Suivez les erreurs du serveur à l'aide de métriques et d'alertes personnalisées

Publié: 2023-09-14

Bien que le système ExtraHop propose plus de 5 000 métriques intégrées, il existe de nombreuses situations dans lesquelles il est plus efficace de suivre les problèmes de réseau à l'aide d'une métrique personnalisée. Par exemple, alors que les métriques intégrées indiquent les problèmes liés aux réponses et aux demandes HTTP, une métrique personnalisée peut identifier les erreurs de serveur de niveau 500. Ces types d'erreurs peuvent indiquer des problèmes de passerelle, un serveur surchargé ou des problèmes de configuration.

Dans cette procédure pas à pas, vous allez apprendre à écrire un déclencheur pour collecter des métriques personnalisées relatives aux erreurs de serveur et à créer une alerte qui envoie une notification par e-mail uniquement lorsque ces erreurs spécifiques se produisent. Vous pourrez ensuite répondre aux types de questions suivants concernant les erreurs de serveur sur votre réseau :

- Mes clients reçoivent-ils des erreurs de serveur de niveau 500 ?
- Quels sont les codes d'erreur survenus ?
- Quand les erreurs se sont-elles produites ?
- À quelle URI le client tentait-il d'accéder ?
- Quelle est l'adresse IP du client et du serveur concernés par la transaction ?

Prérequis

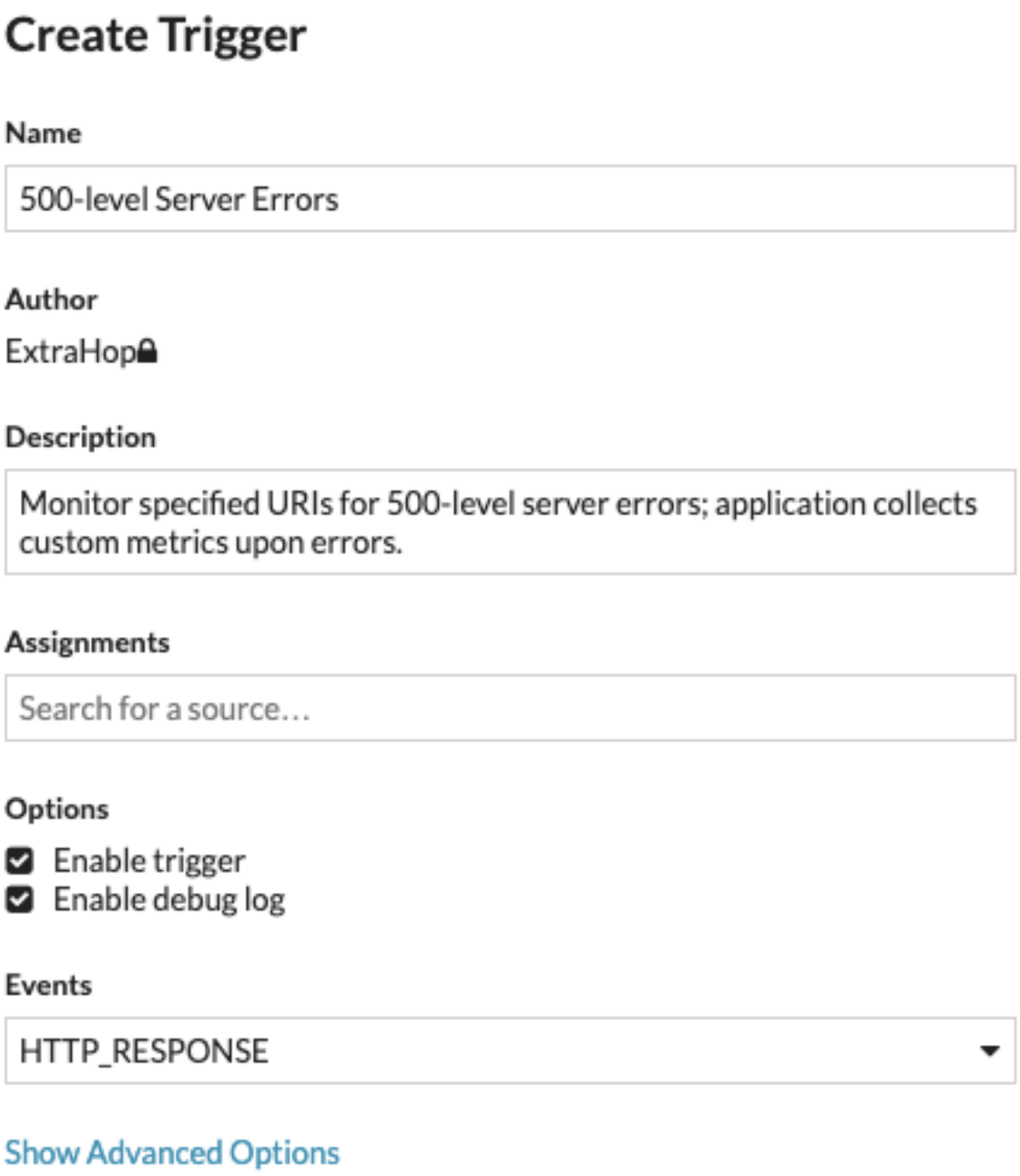
- Vous devez disposer d'un compte utilisateur doté de privilèges d'administration du système et d'accès.
- Votre système ExtraHop doit disposer de données réseau avec le trafic du serveur Web.
- Votre système ExtraHop doit être configuré pour envoyer des notifications par e-mail avant de pouvoir envoyer des e-mails d'alerte.
- Familiarisez-vous avec les concepts présentés dans cette procédure pas à pas en lisant déclencheurs et Alertes.
- Familiarisez-vous avec les processus de création de déclencheurs en lisant Créez un déclencheur.
- Il est utile d'avoir des connaissances de base en JavaScript.

