Verfolgen Sie Serverfehler mit benutzerdefinierten Metriken und Warnmeldungen

Veröffentlicht: 2025-03-28

Das ExtraHop-System bietet zwar über 5.000 integrierte Messwerte, aber es gibt viele Situationen, in denen es effektiver ist, Netzwerkprobleme mit einer benutzerdefinierten Metrik zu verfolgen. Während integrierte Metriken Ihnen beispielsweise Probleme mit HTTP-Antworten und -Anfragen anzeigen, kann eine benutzerdefinierte Metrik Serverfehler der Stufe 500 identifizieren. Diese Art von Fehlern kann auf Gateway-Probleme, einen überlasteten Server oder Konfigurationsprobleme hinweisen.

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie einen Auslöser schreiben, um benutzerdefinierte Messwerte für Serverfehler zu sammeln, und wie Sie eine Alarm erstellen, die nur dann eine E-Mail-Benachrichtigung sendet, wenn diese spezifischen Fehler auftreten. Anschließend können Sie die folgenden Arten von Fragen zu Serverfehlern in Ihrem Netzwerk beantworten:

- Erhalten meine Kunden Serverfehler der Stufe 500?
- Welche Fehlercodes sind aufgetreten?
- Wann sind die Fehler aufgetreten?
- Auf welche URI wollte der Kunde zugreifen?
- Was ist die IP-Adresse des Client und Server, die von der Transaktion betroffen sind?

Voraussetzungen

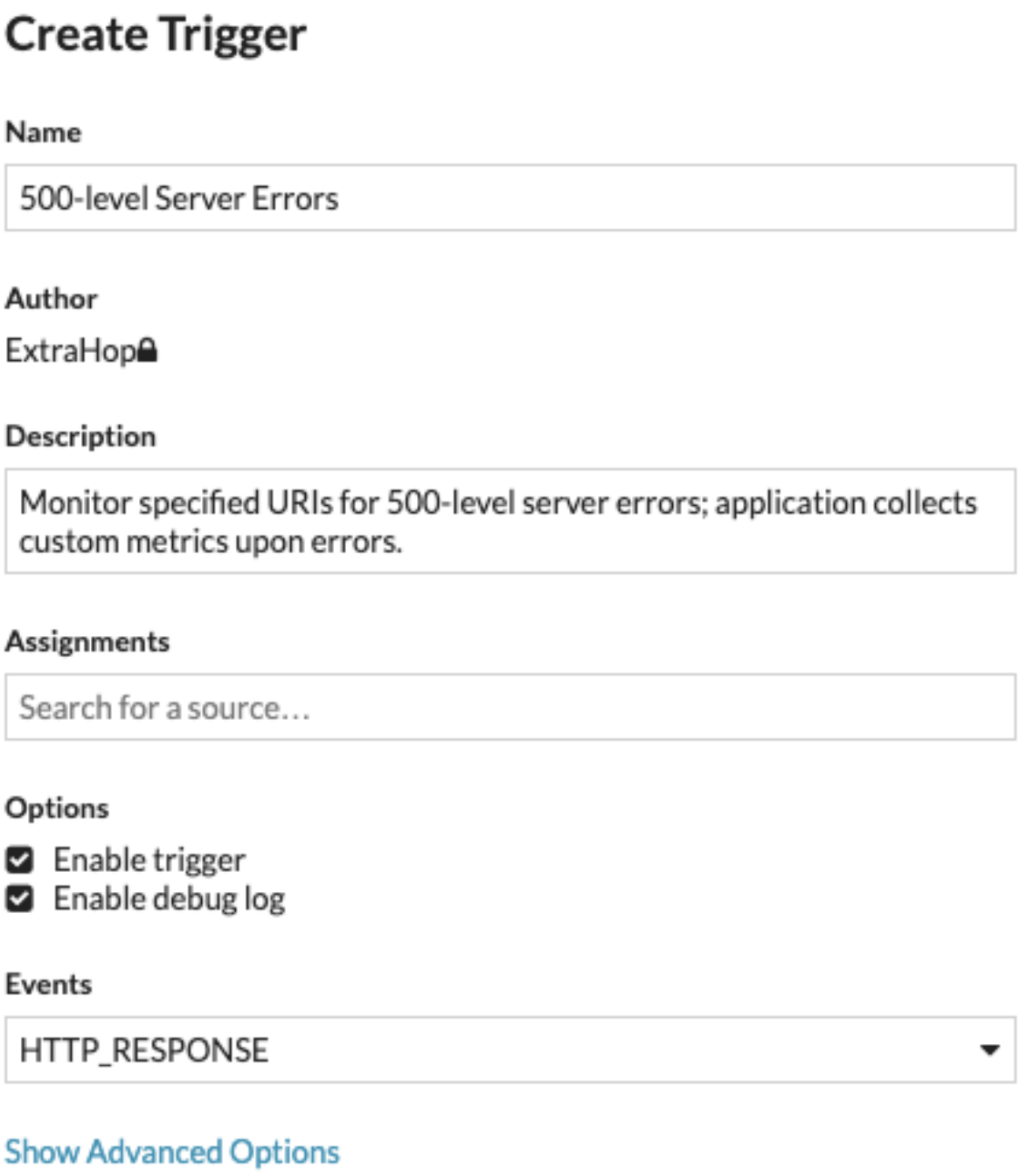
- Sie benötigen ein Benutzerkonto mit System- und Zugriffsadministrationsrechten.
- Ihr ExtraHop-System muss über Netzwerkdaten mit Webserver-Traffic verfügen.
- Ihr ExtraHop-System muss konfiguriert für das Senden von E-Mail-Benachrichtigungen bevor Sie Warn-E-Mails senden können.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie lesen Trigger und Warnmeldungen.
- Machen Sie sich mit den Prozessen zur Erstellung von Triggern vertraut, indem Sie lesen Einen Auslöser erstellen.
- Es ist hilfreich, grundlegende JavaScript-Kenntnisse zu haben.

