Analysieren Sie Systemzustandsdiagramme, um die Triggerleistung zu bewerten

Veröffentlicht: 2023-09-14

Trigger sind ein leistungsstarkes Tool, mit dem Sie detaillierte Einblicke in Ihre Umgebung erhalten können. Trigger verbrauchen jedoch Ressourcen und beeinträchtigen die Systemleistung. Aus diesem Grund müssen Sie die Auswirkungen von Triggern auf Ihr ExtraHop-System mithilfe von Systemintegritätstools überwachen und bewerten.

In dieser exemplarischen Vorgehensweise erfahren Sie, wie Sie einen fehlerhaften Auslöser erstellen, die negativen Auswirkungen auf die Leistung mit Systemintegritätstools bewerten und dann den fehlerhaften Auslöser korrigieren. Sie werden auch lernen, wie Sie eine erstellen Dashboard um die Triggerleistung weiter zu überwachen.

Die Aufgaben in dieser exemplarischen Vorgehensweise helfen Ihnen bei der Beantwortung der folgenden Fragen zu den Auswirkungen von Triggern auf das ExtraHop-System:

- Hat mein neuer Auslöser zu einem Ausnahmefehler geführt?
- Wie viele Ausnahmefehler sind aufgetreten?
- Wie wirkt sich mein neuer Trigger auf die Leistung aus?

Voraussetzungen

- Sie benötigen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto mit eingeschränkten Schreibrechten oder vollen Schreibrechten.
- Ihr ExtraHop-System muss SMTP Verkehr.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Systemintegritäts-Dashboard und Auslöser Abschnitte in der ExtraHop System-Benutzerhandbuch.
- Machen Sie sich mit den Prozessen zur Erstellung von Triggern und Dashboards vertraut, indem Sie die Komplettlösung für Trigger und der Exemplarische Vorgehensweise für das Dashboard.

Einen Auslöser mit Ausnahmen erstellen

In diesem Verfahren erstellen Sie einen einfachen Auslöser, der die Verarbeitungszeit von protokolliert SMTP Antworten. Sie führen einen bewussten Fehler in die Triggerkonfiguration ein, um sicherzustellen, dass eine Trigger-Ausnahme auftritt.

1. Klicken Sie auf Systemeinstellungen Symbol, und klicken Sie dann **Auslöser**.
2. klicken **Erstellen**.
3. In der Name Feld, Typ `Bearbeitungszeit verfolgen`.
4. klicken **Debug-Log aktivieren**.
5. Klicken Sie auf **Ereignisse** Feld und fügen Sie dann die folgenden Ereignisse zur Triggerkonfiguration hinzu:
   - SMTP_REQUEST
   - SMTP_RESPONSE
   - SMPP_ANTWORT
6. Kopieren Sie den folgenden Code und fügen Sie ihn in den rechten Bereich ein:

```
var proto;
switch(event) {
    case 'SMTP_REQUEST':
    case 'SMTP_RESPONSE':
```

```
        proto = SMTP;
        break;
    case 'SMPP_RESPONSE':
        proto = SMPP;
        break;
}

if (!proto || !proto.processingTime) {
    debug('Processing Time = ' + proto.processingTime + " on " + event);
}
```

7. Klicken Sie auf Erweiterte Optionen anzeigen und wählen Sie dann **Allen Geräten zuweisen**.
8. klicken **Speichern**.
   Es wird eine Bestätigungsmeldung angezeigt, die besagt, dass das Triggerskript Fehler enthält. Ignorieren Sie die Meldung für die Zwecke dieser exemplarischen Vorgehensweise.
9. klicken **Trigger speichern**.

Nächste Schritte
Lassen Sie den Auslöser mindestens zehn Minuten lang laufen und überprüfen Sie dann das Systemstatus-Dashboard.

Hinweis: Überprüfen Sie immer die Leistungsdiagramme der Auslöser im Systemstatus-Dashboard, nachdem Sie einen neuen Auslöser erstellt oder einen vorhandenen geändert haben. Wenn Sie nur Auslöserergebnisse überprüfen, z. B. Metriken in einem benutzerdefinierten Dashboard oder Datensatzabfragen, verpassen Sie möglicherweise das vollständige Bild. Ein Auslöser scheint beispielsweise erwartungsgemäß Metriken zu sammeln, verbraucht aber möglicherweise auch eine große Menge an Ressourcen, was die Trigger-Warteschlange blockieren und dazu führen kann, dass Trigger aus der Warteschlange gelöscht werden.

