ExtraHop

Konfigurieren Sie einen offenen Datenstream zum Senden von Metrikdaten an AWS Cloudwatch

Veröffentlicht: 2023-09-14

Das ExtraHop-System bietet mehrere Tools zum Anzeigen und Überwachen von Metriken zu Ihren Netzwerkdaten. Möglicherweise möchten Sie Metrikdaten jedoch mit einem Remote-Tool eines Drittanbieters wie Splunk, MongoDB oder Amazon Web Services (AWS) speichern oder analysieren. Die Datenstrom öffnen Mit der Funktion (ODS) können Sie eine Verbindung zu einem Drittanbieter-Tool konfigurieren, über das Sie bestimmte Metrikdaten senden können.

In dieser exemplarischen Vorgehensweise konfigurieren Sie ein ODS-Ziel für Amazon CloudWatch, schreiben einen Auslöser, der festlegt , welche HTTP-Metriken gesendet werden sollen, und initiieren die Übertragung von Daten an das Ziel.

Voraussetzungen

- Sie benötigen Zugriff auf ein ExtraHop-System mit einem Benutzerkonto, das über System- und Zugriffsadministrationsrechte verfügt.
- Ihr ExtraHop-System muss über Netzwerkdaten mit Webserver-Traffic verfügen.
- Sie müssen über ein Amazon Web Services-Konto verfügen und mit dem CloudWatch-Service vertraut sein.
- Machen Sie sich mit den Konzepten in dieser Komplettlösung vertraut, indem Sie die Offene Datenströme Abschnitt in der ExtraHop Admin-UI-Leitfaden und der Auslöser Thema.
- Machen Sie sich mit den Prozessen zur Erstellung von Triggern vertraut, indem Sie die Komplettlösung für Trigger.

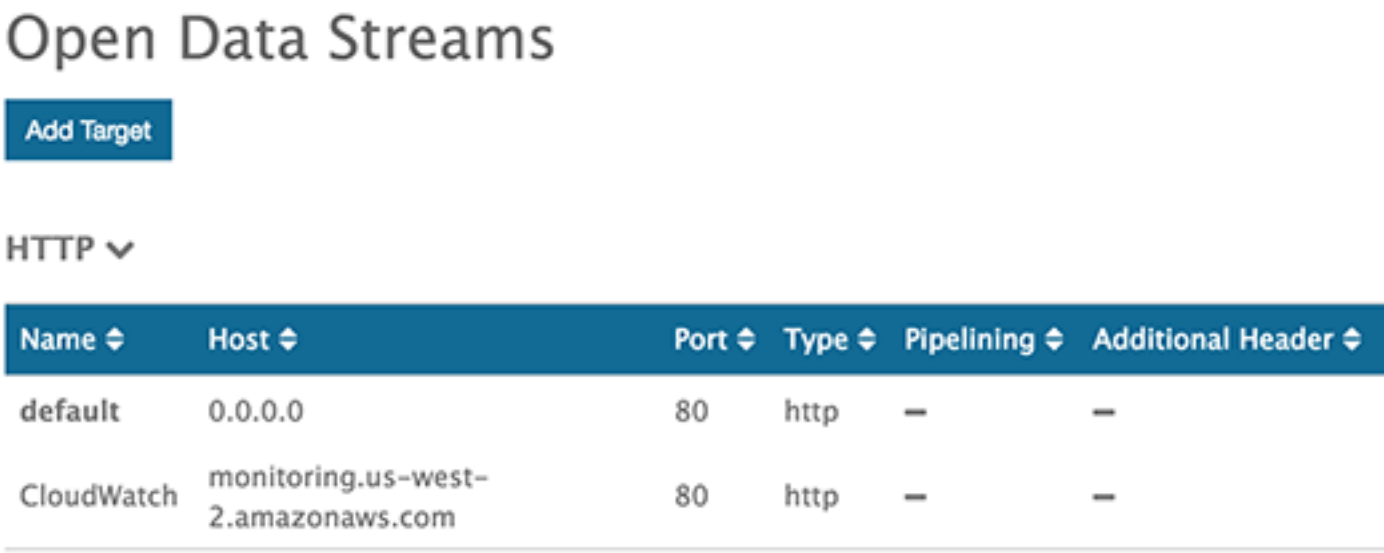
Ein ODS-Ziel konfigurieren

In den folgenden Schritten konfigurieren Sie den Host, den Port und die Authentifizierungsmethode für ein HTTP-Open-Data-Stream-Ziel.