Schreiben Sie einen Auslöser zum Sammeln von Fehlerdaten

Lassen Sie uns zunächst einen Auslöser erstellen, der bestimmte URIs auf Serverfehler der Stufe 500 überwacht. Wenn Fehler auftreten, sammelt der Auslöser Daten wie Fehlercodes und Server- und Client-IP-Adressen und überträgt diese Daten als benutzerdefinierte Messwerte an eine Anwendung.

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie auf die Systemeinstellungen ⚙ Symbol, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der **Name** Feld, geben Sie einen Namen für den Auslöser ein. Geben Sie für diese exemplarische Vorgehensweise ein `Serverfehler der Stufe 500`.
5. In der **Beschreibung** Feld, geben Sie Informationen über den Auslöser ein. Geben Sie für diese exemplarische Vorgehensweise ein `Überwachen Sie angegebene URIs auf Serverfehler der Stufe 500; die Anwendung sammelt bei Fehlern benutzerdefinierte Metriken .`

6. klicken **Debug-Log aktivieren**.
7. Klicken Sie in den **Ereignisse** Feld und Auswahl **HTTP_RESPONSE** aus der Liste.
   Die folgende Abbildung zeigt die Trigger-Einstellungen, die wir oben konfiguriert haben:



8. Klicken Sie auf **Herausgeber** Registerkarte.
9. Kopieren Sie im Trigger-Skript-Editor den folgenden Code und fügen Sie ihn ein:

```
// 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. In der `CHECK_URI_LIST` Variablen-Array, ersetzen Sie example.com durch die Hosts, URIs und Host-URI-Kombinationen, die der Auslöser überwachen soll.
11. In der `IGNORE_CLIENT_IP` variables Array, ersetzen Sie die Beispiel-IP-Adressen (180.57.175.147 und 172.16.156.130) durch die IP-Adressen, die der Auslöser ignorieren soll.

    Löschen Sie dieses Array oder kommentieren Sie es aus, wenn es keine zu ignorierenden IP-Adressen gibt.
12. klicken **Speichern und schließen**.

Der Trigger-Editor validiert die Syntax Ihres Skripts. Ungültige Aktionen, Syntaxfehler oder veraltete Elemente verhindern, dass Sie den Auslöser speichern, bis Sie den Code korrigiert oder die Syntaxüberprüfung deaktiviert haben.

Nachdem der Auslöser zugewiesen wurde und ausgeführt wurde, erstellt er die folgenden Komponenten, auf die wir bei der Konfiguration der Warnungseinstellungen in den nächsten Abschnitten verweisen werden:

HTTP-Serverfehler

Der Auslöser überträgt die aus den benutzerdefinierten Metriken gesammelten Daten an diese Anwendung.