Überprüfen Sie die Triggerdiagramme im Systemstatus-Dashboard

Das Systemstatus-Dashboard enthält Diagramme, die sich auf den Zustand und die Leistung der ExtraHop-Systemkomponenten und -dienste beziehen. In diesem Verfahren sehen Sie sich die Leistungsdiagramme der Auslöser im Systemstatus-Dashboard an, um die Auswirkungen des Auslöser zu überprüfen, den Sie im vorherigen Abschnitt erstellt haben.

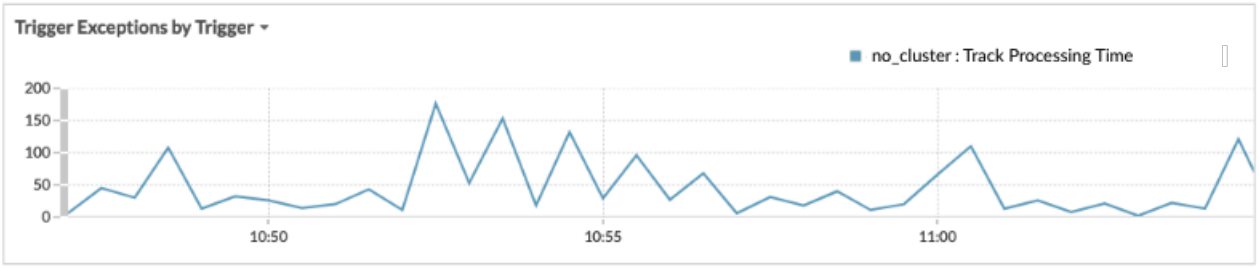
Hinweis: Die für den Beispiel-Trigger auf Ihrem System gemeldeten Leistungsergebnisse unterscheiden sich von den in diesem Abschnitt angezeigten Ergebnissen.

1. Klicken Sie in der oberen rechten Ecke des Fensters auf das Symbol Systemeinstellungen und wählen Sie dann **Gesundheit des Systems**.
2. Scrollen Sie nach unten zum Auslöser Region des Dashboard und suchen Sie den Einzelheiten zum Auslöser Diagramm.
   In diesem Diagramm sind die aktivsten Trigger auf Ihrem System zusammen mit den Zyklen, Ausführungen und Ausnahmen aufgeführt, die mit diesen Triggern verknüpft sind.

Trigger Details

Trigger	Trigger Cycles ↓	Trigger Executes	Trigger Exceptions
no_cluster: HTTP	13,961,591,464	293,620	0
no_cluster: System	13,486,481,553	587,356	0
no_cluster: Protocols	721,440,475	293,620	0
no_cluster:Track Processing Time	253,942,450	4,872	2,436