Écrire un déclencheur pour collecter les données d'erreur

Créons d'abord un déclencheur qui surveille certains URI pour détecter les erreurs de serveur de niveau 500. Lorsque des erreurs se produisent, le déclencheur collecte des données telles que les codes d'erreur et les adresses IP du serveur et du client et les transmet sous forme de mesures personnalisées à une application.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur les paramètres système icône, puis cliquez sur **DÉCLENCHEURS**.
3. Cliquez **Créez**.
4. Dans le **Nom** champ, saisissez le nom du déclencheur. Pour cette procédure pas à pas, tapez `Erreurs de serveur de niveau 500`.
5. Dans le **Description** champ, saisissez les informations relatives au déclencheur. Pour cette procédure pas à pas, tapez `Surveillez les URI spécifiées pour détecter les erreurs de serveur de niveau 500 ; l'application collecte des métriques personnalisées en cas d'erreur .`
6. Cliquez **Activer le journal de débogage**.
7. Cliquez dans le **Évènements** champ et sélectionnez **HTTP_RESPONSE** depuis la liste.

La figure suivante montre les paramètres du déclencheur que nous avons configurés ci-dessus :



8. Cliquez sur le **Rédacteur** onglet.
9. Dans l'éditeur Trigger Script, copiez et collez le code suivant :

```
// VARIABLES TO EDIT //

// Edit this array with hosts and URIs to monitor
var CHECK_URI_LIST = [
'www.example.com',
'example.com/about/main_page',
```

```
'http://www.example.com/about/main_page',
];

// Edit this array with client IP addresses to ignore
var IGNORE_CLIENT_IP = [
'180.57.175.147',
'172.16.156.130'
];

// END VARIABLES TO EDIT //

// DO NOT EDIT REMAINDER OF SCRIPT //

// If client IP is in array above, end process
if (IGNORE_CLIENT_IP.indexOf(Flow.client.ipaddr.toString()) > -1){
//debug ('Ignoring client IP: ' + Flow.client.ipaddr);
return}

// If URI is empty, end process
var uri = HTTP.uri || HTTP.host;
if (uri === null){//debug ('No URI Found, ending');
return}

// If URI/hostname does not match array above, end process
var matches = CHECK_URI_LIST.filter(condition => uri.indexOf(condition) >
 -1);
if (matches.length === 0) {
//debug ('URI or host did not match: ' + uri);
return}

var app = "HTTP Server Errors",
code = HTTP.statusCode,
client = Flow.client.ipaddr.toString(),
server = Flow.server.ipaddr.toString(),
detail = 'Code: ' + code + ' || Server: ' + server + ' || Client: ' +
 client + ' || URI: '
          + uri;

if (code < 500 || code > 600) {return}

var code = HTTP.statusCode.toString();

// If URI matches and is a 5xx error, commit custom metrics
// to the application, which is created upon the initial event
Application(app).metricAddCount('HTTP_error', 1);
Application(app).metricAddDetailCount('HTTP_error_uri', uri, 1);
Application(app).metricAddDetailCount('HTTP_error_serverIP', server, 1);