HTTP_Fehler

Eine benutzerdefinierte Zählmetrik, die die Anzahl der aufgetretenen Fehler auf 500 Stufen erfasst .

HTTP_Error_AllDetail

Ein Brauch Detail-Metrik das sammelt die Codenummer, URI, Server-IP und Client-IP, auf denen jeder Fehler aufgetreten ist.

Weisen Sie den Auslöser einem Gerät zu

Bevor der Auslöser ausgeführt werden kann, muss er mindestens einem Gerät zugewiesen werden. In diesem Schritt weisen wir den Auslöser einem oder mehreren HTTP-Servern zu, die den Datenverkehr über die URIs unterstützen, die Sie im Auslöser angegeben haben.

1. klicken **Vermögenswerte**aus dem oberen Menü.
2. Klicken Sie unter Geräte nach Protokollaktivität auf **HTTP-Server**, und klicken Sie dann **Geräte** aus dem linken Bereich.
3. Wählen Sie in der Geräteliste das Kontrollkästchen neben einem oder mehreren Geräten aus, die den Datenverkehr über die URIs unterstützen.
4. Klicken Sie oben auf der Seite auf **Trigger zuweisen** um eine Liste von Triggern zu öffnen.
5. Wählen Sie den genannten Auslöser **Serverfehler der Stufe 500** die wir im vorherigen Abschnitt erstellt haben, und klicken Sie dann auf **Trigger zuweisen**.

Nächste Schritte

Hinweis: Weisen Sie Trigger nur relevanten Geräten zu, um unnötige Leistungseinbußen auf das System zu vermeiden. Eine gute Methode, um sicherzustellen, dass ein Auslöser nur auf relevanten Geräten ausgeführt wird, besteht darin, eine Gerätegruppe erstellen und weisen Sie den Auslöser dieser Gruppe zu.

Konfigurieren Sie eine Alarm, um eine benutzerdefinierte Metrik zu verfolgen

Als Nächstes konfigurieren wir die Warnungseinstellungen, die jedes Mal eine Alarm ausgeben und eine E-Mail-Benachrichtigung senden, wenn auf den URIs, die vom Auslöser überwacht werden, ein 500-Level-Fehler auftritt.

In den Warnungseinstellungen verweisen wir auf die folgenden benutzerdefinierten Metriken, die wir im Triggerskript erstellt haben:

HTTP_Fehler

Die benutzerdefinierte Zählmetrik, die die Anzahl der Fehler erfasst, die auf 500 Stufen auftreten. Wir werden die Warnungseinstellungen so konfigurieren, dass diese Metrik nachverfolgt wird, und jedes Mal, wenn ein Fehler auftritt, eine Alarm ausgeben.

http_error_AllDetail