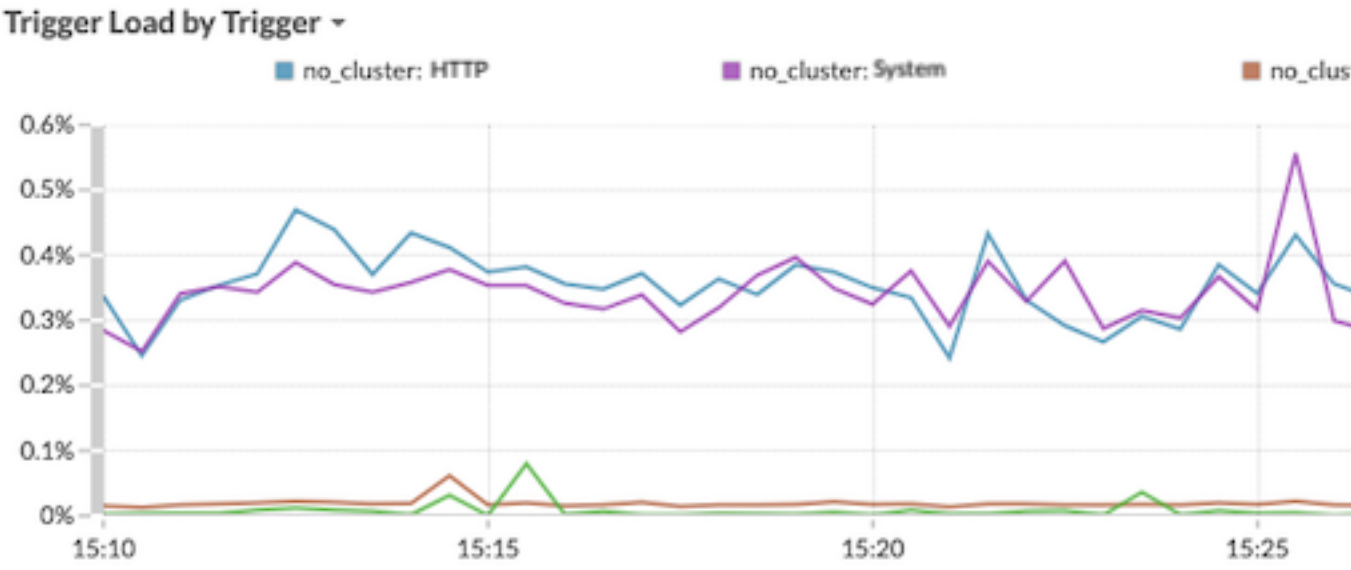
3. Suchen Sie Ihren Auslöser „Bearbeitungszeit verfolgen“ und sehen Sie sich die folgenden Informationen an:
   a) Vergleichen Sie die Werte in Trigger wird ausgeführt und Ausnahmen auslösen spalten. Diese Information zeigt, dass in der Hälfte der Fälle, in denen der Auslöser ausgeführt wird, eine Ausnahme auftritt. Da dieser Auslöser nicht sehr oft ausgeführt wird, sind die Auswirkungen nicht kritisch. Wenn der Auslöser jedoch so geändert würde, dass er bei einem beliebten Ereignis wie HTTP ausgeführt wird, könnte dies extreme Auswirkungen haben.
   b) Vergleichen Sie den Wert in Zyklen auslösen Spalte mit demselben Wert für andere Trigger, die auf Ihrem System ausgeführt werden. Diese Information zeigt, dass die durchschnittliche Anzahl der vom Auslöser verbrauchten Zyklen im Vergleich zu anderen laufenden Triggern relativ gering ist. Ein hoher Zyklusverbrauch kann darauf hindeuten, dass ein Triggerskript nicht effizient ist und möglicherweise zum Stillstand neigt, sodass Trigger in der Warteschlange sich sichern und aus der Warteschlange entfernt werden.
4. Scrollen Sie im Systemintegritäts-Dashboard nach unten und suchen Sie den Ausnahmen nach Trigger auslösen Diagramm. Das Diagramm zeigt den Auslöser „Verarbeitungszeit verfolgen“, den Sie erstellt haben, ähnlich der folgenden Abbildung:



Dieses Diagramm zeigt, welche Trigger Ausnahmen haben und wie viele Ausnahmen im angegebenen Zeitraum generiert wurden. Zeitstempel können Ihnen helfen, Ausnahmefehlermeldungen im Debug-Protokoll zu finden.

Hinweis: Um eine einzelne Linie im Diagramm hervorzuheben, klicken Sie auf den Namen des Auslöser und wählen Sie dann im Dropdownmenü die Option Fokus halten aus.

5. Scrollen Sie im Systemintegritäts-Dashboard nach oben und suchen Sie den Laden nach Trigger auslösen Diagramm. In dieser Tabelle ist der Prozentsatz der Zyklen auf dem ExtraHop-System aufgeführt, die von jedem Auslöser verbraucht werden.

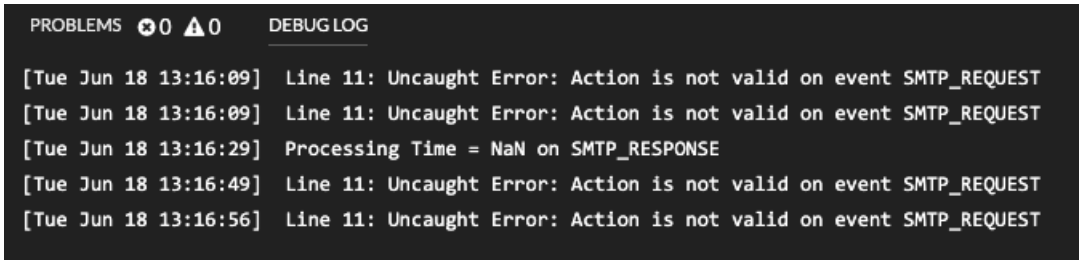


Anhand dieser Daten können Sie feststellen, ob der Ressourcenverbrauch zunimmt, ob der Auslöser häufiger ausgeführt wird als andere und ob Trigger-Ausnahmen auftreten. Es ist wichtig, die Triggerlast auf konsistente Erhöhungen des Ressourcenverbrauchs zu überprüfen, insbesondere wenn der Verbrauch nahe an der maximalen Speichermenge liegt, die für die Ausführung von Triggern verfügbar ist. Wenn nur wenig Triggerspeicher zur Verfügung steht, können Sie möglicherweise keine neuen Trigger ausführen.