Application(app).metricAddDetailCount('HTTP_error_clientIP', client, 1);
Application(app).metricAddDetailCount('HTTP_error_allDetail', detail, 1);
debug ('Detail: ' + detail);
```

10. Dans le `CHECK_URI_LIST` tableau de variables, remplacez example.com par les hôtes, les URI et les combinaisons hôte-URI que vous souhaitez que le déclencheur surveille.
11. Dans le `IGNORE_CLIENT_IP` tableau variable, remplacez les adresses IP d'exemple (180.57.175.147 et 172.16.156.130) par les adresses IP que vous souhaitez que le déclencheur ignore.

    Supprimez ou commentez ce tableau s'il n'y a aucune adresse IP à ignorer.
12. Cliquez **Enregistrer et fermer**.
    L'éditeur de déclencheurs valide la syntaxe de votre script. Les actions non valides, les erreurs de syntaxe ou les éléments obsolètes vous empêcheront d'enregistrer le déclencheur tant que vous n'avez pas corrigé le code ou désactivé la validation de la syntaxe.

Une fois le déclencheur attribué et exécuté, il crée les composants suivants auxquels nous ferons référence lors de la configuration des paramètres d'alerte dans les sections suivantes :

Erreurs du serveur HTTP

Le déclencheur valide les données collectées à partir des métriques personnalisées vers cette application.

Erreur_HTTP

Une métrique de comptage personnalisée qui collecte le nombre d'erreurs de niveau 500 qui se produisent.

HTTP_Error_AllDetail

Une coutume métrique détaillée qui collecte le numéro de code, l'URI, l'adresse IP du serveur et l'adresse IP du client sur lesquels chaque erreur s'est produite.

Attribuer le déclencheur à un équipement

Avant que le déclencheur puisse s'exécuter, il doit être attribué à au moins un équipement. Au cours de cette étape, nous allons attribuer le déclencheur à un ou plusieurs serveurs HTTP qui prennent en charge le trafic via les URI que vous avez spécifiés dans le déclencheur.

1. Cliquez **Actifs**depuis le menu supérieur.
2. Dans Appareils par activité de protocole, cliquez sur **Serveurs HTTP**, puis cliquez sur **Appareils** depuis le volet de gauche.
3. Dans la liste des équipements, cochez la case à côté d'un ou de plusieurs appareils prenant en charge le trafic via les URI.
4. En haut de la page, cliquez sur **Assigner un déclencheur** pour ouvrir une liste de déclencheurs.
5. Sélectionnez le déclencheur nommé **Erreurs de serveur de niveau 500** que nous avons créé dans la section précédente, puis cliquez sur **Assigner des déclencheurs**.

Prochaines étapes

Conseil Attribuez des déclencheurs uniquement aux appareils concernés afin d'éviter tout impact inutile sur les performances du système. Un bon moyen de s'assurer qu'un déclencheur ne s'exécute que sur les appareils concernés est de créer un groupe déquipements et assignez le déclencheur à ce groupe.

