Configurer une alerte de tendance

Publié: 2023-09-19

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

Avant de commencer
Vous devez disposer des droits d'écriture complets ou d'un niveau supérieur.

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

   Conseil Les descriptions d'alerte prennent en charge Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le site Alertes FAQ.
6. Dans la section **Type d'alerte**, cliquez sur **Alerte de tendance**.
7. Dans le champ **Sources attribuées**, saisissez le nom d'un dispositif, d'un groupe de dispositifs ou d'une application, puis sélectionnez-le dans les résultats de la 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 la recherche.
8. Optionnel : Cliquez sur **Ajouter une source** pour affecter l'alerte à plusieurs sources. Les sources multiples doivent être du même type, par exemple uniquement des dispositifs et des groupes de dispositifs ou uniquement des applications.

   Conseil Affectez une alerte à un groupe de dispositifs pour gérer efficacement les affectations à plusieurs dispositifs.
9. Dans le champ **Métrique surveillée**, tapez le nom d'une métrique, puis sélectionnez-la dans les résultats de la recherche.

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

   . 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	Agréger toutes les valeurs des ensembles de données métriques et appliquer le modèle de pondération des tendances à un surensemble de données .Par exemple, un rollup agrégé de 30 secondes, ou cycle métrique, contient un seul ensemble de données pour chaque intervalle de 30 secondes. Par conséquent, un intervalle de 30 minutes comporte 60 ensembles de données .

Moyenne	Agrégation de la moyenne de chaque ensemble de données métriques.
Percentile	Agréger le percentile de chaque jeu de données métriques en fonction de la valeur spécifiée pour **Percentile**.
Écart-type absolu	Agréger l'ensemble de données métriques à 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 surveiller la valeur d'une mesure divisée par une mesure secondaire, cliquez sur **Ratio**, puis sélectionnez une mesure secondaire.

    Par exemple, divisez les erreurs de réponse HTTP par les réponses HTTP pour surveiller les tendances du pourcentage d'erreurs HTTP.

11. Dans la section Définition de la tendance, indiquez comment la tendance est calculée :
    a) Dans la liste déroulante Modèle de pondération des tendances, sélectionnez un modèle. Le modèle de pondération agrège les valeurs historiques des métriques pour calculer une tendance.

Moyenne	Calculer une tendance en faisant la moyenne de toutes les valeurs métriques, pondérées de manière égale.
Valeur minimale	Calcule une tendance à partir des valeurs les plus faibles.
Valeur médiane	Calculer une tendance à partir de la médiane des valeurs métriques historiques.
Valeur maximale	Calculer une tendance à partir des valeurs les plus élevées.
Percentile	Calcule une tendance à partir du percentile de chaque mesure en fonction de la valeur spécifiée pour la **valeur du percentile**.
Écart-type absolu	Calcule une tendance en comparant l'écart type en tant que valeur constante à la tendance actuelle . Dans la liste déroulante **Type d'écart**, sélectionnez un type : • Basé sur l'échantillon • Basé sur la population
Écart type relatif	Calculer une tendance en comparant l'écart **type**

	en tant que valeur relative à la moyenne de la tendance actuelle : • Basé sur l'échantillon • Basé sur la population
Régression linéaire	Calcule une tendance linéaire basée sur les valeurs métriques précédentes.
Régression polynomiale du 2e degré	Calculer une tendance quadratique en projetant une courbe avec l'équation suivante : `y=ax^2+bx+c`
Moyenne exponentielle simple	Dans le champ **Calcul de la pondération des valeurs récentes**, 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	Dans le champ **Calcul du poids des valeurs récentes**, 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	Calculer une tendance sur la base d'une valeur métrique statique comparée à un calcul métrique .spécifier une valeur statique et sélectionner un calcul métrique : • Taux par heure • Taux par minute • Comptage Ce modèle est utile pour tracer des lignes constantes pour les accords de niveau de service.
Trimean	Calcule une tendance basée sur la moyenne pondérée des valeurs métriques des 25e, 50e et 75e percentiles.
Temps Delta	Calcule une tendance en comparant les valeurs métriques actuelles aux données historiques.

Moyenne winsorisée	Calcule une tendance en récupérant les valeurs métriques à des pourcentages faibles 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 la même valeur que le 90e, et les valeurs métriques inférieures au 10e percentile deviennent la même valeur que le 10e. Dans la liste déroulante **Winsorization**, sélectionnez une paire de pourcentages : • 5/95e centile • 10/90e centile • 25/75e centile

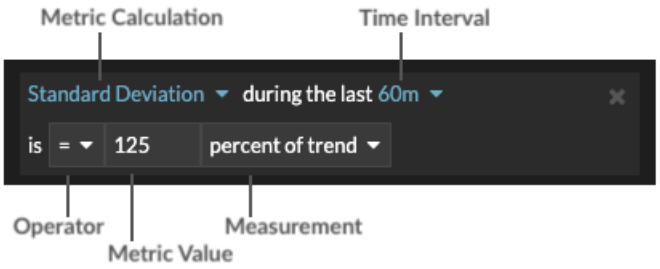
b) Dans la liste déroulante **Trend Window**, sélectionnez une fenêtre de calcul.

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

c) Dans le champ **Trend Lookback**, indiquez la fenêtre temporelle des données historiques que le système ExtraHop examinera pour calculer la tendance. Les valeurs de rétrospection valides sont déterminées par la fenêtre de tendance sélectionnée.

- Indiquez 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 l'option Hour Rolling Average est sélectionnée.
- Indiquez une valeur comprise entre 1 et 999 minutes si l'option Moyenne mobile en minutes est sélectionnée.

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



a) Dans la liste déroulante **Match All**, sélectionnez une option pour générer une alerte lorsque toutes, n'importe quelle ou aucune des conditions d'alerte sont remplies.
b) Sélectionnez un calcul métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps.

Moyenne	Calcule la valeur moyenne de la mesure.
Médiane	Calcule la valeur du 50e percentile de la mesure.
25e percentile	Calcule la valeur du 25e percentile de la métrique.
75e percentile	Calculer la valeur du 75ème percentile de la métrique.
Écart-type	Calculer l'écart-type par rapport à la mesure. L'écart-type est la variation par rapport à la tendance.
Nombre	Indique le total absolu de la mesure. Aucune mesure n'est requise.

c) Sélectionnez l'intervalle de temps pendant lequel la valeur métrique est observée. Vous pouvez sélectionner un intervalle de 30 secondes à 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 métrique.
f) Spécifiez comment mesurer la valeur métrique.

- Pourcentage de la tendance
- Absolu
- Par seconde
- Par minute

g) Optionnel : Cliquez sur **Ajouter une condition** pour ajouter d'autres critères de condition ou cliquez sur **Ajouter un groupe de conditions** pour imbriquer des critères de condition.

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

- Calcul de la métrique : Écart type
- Intervalle de temps : 60m
- Opérateur : =
- Valeur de la métrique : 125
- Mesure : pourcentage de la tendance

13. Optionnel : Dans la section Notifications, ajoutez une notification par courriel à une alerte pour recevoir des courriels ou des traps SNMP lorsqu'une alerte est générée.
14. Dans la section État, cliquez sur une option pour activer ou désactiver l'alerte.

15. Optionnel : Ajoutez un intervalle d'exclusion pour supprimer les alertes pendant des périodes spécifiques.
16. Cliquez sur **Enregistrer**.