Korrigieren Sie den Auslöser und zeigen Sie die Ergebnisse auf der Seite „Systemstatus“ an

In diesem Verfahren werden Sie Ausnahmen im Auslöser anzeigen Debug-Log die identifizieren, wo das Problem im Triggerskript auftritt, und dann beheben Sie den Fehler.

1. Klicken Sie in der oberen rechten Ecke des Fensters auf das Symbol Systemeinstellungen und wählen Sie dann **Auslöser**.
2. klicken **Bearbeitungszeit verfolgen** um den Auslöser zu öffnen.
3. Klicken Sie auf **Debug-Protokoll** Registerkarte.
   In dieser exemplarischen Vorgehensweise zeigt das Debug-Log eine Ausgabe an, die der folgenden Abbildung ähnelt:

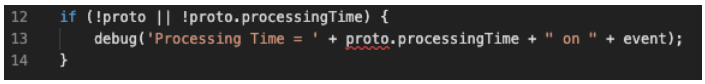


4. Scrollen Sie durch das Protokoll und suchen Sie nach Einträgen, die als Uncaught Error gekennzeichnet sind. Jede Fehlermeldung enthält den Zeitstempel, zu dem der Fehler aufgetreten ist, die Zeilennummer im Skript, die zu dem Fehler geführt hat, und eine Beschreibung des Fehlers.
   Im Protokoll sollte die folgende Fehlermeldung angezeigt werden:

```
Line 12: Uncaught Error: Action is not valid on event SMTP_REQUEST.
```

   Hinweis: Zusätzlich zu Ausnahmefehlern zeigt das Debug-Log auch nicht erfasste Syntaxfehler an, z. B. eine unerwartete geschweifte Klammer oder einen Typfehler, z. B. einen ungültigen Wert.

5. Klicken Sie auf **Herausgeber** Tabulatortaste, und suchen Sie dann Zeile 12 im Skript, um die Aktion zu identifizieren, die ungültig ist für SMTP Anfragen. In der folgenden Abbildung zeigt Zeile 12, dass die Aktion darin besteht, auf `processingTime` Eigentum an Veranstaltungen:



   Diese Informationen in Kombination mit den Informationen aus den Debug-Log-Fehlermeldungen zeigen, dass der Zugriff auf `processingTime` Die Eigenschaft ist bei SMTP-Anforderungsereignissen ungültig.

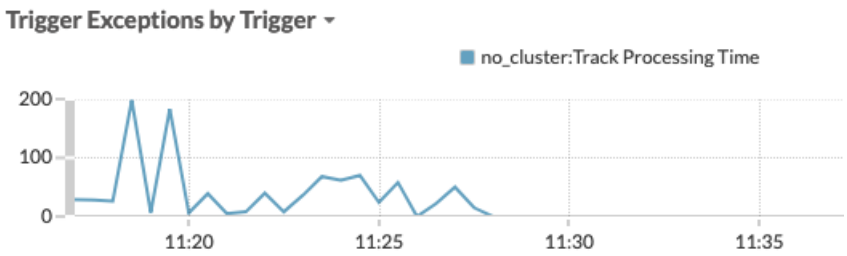
6. Entfernen Sie das nicht unterstützte SMTP-Ereignis aus dem Skript und der Triggerkonfiguration, indem Sie die folgenden Schritte ausführen:
   a) Löschen Sie die folgende Zeile aus dem Trigger-Skript:

```
case 'SMTP_REQUEST':
```

   b) Klicken Sie auf **Konfiguration** Tabulatur.

c) Löschen Sie SMTP_REQUEST aus dem Ereignisse Feld.