Configurer une alerte pour suivre une métrique personnalisée

Configurons ensuite les paramètres d'alerte qui émettront une alerte et enverront une notification par e-mail chaque fois qu'une erreur de niveau 500 se produit sur les URI surveillés par le déclencheur .

Dans les paramètres d'alerte, nous allons faire référence aux métriques personnalisées suivantes que nous avons créées dans le script du déclencheur :

Erreur_HTTP

Mesure de comptage personnalisée qui collecte le nombre d'erreurs de niveau 500 qui se produisent. Nous allons configurer les paramètres d'alerte pour suivre cette métrique et émettre une alerte chaque fois qu'une erreur se produit.

HTTP_Error_AllDetail

La coutume métrique détaillée qui collecte le numéro de code, l'URI, l'adresse IP du serveur et l'adresse IP du client sur lesquels chaque erreur s'est produite. Nous allons configurer les paramètres d'alerte pour afficher ces informations d'erreur dans les e-mails d'alerte.

Avant de commencer

Votre système ExtraHop doit être configuré pour les notifications par e-mail.

1. Cliquez sur les paramètres système icône, puis cliquez sur **Alertes**.
2. Cliquez **Créez** puis tapez le nom de l'alerte dans le **Nom** champ. Pour cette procédure pas à pas, tapez `Erreurs de serveur de niveau 500`.
3. Entrez une description de l'alerte dans le **Descriptif** champ. Pour cette procédure pas à pas, tapez `Alerte émise lorsqu'une erreur de serveur de niveau 500 se produit sur les URI surveillés.`
4. Dans le Type d'alerte section, sélectionnez **Alerte de seuil** pour émettre une alerte lorsque l'événement métrique suivi se produit.
5. Dans le **Métrique surveillée** champ, type `Erreur_HTTP` puis sélectionnez **Personnalisé - HTTP_Error** à partir des résultats de recherche.
6. Dans le Comportement des alertes section, sélectionnez **Alerte une fois lorsque la condition d'alerte est remplie** pour générer une alerte pour chaque occurrence de la métrique suivie.
7. Dans le État d'alerte section, spécifiez la condition suivante pour générer une alerte si l'événement métrique suivi se produit plusieurs fois par période de 30 secondes : `Alert when value > 1 during a 30s rollup`
8. Dans le Notifications section, saisissez une adresse e-mail qui doit recevoir des notifications d'alerte.

   Conseil La liste déroulante des groupes de notifications par e-mail affiche tous groupes de messagerie configurés dans les paramètres d'administration. Vous pouvez sélectionner un ou plusieurs groupes devant recevoir des notifications d'alerte.
9. Cliquez **Afficher les options avancées** puis cliquez sur **Ajouter une métrique**.
10. Dans le champ de recherche, tapez `HTTP_Error_AllDetail`, puis sélectionnez **Personnalisé - Http_Error_AllDetail** à partir des résultats de recherche.
11. Cliquez **Enregistrer**.