1. Melden Sie sich bei dem ExtraHop-System, von dem Sie Daten senden möchten, mit einem Konto an , das über System- und Zugriffsadministrationsrechte verfügt.
2. Klicken Sie auf Systemeinstellungen Symbol, und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Aus dem Konfiguration des Systems Abschnitt, klicken **Offene Datenströme**.
4. klicken **Ziel hinzufügen**.
5. Wählen **HTTP** von der Typ des Ziels Drop-down-Liste.
6. In der Name Feld, Typ `CloudWatch`.
7. In der Gastgeber Feld, geben Sie die IP-Adresse oder den Hostnamen des Amazon-Webservers ein, an den Sie Daten senden möchten.
8. In der Hafen Feld, Typ `443` für die Portnummer, über die Sie Daten senden möchten.
9. In der Typ Feld, wählen **HTTPS** wie die Übertragung Protokoll Sie möchten Daten senden.
10. In der Authentifizierung Feld, wählen **Amazon AWS**.
11. In der Zugriffsschlüssel-ID Feld, geben Sie den Zugriffsschlüssel für Ihr AWS-Konto ein.
12. In der Geheimer Schlüssel Feld, geben Sie den geheimen Schlüssel für Ihr AWS-Konto ein.

13. In der Dienst Feld, geben Sie den Einstiegspunkt für den CloudWatch-Dienst ein, z. B. die Überwachung.
14. In der Region Feld, geben Sie die Region für den CloudWatch-Dienst ein, z. B. us-west-2.
15. In der Methode Feld, wählen **POSTEN** als REST-Methode ruft der Auslöser beim Senden von Daten auf.
16. klicken **Speichern**.

Das Ziel wird der HTTP-Tabelle auf der Seite Open Data Stream hinzugefügt, ähnlich der folgenden Abbildung:



Testen Sie die ODS-Konfiguration

In den folgenden Schritten schreiben Sie eine HTTP-REST-Anfrage, um die Übertragung von Daten vom ExtraHop-System zum AWS-Konto zu testen.

Wie im vorherigen Abschnitt konfiguriert, wendet die Testanforderung die POST-Methode an.

1. In der HTTP Tabelle, klicken **Bearbeiten** um das CloudWatch-Ziel zu öffnen.
2. In der Optionen Feld, kopieren Sie den folgenden HTTP-REST-Anforderungscode und fügen Sie ihn ein, um eine Metrik namens „Test“ mit einem Wert von 4 Byte an den CloudWatch-Dienst zu senden:

```
{
    "path": "/",
        "payload":
 "Action=PutMetricData&Version=2010-08-01&Namespace=test&MetricData.member.1.MetricN
            "headers": {
                "Content-Type": [
                    "application/x-www-form-urlencoded"
                ]
            }
}
```

Hinweis Weitere Informationen zur Syntax für die HTTP-REST-Anfrage finden Sie in Remote.HTTP Abschnitt der ExtraHop Trigger API-Referenz.

3. klicken **Speichern**.

4. In der HTTP Tabelle, bewegen Sie den Mauszeiger über den Status des Ziels, um die Verbindungsaktivität anzuzeigen.
   Wenn der Test erfolgreich ist, zeigt das Fenster die Anzahl der gesendeten und empfangenen Nachrichten und Byte sowie die Anzahl der Verbindungsversuche an, ähnlich der folgenden Abbildung:

Schreiben Sie den ODS-Trigger

In den folgenden Schritten schreiben Sie einen Auslöser, der angibt, welche Metriken an den CloudWatch-Dienst gesendet werden sollen, und der den Befehl zum Senden von Metrikdaten über den offenen Datenstream enthält.

Hinweis: Fügen Sie beim Erstellen des Auslöser in diesem Verfahren Kommentare hinzu, die den Zweck eines Codeausschnitts, Einschränkungen oder bewährte Methoden beschreiben.

1. Klicken Sie auf das ExtraHop-Logo in der oberen linken Ecke, um zum ExtraHop-System zurückzukehren.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann **Auslöser**.
3. klicken **Erstellen**.
4. In der Name Feld, Typ `Metriken für CloudWatch`.
5. klicken **Debug-Log aktivieren**.
6. In der Ereignisse Feld, wählen **HTTP_RESPONSE**.
7. Fügen Sie im rechten Bereich den folgenden Triggercode zum Editor hinzu, um „ExtraHop“ als benutzerdefinierten Namespace für die Metrikdaten anzugeben, die vom CloudWatch-Dienst angezeigt werden:

```
let namespace = 'ExtraHop';
```

Hinweis: Der Namespace-Wert darf nicht „AWS“ sein.

8. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um den Namen des ODS-Ziels anzugeben, das Sie zuvor konfiguriert haben:

```
let target = 'CloudWatch';
```

9. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um anzugeben, welche Metriken an den CloudWatch-Dienst übertragen werden sollen:

```
let metrics = [
    {
        'MetricName': 'processingTime',
        'Unit': 'Milliseconds',
        'Value' : HTTP.processingTime
    },
    {
        'MetricName': 'rspSize',
        'Unit': 'Bytes',
        'Value' : HTTP.rspSize
    }
];
```

10. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um die Struktur der Nutzlast zu spezifizieren, die definiert ist durch `PutMetricData` Methode in der Amazon CloudWatch-API:

```
let payload = 'Action=PutMetricData&Version=2010-08-01&Namespace=' +
 namespace;

let i,
    count = 0;

for (i = 0; i < metrics.length; i++) {
    let idx = i + 1,
        metric = metrics[i],
        val = metric.Value,
        attr;

    // If the metric value is NaN, do not publish.
    if (Number.isNaN(val)) {
        continue;
    }

    for (attr in metric) {
        payload += '&MetricData.member.' + idx + '.' +
            encodeURIComponent(attr) + '=' +
            encodeURIComponent(metric[attr]);
    }
    count++;
}

if (count == 0) {
    // No metrics to publish.
    return;
}
```

11. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um die HTTP-REST-Anfrage zu definieren, die den Anforderungspfad, die Header und die Nutzlast angibt:

```
let req = {
    'path': '/',
    'headers': {
        'Content-Type': 'application/x-www-form-urlencoded'
    },
```

```
    'payload': payload
};
```

Dieser Code ähnelt der Testanforderung, die Sie im vorherigen Verfahren ausgeführt haben.

12. Fügen Sie dem vorhandenen Skript den folgenden Triggercode hinzu, um das ODS-Ziel anzugeben und die Anforderung zur Übertragung von Metrikdaten an dieses Ziel zu initiieren:

```
Remote.HTTP(target).post(req);
```

13. klicken **Speichern**.

Weisen Sie den ODS-Trigger einem Gerät zu

Bevor der Auslöser Metrikdaten an den CloudWatch-Dienst senden kann, müssen Sie den Auslöser mindestens einem Gerät zuweisen. In dieser exemplarischen Vorgehensweise weisen Sie den Auslöser einem einzelnen HTTP-Server in einem Gerätegruppe.

Wenn Sie Ihre eigenen Trigger erstellen, weisen Sie Trigger nur den Geräten zu, von denen Sie Messwerte sammeln müssen, um die Leistungseinbußen Ihrer Trigger auf das ExtraHop-System zu minimieren.

1. klicken **Vermögenswerte** aus dem oberen Menü.
2. Klicken Sie im linken Bereich auf **Geräte**.
3. Wählen Sie in der Tabelle das Kontrollkästchen für ein einzelnes Gerät aus, von dem Sie wissen, dass es Web-Traffic hat.
4. Klicken Sie im Symbolmenü oben auf der Seite auf das Symbol „Auslöser zuweisen“.
5. Klicken Sie auf das Kästchen neben dem **Metriken für CloudWatch** Auslöser und dann klicken **Trigger zuweisen**.

Nachdem der Auslöser zugewiesen wurde, führt das System den Trigger kontinuierlich aus, bis der Auslöser deaktiviert wird.

Überprüfen Sie die Datenübertragung zum ODS-Ziel

Überprüfen Sie nach der Ausführung des Auslöser, ob Daten vom ODS-Ziel empfangen wurden, und deaktivieren Sie dann den Auslöser.

Wichtig: Amazon Web Services ist eine mehrstufige Lösung. Für die erste Stufe fallen keine Kosten an, sofern die Nutzung nicht überschritten wird. Führen Sie diesen Auslöser für einen kurzen Zeitraum aus , um zu verhindern, dass die zulässige Datenmenge überschritten wird. Wenn Sie den Auslöser nicht deaktivieren und die Nutzung Ihre zugewiesenen Bedingungen überschreitet, können Ihnen zusätzliche Kosten entstehen.