Der Brauch Detail-Metrik das erfasst die Codenummer, den URI, die Server-IP-Adresse und die Client-IP-Adresse, auf der jeder Fehler aufgetreten ist. Wir werden die Warnungseinstellungen so konfigurieren, dass diese Fehlerdetails in Warn-E-Mails angezeigt werden.

Bevor Sie beginnen
Ihr ExtraHop-System muss konfiguriert für E-Mail-Benachrichtigungen.

1. Klicken Sie auf die Systemeinstellungen Symbol und dann klicken **Warnmeldungen**.
2. Klicken Sie **Erstellen** und geben Sie dann einen Namen für die Alarm in das **Name** Feld. Geben Sie für diese exemplarische Vorgehensweise Folgendes ein `Serverfehler auf 500-Level`.
3. Geben Sie eine Beschreibung der Alarm in das **Beschreibung** Feld. Geben Sie für diese exemplarische Vorgehensweise Folgendes ein `Warnung wird ausgegeben, wenn ein 500-Level-Serverfehler auf überwachten URIs auftritt.`
4. In der Art der Warnung Abschnitt, auswählen **Schwellenwert-Warnung** um eine Alarm auszugeben, wenn das Ereignis der verfolgten Metrik eintritt.
5. In der **Überwachte Metrik** Feld, Typ `HTTP_Fehler` und wählen Sie dann **Benutzerdefiniert - HTTP_Error** aus den Suchergebnissen.
6. In der Verhalten bei Warnmeldungen Abschnitt, auswählen **Einmal Alarm, wenn die Alarmbedingung erfüllt ist** um eine Alarm für jedes Vorkommen der verfolgten Metrik zu generieren.
7. In der Zustand der Warnung Abschnitt, geben Sie die folgende Bedingung an, um eine Alarm zu generieren, wenn das Ereignis der verfolgten Metrik mehr als einmal in einem Zeitraum von 30 Sekunden auftritt: `Alert when value > 1 during a 30s rollup`
8. In der Benachrichtigungen Abschnitt, geben Sie eine E-Mail-Adresse ein, die Warnmeldungen erhalten soll.

   Hinweis: Das Drop-down-Menü für E-Mail-Benachrichtigungsgruppen zeigt alle E-Mail-Gruppen, die in den Administrationseinstellungen konfiguriert sind. Sie können eine oder mehrere Gruppen auswählen , die Warnmeldungen erhalten sollen.
9. Klicken Sie **Erweiterte Optionen anzeigen** und klicken Sie dann **Metrik hinzufügen**.
10. Geben Sie in das Suchfeld ein `http_error_AllDetail`, und wählen Sie dann **Benutzerdefiniert - Http_Error_AllDetail** aus den Suchergebnissen.
11. Klicken Sie **Speichern**.

Weisen Sie die Alert-Konfiguration einer Quelle zu

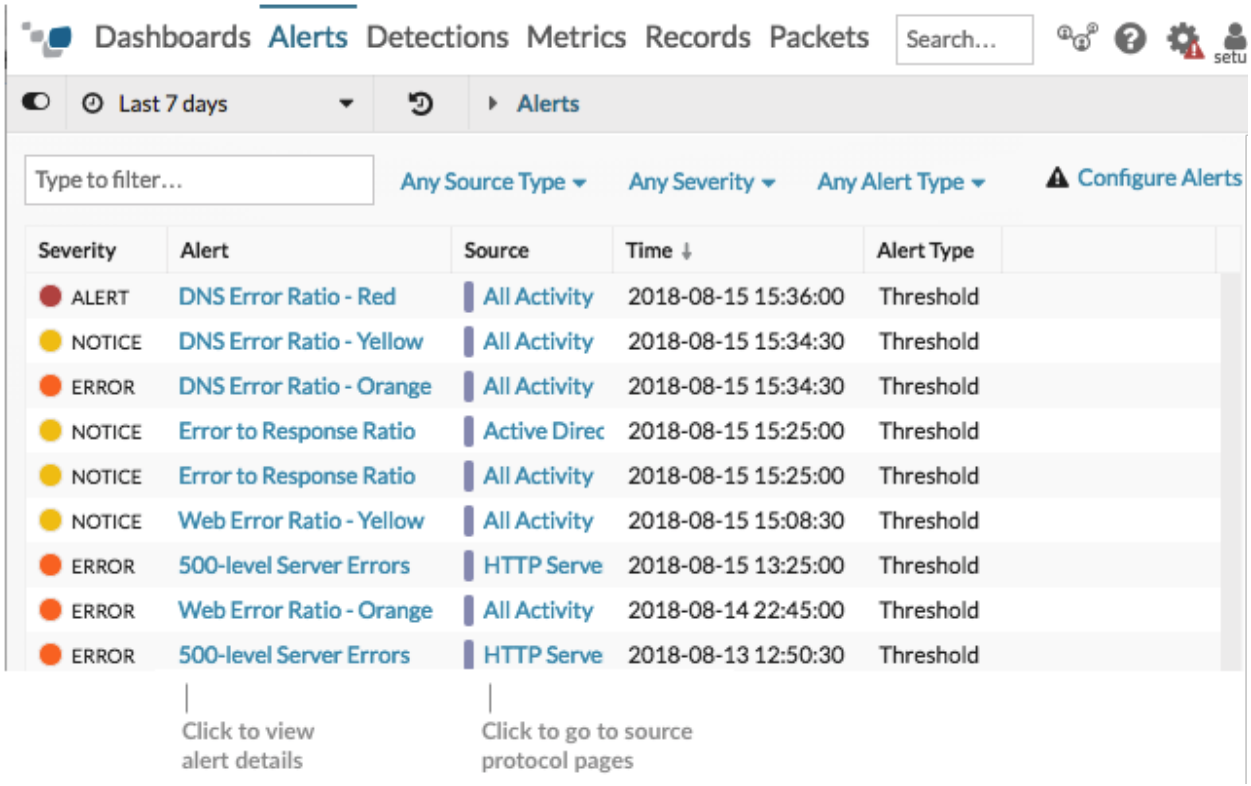
