Configuration d'un seuil d'alerte

Publié: 2023-09-19

Configurez un seuil d'alerte pour surveiller le franchissement d'une limite définie par une mesure spécifique. Par exemple, vous pouvez générer une alerte lorsqu'un code d'état HTTP 500 est observé plus de 100 fois au cours d'une période de dix minutes.

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 System Settings (Paramètres système), puis sur **Alerts (Alertes)**.
3. Cliquez sur **Créer**.
4. Saisissez un nom unique pour la configuration de l'alerte dans le champ **Nom**.
5. Dans le champ **Description**, ajoutez des informations sur l'alerte.

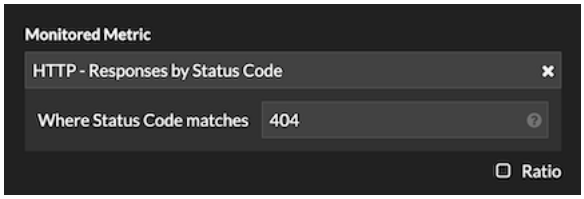
   Conseil: Les descriptions d'alertes prennent en charge Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le site Alertes FAQ.
6. Dans la section **Type d'alerte**, cliquez sur **Alerte de seuil**.
7. Dans le champ **Sources attribuées**, tapez 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 périphériques pour gérer efficacement les affectations à plusieurs périphériques.
9. Dans le champ **Mesure surveillée**, tapez le nom d'une mesure, puis sélectionnez-la dans les résultats de la recherche.

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

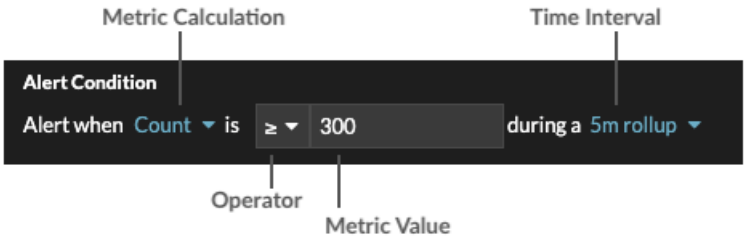
   Note: .Si vous sélectionnez une métrique de détail, vous pouvez spécifier une valeur clé. Par exemple, vous pouvez sélectionner HTTP - Réponses par code d'état, puis spécifier 404 comme valeur clé. Une alerte est générée uniquement lorsque des réponses HTTP avec des codes d'état 404 se produisent.



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

    Par exemple, vous pouvez surveiller le pourcentage d'erreurs HTTP survenant dans les réponses en divisant les erreurs de réponse HTTP par les réponses HTTP.

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



a) Sélectionnez un calcul de métrique pour spécifier comment calculer la valeur de la métrique dans l'intervalle de temps. Les options disponibles dépendent du type de données.

Compter	• Compte • Taux par seconde • Taux par minute • Taux par heure
Ensemble de données	• Minimum • 25ème percentile • Médiane • 75ème percentile • Maximum
Ensemble d'échantillons	• Moyenne • +1 à +7 écarts types • -1 à -7 écarts types
Maximum, instantané	Pas de mesure ; l'opérateur compare la valeur métrique réelle.

b) Sélectionnez un opérateur pour spécifier comment comparer le calcul métrique à la valeur métrique.
c) Spécifiez la valeur métrique à comparer au calcul métrique.
d) Sélectionnez l'intervalle de temps pendant lequel la valeur métrique est observée et les données métriques sont agrégées. Vous pouvez sélectionner un intervalle de temps de 30 secondes à 30 minutes.

Par exemple, pour générer une alerte lorsque plus de 300 erreurs de réponse HTTP se produisent en l'espace de 5 minutes, spécifiez les conditions suivantes :

- Calcul de la métrique : Compter
- Opérateur : >
- Valeur de la métrique : 300
- Intervalle de temps : 5m rollup

12. 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.
13. Dans la section État, cliquez sur une option pour activer ou désactiver l'alerte.
14. Optionnel : Ajoutez un intervalle d'exclusion pour supprimer les alertes pendant des périodes spécifiques.
15. Cliquez sur **Enregistrer**.