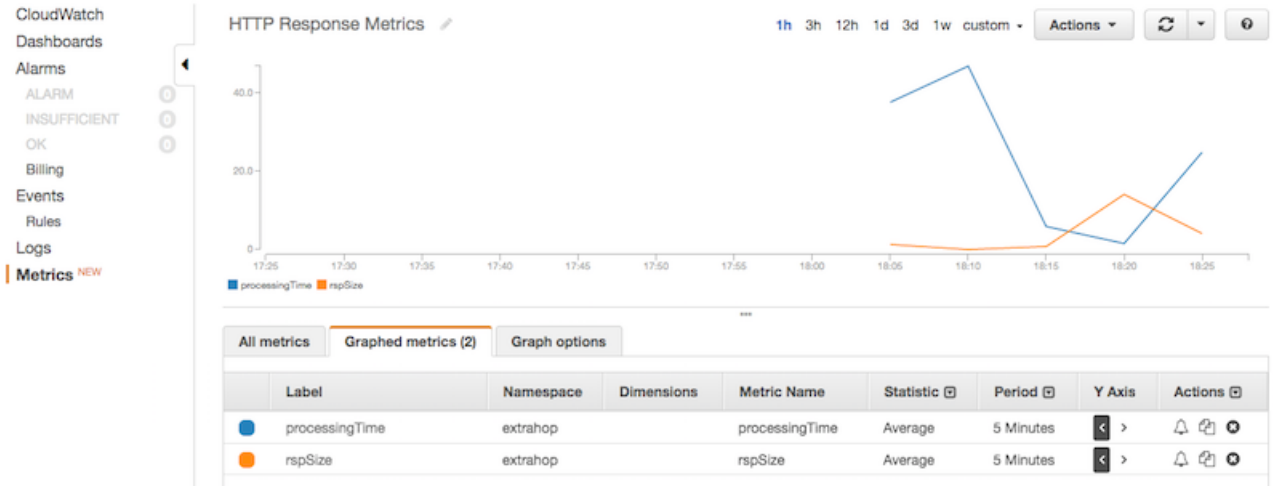
1. Lassen Sie den Auslöser für 10-15 Minuten laufen.
2. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Die gesamte Verwaltung**.
3. Aus dem Konfiguration des Systems Abschnitt, klicken **Offene Datenströme**.
4. In der HTTP Tabelle, bewegen Sie den Mauszeiger über den Status des CloudWatch-Ziels, um die Aktivität über die Verbindung anzuzeigen.

   Wenn der Auslöser erfolgreich ist, zeigt das Fenster die Anzahl der gesendeten und empfangenen Nachrichten und Byte sowie die Anzahl der Verbindungsversuche an.
5. Schließen Sie das Fenster mit den Administrationseinstellungen.
6. Klicken Sie auf das Symbol Systemeinstellungen, und klicken Sie dann auf **Auslöser**.
7. In der **Auslöser** Tabelle, klicken **Metriken für CloudWatch**.
8. klicken **Auslöser deaktivieren**.
9. klicken **Speichern und schließen**.

Ergebnisse in AWS CloudWatch anzeigen

Nachdem Sie überprüft haben, dass Metrikdaten an das ODS-Ziel gesendet wurden, können Sie die Daten mit dem CloudWatch-Dienst anzeigen. In den folgenden Schritten finden Sie die Metriken in CloudWatch und zeigen die Metrikdaten in einem Diagramm an.

1. Gehe zum Amazon Web Services Standort.
2. klicken **Melden Sie sich bei der Konsole an** und geben Sie Ihre AWS-Anmeldeinformationen Anmeldedaten.
3. Klicken Sie in der Liste der AWS-Services auf **CloudWatch**.
4. Klicken Sie im Menü auf der linken Seite auf **Vermögenswerte**.
   Auf der Registerkarte Alle Metriken werden der vom Auslöser erstellte „ExtraHop“ -Namespace und der durch die Testanforderung erstellte „Test“ -Namespace angezeigt.
5. klicken **ExtraHop**, und klicken Sie dann **Metriken ohne Dimensionen**.
   Auf der Registerkarte werden die beiden im Auslöser angegebenen Metriken „ProcessingTime“ und „RspSize“ angezeigt.
6. Aktivieren Sie das Kontrollkästchen neben jeder Metrik, um Metrikdaten im Diagramm anzuzeigen, ähnlich der folgenden Abbildung:



Nächste Schritte

Nachdem Sie erfolgreich Metrikdaten von Ihrem ExtraHop-System an AWS CloudWatch gesendet haben, versuchen Sie, den Auslöser so zu ändern, dass zusätzliche Metriken gesendet werden, oder ein neues ODS-Ziel zu erstellen, um Daten an andere Tools von Drittanbietern zu senden.