Attribuer la configuration d'alerte à une source

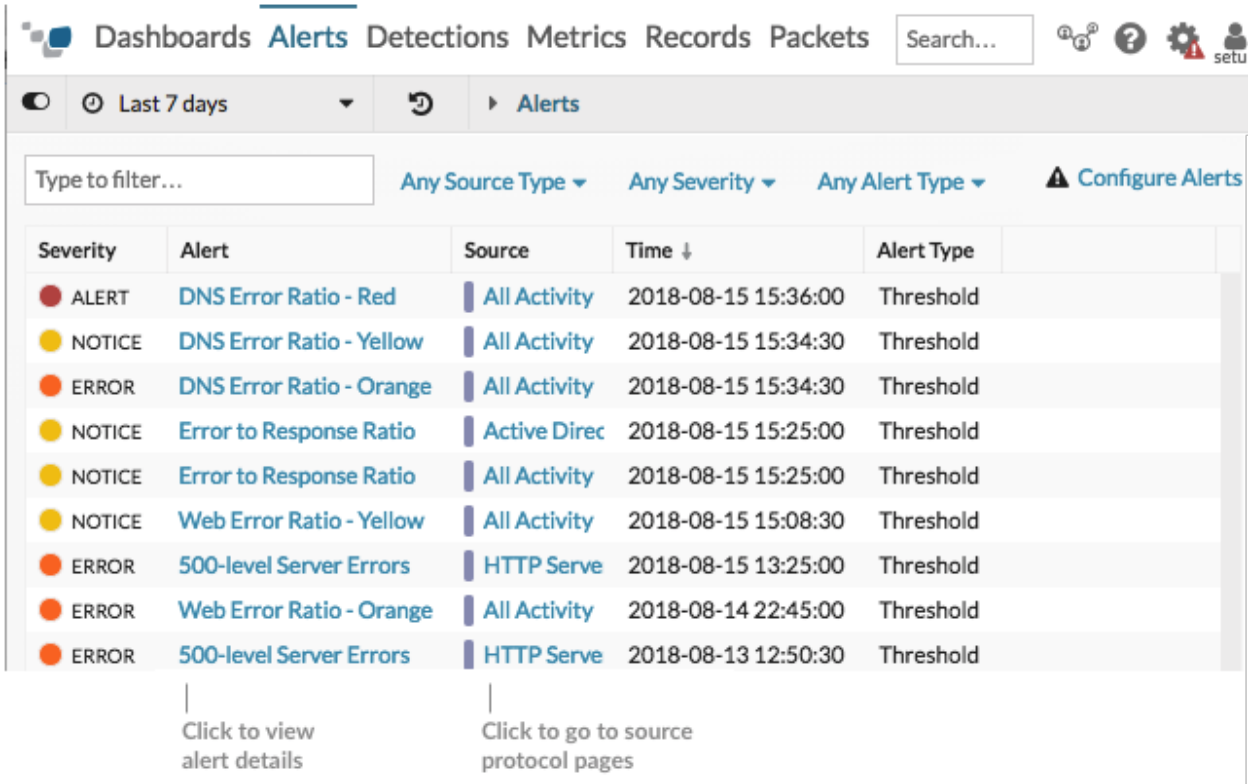
Comme pour les déclencheurs, le système ne génère pas d'alertes tant que la configuration des alertes n'est pas affectée à au moins une métrique source. Au cours de cette étape, nous allons attribuer la configuration d'alerte à l'application nommée HTTP Server Errors que nous avons créée avec le script déclencheur. Les métriques personnalisées que nous voulons suivre par l'alerte sont enregistrées dans cette application.

1. Cliquez **Actifs** depuis le menu supérieur.
2. Cliquez **Demandes**, puis sélectionnez **Erreurs du serveur HTTP** case à cocher.
3. Cliquez **Attribuer une alerte** en haut de la page pour ouvrir une liste des configurations d'alerte éligibles à l'attribution.
4. Sélectionnez le **Erreurs de serveur de niveau 500** alerte, puis cliquez sur **Attribuer des alertes**.