7. klicken **Speichern und schließen**.
   Der Auslöser wird gespeichert, ohne dass ein Validierungsfehler angezeigt wird.
8. Klicken Sie in der oberen rechten Ecke des Fensters auf das Symbol Systemeinstellungen und wählen Sie dann **Gesundheit des Systems**.
9. Warten Sie 5-10 Minuten und blättern Sie dann zum Ausnahmen auslösen Diagramm, das der folgenden Abbildung ähneln sollte:



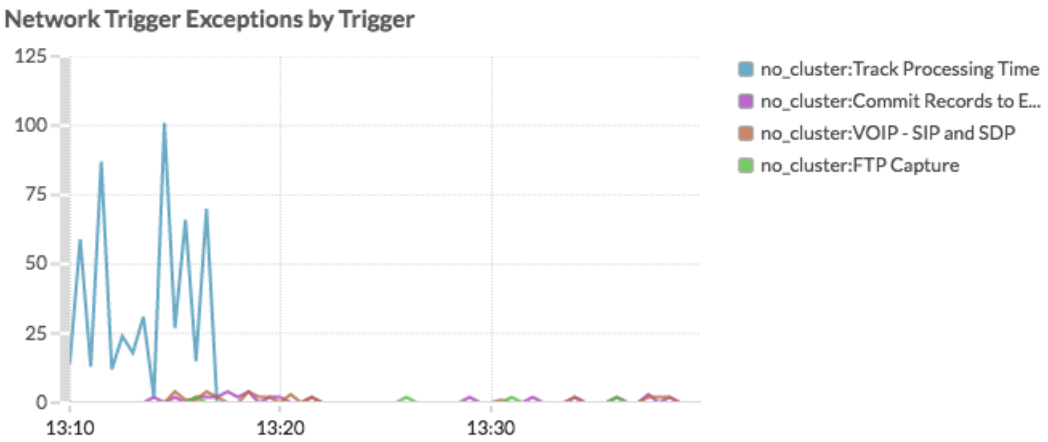
Erstellen Sie ein Trigger-Performance-Dashboard

In diesem Abschnitt erstellen Sie ein benutzerdefiniertes Dashboard zur Triggerleistung und fügen mehrere Diagramme hinzu, die in dieser exemplarischen Vorgehensweise beschrieben werden.

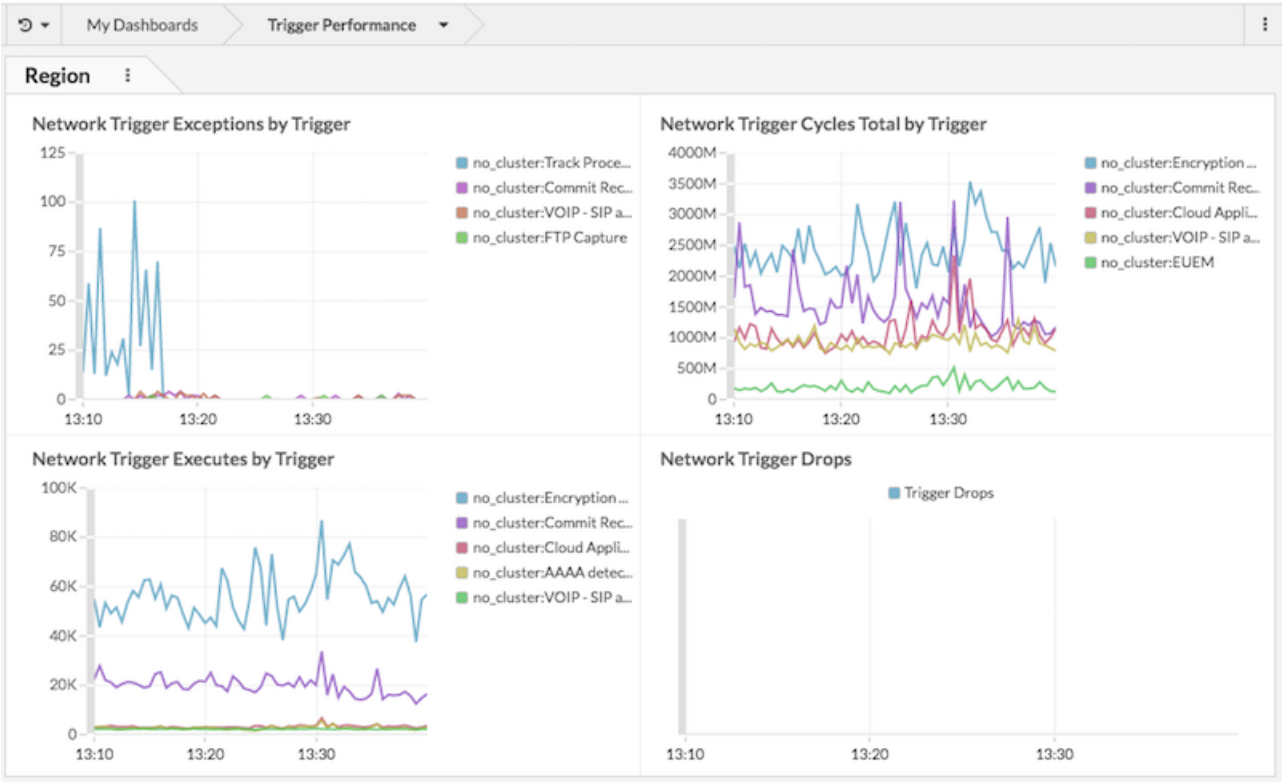
Durch das Hinzufügen von Systemintegritätsmetriken zu einem Dashboard können Sie anpassen, wie Sie die Daten anzeigen, z. B. den Diagrammtyp auswählen, Diagrammnotizen und Tipps in Textfeldern hinzufügen oder mehrere Metriken zu einem Diagramm hinzufügen.

