : • Sur la base d'échantillons • Basé sur la population
Écart type relatif	Calculez une tendance en comparant l' écart type en tant que valeur relative à la moyenne de la tendance actuelle. À partir du Type de déviation menu déroulant, sélectionnez un type :

	• Sur la base d'échantillons • Basé sur la population
Régression linéaire	Calculez une tendance linéaire sur la base des valeurs métriques précédentes.
Régression polynomiale du 2e degré	Calculez une tendance quadratique en projetant une courbe à l'aide de l'équation suivante : $y=ax^2+bx+c$
Moyenne exponentielle unique	Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids. Dans le Calcul de la valeur et du poids récents champ, spécifiez un grand nombre pour donner plus de poids aux valeurs métriques les plus récentes ou spécifiez un petit nombre pour donner plus de poids aux valeurs métriques les plus anciennes.
Moyenne exponentielle double	Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids. Dans le Calcul de la valeur et du poids récents champ, spécifiez un grand nombre pour donner plus de poids aux valeurs métriques les plus récentes ou spécifiez un petit nombre pour donner plus de poids aux valeurs métriques les plus anciennes. Notez que les calculs de moyenne exponentielle double sont plus précis pour prédire la trajectoire de la tendance.
Valeur statique	Calculez une tendance sur la base d'une valeur métrique statique par rapport à un calcul métrique. Spécifiez une valeur statique et sélectionnez un calcul métrique : • Tarif par heure • Tarif par minute • Compter Ce modèle est utile pour tracer des lignes constantes pour les SLA.
Trimesan	Calculez une tendance sur la base de la moyenne pondérée des valeurs métriques des 25e, 50e et 75e centiles.
Delta horaire	Calculez une tendance en comparant les valeurs métriques actuelles aux données historiques.
Moyenne winsorisée	Calculez une tendance en récupérant les valeurs métriques à des pourcentages bas et élevés spécifiés et en les remplaçant par les valeurs restantes les plus basses et les plus élevées.

Par exemple, les valeurs métriques supérieures au 90e percentile deviennent la même valeur que le 90e, et les valeurs métriques inférieures au 10e percentile deviennent la même valeur que le 10e.

À partir du **Winsorisation** menu déroulant, sélectionnez une paire de pourcentages :

- 5/95e percentile
- 10/90e percentile
- 25/75e percentile

b) À partir du **Fenêtre de tendance** menu déroulant, sélectionnez une fenêtre de calcul.

Même heure de la semaine	Calculez une tendance en comparant les mesures recueillies sur la même fenêtre d'une heure chaque semaine.
Même heure de la journée	Calculez une tendance en comparant les mesures recueillies chaque jour dans la même fenêtre d'une heure.
Moyenne mobile par minute	Calculez une tendance en faisant la moyenne des valeurs métriques collectées chaque minute dans un laps de temps spécifié à partir de l'heure actuelle.
Moyenne mobile horaire	Calculez une tendance en faisant la moyenne des valeurs métriques collectées chaque heure dans un laps de temps spécifié à partir de l'heure actuelle.

c) Dans le **Aperçu des tendances** champ, spécifiez la fenêtre temporelle des données historiques que le système ExtraHop examinera pour calculer la tendance. Les valeurs rétrospectives valides sont déterminées par la fenêtre de tendance sélectionnée.

- Spécifiez une valeur comprise entre 1 et 45 jours si l'option Même heure du jour est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 15 semaines si l'option Même heure de la semaine est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 48 heures si la moyenne mobile horaire est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 999 minutes si la moyenne mobile par minute est sélectionnée.

12. Dans la section Condition d'alerte, spécifiez les conditions de génération d'une alerte.

Metric Calculation

Time Interval

Standard Deviation ▾ during the last 60m ▾

is = 125 percent of trend ▾

Operator

Metric Value

Measurement

- a) À partir du **Tout faire correspondre** menu déroulant, sélectionnez une option pour générer une alerte lorsque toutes les conditions d'alerte, ou aucune d'entre elles, sont remplies.
- b) Sélectionnez un calcul métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps.

Moyenne	Calculez la valeur moyenne de la métrique.
Médiane	Calculez la valeur du 50e percentile de la métrique .
25e percentile	Calculez la valeur du 25e percentile de la métrique .
75e percentile	Calculez la valeur du 75e percentile de la métrique.
Écart type	Calculez l'écart type par rapport à la métrique. L'écart type est l'ampleur de la variation par rapport à la tendance.
Compter	Spécifiez le total absolu de la métrique. Aucune mesure n'est requise.

- c) Sélectionnez l'intervalle de temps pendant lequel la valeur métrique est observée. Vous pouvez sélectionner un intervalle compris entre 30 secondes et 30 minutes.
- d) Sélectionnez un opérateur pour spécifier comment le calcul métrique est comparé à la valeur métrique.
- e) Spécifiez la valeur métrique à comparer au calcul métrique.
- f) Spécifiez comment mesurer la valeur métrique.
 - Pourcentage de tendance
 - Absolu
 - Par seconde
 - Par minute
- g) Optionnel : Cliquez **Ajouter une condition** pour ajouter d'autres critères de condition ou cliquez sur **Ajouter un groupe de conditions** aux critères de condition du nid.

Par exemple, pour générer une alerte lorsque l'écart type de la métrique observée sur un intervalle de 60 minutes est égal à une valeur de tendance de 25 %, spécifiez les conditions suivantes :

- Calcul métrique : écart type
 - Intervalle de temps : 60 m
 - Opérateur : =
 - Valeur métrique : 125
 - Mesure : pourcentage de la tendance
13. Optionnel : Dans la section Notifications, **ajouter une notification par e-mail à une alerte**  pour recevoir des e-mails ou des interruptions SNMP lorsqu'une alerte est générée.
 14. Dans la section État, cliquez sur une option pour activer ou désactiver l'alerte.
 15. Optionnel : **Ajouter un intervalle d'exclusion**  pour supprimer les alertes à des moments précis.
 16. Cliquez **Enregistrer**.