Ähnlich wie bei Triggern generiert das System erst dann Alerts, wenn die Alert-Konfiguration mindestens einer Metrik zugewiesen ist. Quelle. In diesem Schritt weisen wir die Alert-Konfiguration der Anwendung mit dem Namen HTTP Server Errors zu, die wir mit dem Trigger-Skript erstellt haben. Die benutzerdefinierten Metriken, die die Alarm verfolgen soll, sind für diese Anwendung bestimmt.

1. klicken **Vermögenswerte** aus dem oberen Menü.
2. klicken **Bewerbungen**, und wählen Sie dann die **HTTP-Serverfehler** Checkbox.
3. klicken **Warnung zuweisen** vom oberen Seitenrand aus, um eine Liste der Warnungskonfigurationen zu öffnen, die für eine Zuweisung in Frage kommen.
4. Wählen Sie den **Serverfehler der Stufe 500** Alarm, und klicken Sie dann auf **Alerts zuweisen**.

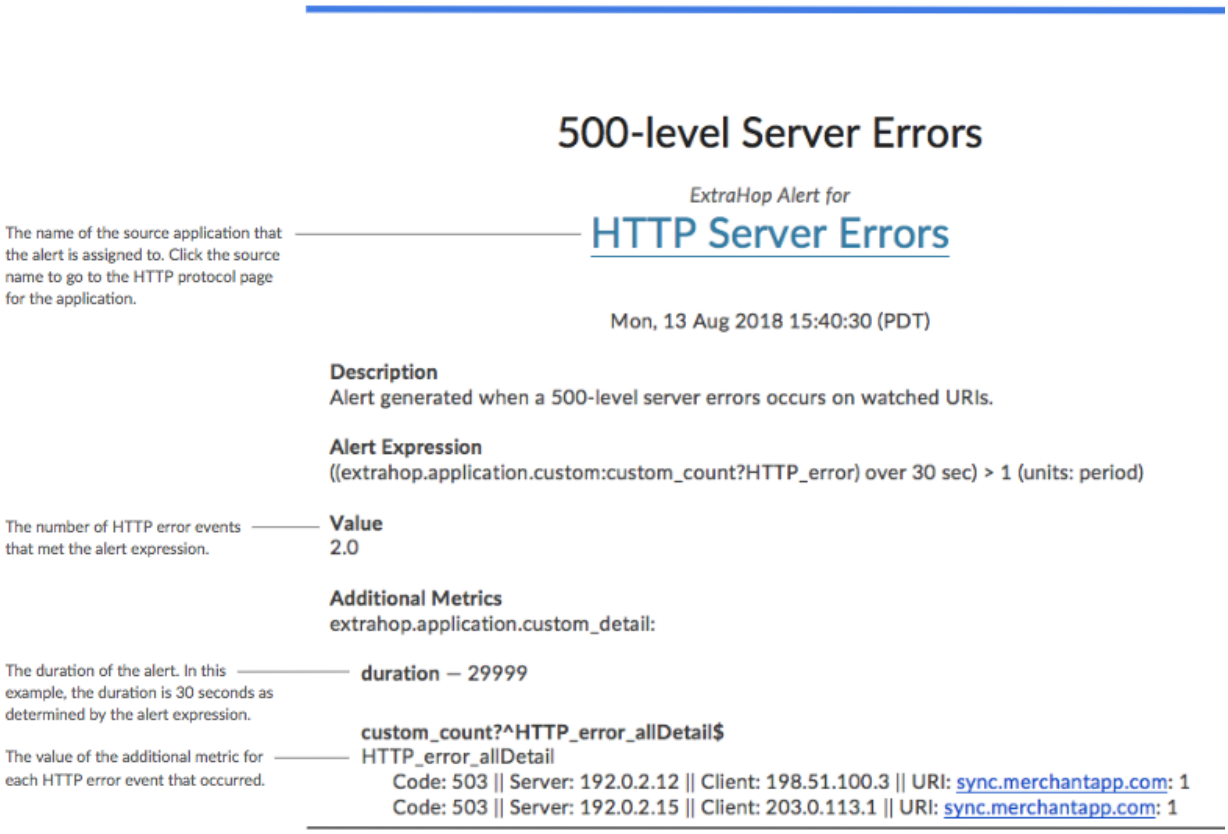
Überprüfen Sie die Seite „Benachrichtigungen“ und sehen Sie sich E-Mail-Benachrichtigungen an

Nachdem wir die Alarm konfiguriert und einer Quelle zugewiesen haben, können wir überprüfen, ob die Alarm Einträge ausgegeben hat.

klicken **Alerts** vom oberen Menü aus, um die Seite „Benachrichtigungen“ aufzurufen und nach Warnmeldungen zu suchen, die während des ausgewählten Zeitintervalls ausgegeben wurden, ähnlich der folgenden Abbildung:



Wenn eine Alarm ausgegeben wird, wird eine Benachrichtigung an die angegebenen E-Mail-Empfänger gesendet. Das folgende E-Mail-Beispiel zeigt, dass zwei HTTP-Fehlerereignisse aufgetreten sind, die die Bedingungen erfüllten, die wir im Warnungsausdruck festgelegt haben, und bietet zusätzliche Informationen, mit denen wir die Fehlerquelle untersuchen können:



In unserem Beispiel sehen wir, dass zwei 503-Fehler für dieselbe URI über zwei verschiedene Server-IP-Adressen zurückgegeben wurden. Ein 503-Statuscode kann auf einen überlasteten Server hinweisen, der mehr CPU- oder Speicherressourcen benötigt, um Anfragen zu bearbeiten. Wenn Sie die betroffenen IP-Adressen kennen, können Sie potenzielle Probleme auf den aufgelisteten Servern sofort untersuchen.

Nächste Schritte

- Diagramme erstellen um Ihre benutzerdefinierten Metriken auf einer Dashboard- oder Protokollseite zu überwachen.
- Eine Trendwarnung konfigurieren Warnmeldungen nur dann auszugeben, wenn Serverfehler im Trend liegen und nicht bei jedem Auftreten eines Fehlers.
- Fügen Sie Ihrer Alarm ein Ausschlussintervall hinzu um Warnmeldungen zu Zeiten zu unterdrücken, in denen Fehler zu erwarten sind.