Configuration d'une alerte de seuil

Publié: 2024-08-07

Configurez une alerte de seuil pour surveiller le moment où une métrique spécifique franchit une limite définie. 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
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.

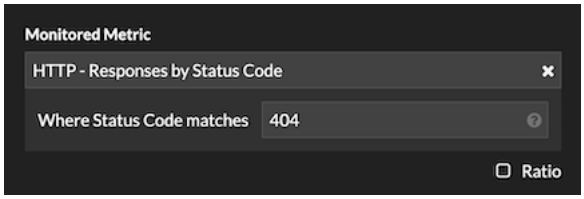
   Conseil: Les descriptions des alertes prennent en charge le Markdown, une syntaxe de formatage simple qui convertit le texte brut en HTML. Pour plus d'informations, consultez le FAQ sur les alertes.
6. Dans le **Type d'alerte** section, cliquez **Alerte de seuil**.
7. Dans le **Sources assignées** dans 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 déquipements 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.

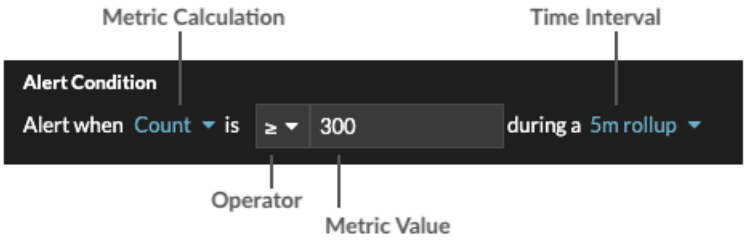
   Note: Si vous sélectionnez un métrique de détail, vous pouvez spécifier une valeur clé. Par exemple, vous pouvez sélectionner HTTP - Réponses par code d'état, puis spécifier 404 comme valeur clé. Une alerte est générée uniquement lorsque des réponses HTTP contenant des codes d'état 404 se produisent.

10. Optionnel : Pour surveiller la valeur d'une métrique divisée par une métrique secondaire, cliquez sur **Ratio** puis sélectionnez une métrique 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 métrique pour spécifier comment calculer la valeur métrique dans l'intervalle de temps. Les options disponibles dépendent du type de données.

Compter	• Compter • Débit par seconde • Tarif par minute • Tarif par heure
Ensemble de données	• Minimum • 25e percentile • Médiane • 75e percentile • Maximum
Set d'échantillons	• Méchant • +1 à +7 écarts types • -1 à -7 écarts types
Maximum, instantané	Aucune mesure ; l'opérateur compare la valeur métrique réelle.

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

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

- Calcul métrique : nombre
- Opérateur : >
- Valeur métrique : 300
- Intervalle de temps : cumul de 5 m

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