Wenn Sie mit der Erstellung von Dashboards nicht vertraut sind, füllen Sie die Exemplarische Vorgehensweise für das Dashboard. Umfassende Informationen und Verfahren zum Erstellen und Anpassen von Dashboards finden Sie in der Dashboards Abschnitt der ExtraHop System-Benutzerhandbuch.

1. klicken **Dashboards** oben auf der Seite.
2. Klicken Sie auf das Befehlsmenü in der oberen rechten Ecke, und wählen Sie **Neues Dashboard**.
3. In der Titel Feld, Typ `Leistung auslösen`.
4. klicken **Erstellen**.
5. Klicken Sie in Ihrem neu erstellten Dashboard auf das leere Diagramm-Widget, um das zu starten Metric Explorer.
6. klicken **Quelle hinzufügen**.
7. Klicken Sie auf **Beliebiger Datensatztyp** Drop-down-Menü und wählen **Geräte**.
8. Wählen Sie aus der Liste den Namen des gewünschten ExtraHop-Systems aus.
9. In der Metriken Feld, Typ `Auslösen`, und wählen Sie dann **Systemzustand erfassen — Ausnahmen per Trigger auslösen** aus der Liste.
10. klicken **Speichern** um zu Ihrem Dashboard zurückzukehren.
    Das Diagramm sollte der folgenden Abbildung ähneln:



11. Ziehen Sie ein neues Diagramm-Widget in die Region und konfigurieren Sie das Diagramm, indem Sie die folgenden Schritte ausführen:
    a) Wählen Sie dasselbe ExtraHop-System aus, das Sie für das vorherige Diagramm angegeben haben.
    b) In der Metriken Feld, geben Sie Trigger ein, und wählen Sie dann **Systemzustand erfassen — Zyklen auslösen**.
    c) In der Einzelheiten Abschnitt, klicken **Keine**, und wählen Sie dann **Auslösen**.
    d) klicken **Speichern**.
12. Ziehen Sie ein neues Diagramm-Widget in die Region und konfigurieren Sie das Diagramm, indem Sie die folgenden Schritte ausführen:
    a) Wählen Sie dasselbe ExtraHop-System aus, das Sie für das vorherige Diagramm angegeben haben.
    b) In der Metriken Feld, geben Sie Trigger ein, und wählen Sie dann **Systemzustand erfassen — Trigger wird ausgeführt**.
    c) In der Einzelheiten Abschnitt, klicken **Keine**, und wählen Sie dann **Auslösen**.
    d) klicken **Speichern**.
13. Ziehen Sie ein neues Diagramm-Widget in die Region und konfigurieren Sie das Diagramm, indem Sie die folgenden Schritte ausführen:
    a) Wählen Sie dasselbe ExtraHop-System aus, das Sie für das vorherige Diagramm angegeben haben.
    b) In der Metriken Feld, geben Sie Trigger ein, und wählen Sie dann **Systemzustand erfassen — Ausfälle auslösen**.
    c) klicken **Speichern**.
14. klicken **Layoutmodus verlassen** aus der oberen rechten Ecke.
    Das Dashboard sollte der folgenden Abbildung ähneln:



Nächste Schritte

Hinweis Als nächsten Schritt können Sie das hochladen ExtraHealth-Paket zum ExtraHop-System, das ein Dashboard installiert, das eine Vielzahl von Systemzustandsdiagrammen enthält. Passen Sie das ExtraHealth-Dashboard an Ihre Bedürfnisse an oder kopieren Sie die gewünschten Diagramme in ein neues Dashboard. Weitere Informationen zu Bundles finden Sie im Bündel Abschnitt der ExtraHop System-Benutzerhandbuch.