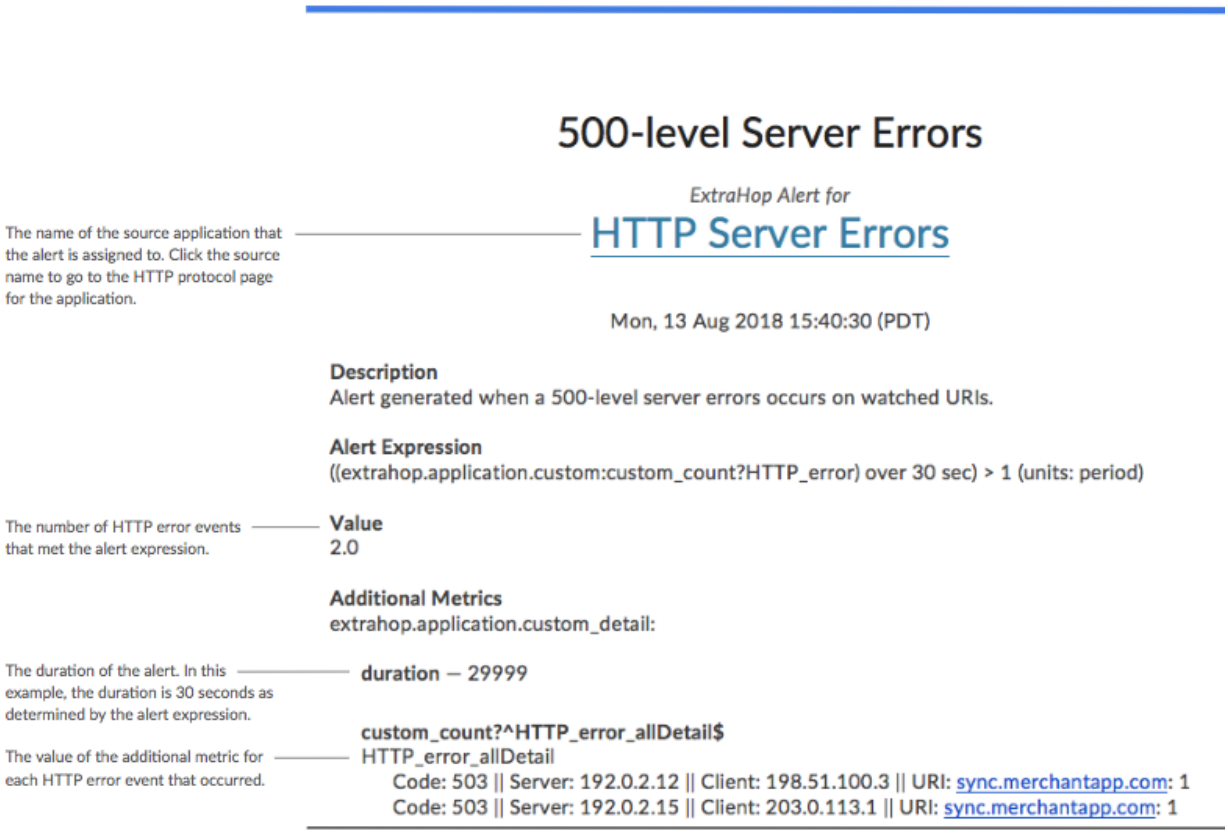
Consultez la page Alertes et consultez les notifications par e-mail

Maintenant que nous avons configuré l'alerte et l'avons attribuée à une source, nous pouvons vérifier si l' alerte a émis des entrées.

Cliquez **Alertes** depuis le menu supérieur pour afficher la page Alertes et vérifier si des alertes ont été émises pendant l'intervalle de temps sélectionné, comme dans la figure suivante :



Lorsqu'une alerte est émise, une notification est envoyée aux destinataires de l'e-mail spécifiés. L'exemple d'e-mail suivant montre que deux événements d'erreur HTTP se sont produits et répondaient aux conditions définies dans l'expression d'alerte et fournit des informations supplémentaires qui nous aident à rechercher la source des erreurs :



Dans notre exemple, nous constatons que deux erreurs 503 ont été renvoyées pour le même URI sur deux adresses IP de serveur différentes. Un code datu 503 peut indiquer un serveur surchargé qui nécessite davantage de ressources en processeur ou en mémoire pour traiter les demandes. En connaissant les adresses IP concernées, vous pouvez immédiatement examiner les problèmes potentiels sur les serveurs répertoriés.

Prochaines étapes

- Création de graphiques pour surveiller vos indicateurs personnalisés sur un tableau de bord ou une page de protocole.
- Configuration d'une alerte de tendance pour n'émettre des alertes que lorsque les erreurs du serveur évoluent, plutôt que pour chaque occurrence d'erreur.
- Ajoutez un intervalle d'exclusion à votre alerte pour supprimer les alertes lorsque des erreurs sont attendues.