


Configuration d'une alerte de tendance

Publié: 2024-08-08

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 dont le trafic est anormalement faible, ce qui peut indiquer un échec de 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 des paramètres système  puis cliquez sur **Alertes**.
3. Cliquez **Créez**.
4. Entrez un nom unique pour la configuration de l'alerte dans **Nom** champ.
5. Dans le **Descriptif** champ, ajoutez des informations sur l'alerte.



Conseils Les descriptions des alertes prennent en charge le Markdown, une syntaxe de formatage 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 **Alerte de tendance**.
7. Dans le **Sources assignées** dans ce 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 en haut des résultats de recherche.
8. Optionnel : Cliquez **Ajouter une source** pour attribuer l'alerte à plusieurs sources. Plusieurs sources doivent être du même type, par exemple uniquement des appareils et des groupes d'équipements ou uniquement des applications.



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

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

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

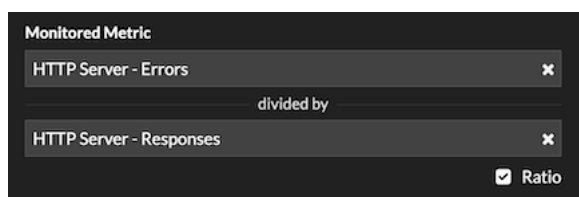
Si vous sélectionnez une métrique de jeu de données telle que le temps de traitement du serveur HTTP, vous devez spécifier l'une des méthodes d'agrégation de données suivantes :

Fusionner	Agrégez toutes les valeurs du jeu 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.
Méchant	Agrégez la moyenne de chaque jeu 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	Agrégez le jeu de données métriques à son écart type sous forme de constante.
Écart type relatif	Agrégez le jeu de données métriques à son écart type par rapport à la moyenne.

10. Optionnel : Pour surveiller 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, spécifiez le mode de calcul de la tendance :

- a) Dans la liste déroulante Modèle de pondération des tendances, sélectionnez un modèle. Le modèle de pondération agrège les valeurs métriques historiques pour calculer une tendance.

Méchant	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 de valeur les plus élevés.
Percentile	Calculez une tendance à partir du percentile 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 sous forme de valeur constante à la tendance actuelle. À partir du Type de déviation liste déroulante, sélectionnez un type : <ul style="list-style-type: none"> • Basé sur des échantillons • Basé sur la population
Écart type relatif	Calculez une tendance en comparant l' écart type sous forme de valeur par rapport à la moyenne de la tendance actuelle. À partir du Type de déviation liste déroulante, sélectionnez un type :

	<ul style="list-style-type: none"> • Basé sur des échantillons • Basé sur la population
Régression linéaire	Calculez une tendance linéaire en fonction des valeurs métriques précédentes.
Régression polynomiale du 2e degré	Calculez une tendance quadratique en projetant une courbe avec l'équation suivante : $y=ax^2+bx+c$
Moyenne exponentielle unique	<p>Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids .</p> <p>Dans le Calcul récent de la valeur et du poids 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.</p>
Moyenne exponentielle double	<p>Calcule une tendance en faisant la moyenne des valeurs métriques basées sur le poids .</p> <p>Dans le Calcul récent de la valeur et du poids 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.</p> <p>Notez que les calculs de moyenne exponentielle doubles sont plus précis pour prédire la trajectoire de la tendance.</p>
Valeur statique	<p>Calculez une tendance en fonction d'une valeur métrique statique par rapport à un calcul métrique.</p> <p>Spécifiez une valeur statique et sélectionnez un calcul métrique :</p> <ul style="list-style-type: none"> • Tarif par heure • Tarif par minute • Compter <p>Ce modèle est utile pour tracer des lignes constantes pour les SLA.</p>
Trimean	Calculez une tendance en fonction de la moyenne pondérée des valeurs métriques des 25e, 50e et 75e percentiles.
Delta temporel	Calculez une tendance en comparant les valeurs métriques actuelles aux données historiques.
Moyen Winsorisé	Calculez une tendance en récupérant les valeurs métriques aux pourcentages bas et élevés spécifiés et en les remplaçant par les valeurs restantes les plus faibles et les plus élevées.

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

À partir du **Winsorisation** liste déroulante, sélectionnez une paire de pourcentages :

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

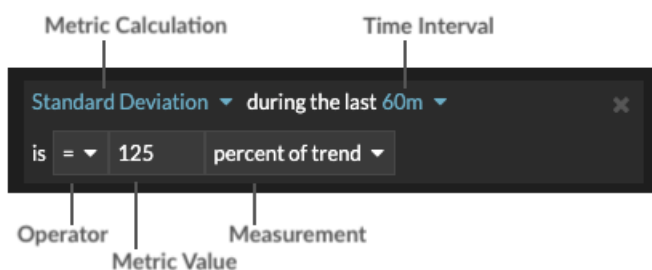
b) À partir du **Fenêtre de tendance** liste déroulante, sélectionnez une fenêtre de calcul.

Même heure de la semaine	Calculez une tendance en comparant les statistiques recueillies au cours de la même fenêtre d'une heure chaque semaine.
Même heure du jour	Calculez une tendance en comparant les indicateurs collectés chaque jour sur la même fenêtre d'une heure.
Moyenne mobile par minute	Calculez une tendance en faisant la moyenne des valeurs métriques recueillies chaque minute dans un laps de temps spécifié à partir de l'heure actuelle.
Moyenne mobile par heure	Calculez une tendance en faisant la moyenne des valeurs métriques recueillies chaque heure dans un laps de temps spécifié à partir de l'heure actuelle.

c) Dans le **Rétrospective 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 la même heure du jour est sélectionnée.
- Spécifiez une valeur comprise entre 1 et 15 semaines si la 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.





a) À partir du **Tout faire correspondre** liste déroulante, sélectionnez une option pour générer une alerte lorsque toutes les conditions d'alerte, certaines ou aucune d'entre elles sont remplies.

- b) Sélectionnez un calcul métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps.

Méchant	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 de la métrique est comparé à la valeur de la métrique.
- e) Spécifiez la valeur métrique à comparer au calcul de la métrique.
- f) Spécifiez le mode de mesure de 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 d' état 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 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**.