Splunk® Supported Add-ons Splunk Add-on for Amazon Kinesis Firehose released

Generated: 6/27/2019 8:32 am
# Table of Contents

Overview................................................................................................................................. 1
  About the Splunk Add-on for Amazon Kinesis Firehose...................................................... 1
  Source types for the Splunk Add-on for Amazon Kinesis Firehose................................... 1
  Release notes for the Splunk Add-on for Amazon Kinesis Firehose.................................. 3
  Release history for the Splunk Add-on for Amazon Kinesis Firehose.............................. 3

Before you install.......................................................................................................................... 7
  Hardware and software requirements for the Splunk Add-on for Amazon Kinesis Firehose.................................................................................................................. 7
  Installation and configuration overview for the Splunk Add-on for Amazon Kinesis Firehose................................................................................................................. 9

Install and configure on a managed Splunk Cloud deployment.............................................. 10
  Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment................................................................. 10
  Install and configure the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment................................................................. 10

Install and configure on a distributed Splunk Enterprise deployment.................................... 13
  Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment................................................................. 13
  Select and prepare your distributed Splunk Enterprise deployment for the Splunk Add-on for Amazon Kinesis Firehose................................................................. 13
  Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose.................................................................................................................. 15
  Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment................................................................. 15
  Configure HTTP event collector for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment.......................... 17

Install and configure on a single-instance Splunk Enterprise deployment............................... 20
  Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment...................................................... 20
  Install the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment...................................................... 20
  Configure HTTP event collector for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment...................... 21
Table of Contents

Configure Amazon Kinesis Firehose...............................................................23
  Configure Amazon Kinesis Firehose to send data to the Splunk platform..........................................................23

Troubleshooting.................................................................................................25
  Troubleshoot the Splunk Add-on for Amazon Kinesis Firehose..................25

Reference............................................................................................................29
  Performance reference for the Splunk Add-on for Amazon Kinesis Firehose..................................................................29
Overview

About the Splunk Add-on for Amazon Kinesis Firehose

<table>
<thead>
<tr>
<th>Version</th>
<th>1.2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Products</td>
<td>Amazon Kinesis Firehose data, CloudWatch, VPC Flow Logs, AWS CloudTrail, AWS GuardDuty</td>
</tr>
<tr>
<td>Visible in Splunk Web</td>
<td>No. This add-on does not contain any views.</td>
</tr>
</tbody>
</table>

The Splunk Add-on for Amazon Kinesis Firehose allows a Splunk software administrator to collect AWS CloudTrail, VPC Flow Logs, CloudWatch events, and raw or JSON data from Amazon Kinesis Firehose. This add-on provides CIM-compatible knowledge for data collected via the HTTP event collector. After the Splunk platform indexes the events, you can analyze the data directly or using other Splunk apps, such as the Splunk App for AWS and Splunk Enterprise Security. If you want to collect data from other AWS sources, see Splunk Add-on for Amazon Web Services.

Download the Splunk Add-on for Amazon Kinesis Firehose from Splunkbase.

For a summary of new features, fixed issues, and known issues, see Release Notes for the Splunk Add-on for Amazon Kinesis Firehose.

For information about installing and configuring the Splunk Add-on for Amazon Kinesis Firehose, see Installation and configuration overview for the Splunk Add-on for Amazon Kinesis Firehose.

See Questions related to Splunk Add-on for Amazon Kinesis Firehose on Splunk Answers.

Source types for the Splunk Add-on for Amazon Kinesis Firehose

The Splunk Add-on for Amazon Kinesis Firehose provides knowledge management for the following Amazon Kinesis Firehose source types:
<table>
<thead>
<tr>
<th>Data source</th>
<th>CIM compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudTrail events</td>
<td>AWS API call history form the AWS CloudTrail service, delivered as CloudWatch events. For CloudTrail events embedded within CloudWatch events, override the source name optional field &quot;aws_firehose_cloudtrail&quot; in the HEC token for index-time field extractions.</td>
</tr>
<tr>
<td>CloudWatch events</td>
<td>Data from CloudWatch. You can extract CloudTrail events embedded within CloudWatch events with this sourcetype as well.</td>
</tr>
<tr>
<td>GuardDuty events</td>
<td>GuardDuty events from CloudWatch. For GuardDuty events embedded within CloudWatch events, override the source name optional field with &quot;aws_cloudwatchevents_guardduty&quot; in the HEC token for index-time field extractions.</td>
</tr>
<tr>
<td>Amazon Kinesis Firehose JSON data</td>
<td>Any JSON formatted Firehose data.</td>
</tr>
<tr>
<td>Amazon Kinesis Firehose text data</td>
<td>Firehose raw text format.</td>
</tr>
<tr>
<td>VPC Flow Logs</td>
<td>VPC Flow Logs from CloudWatch. VPC Flow Logs must be preprocessed by an AWS Lambda.</td>
</tr>
</tbody>
</table>
Fixed issues
Version 1.2.0 of the Splunk Add-on for Amazon Kinesis Firehose fixes the following issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-04-25</td>
<td>ADDON-17577</td>
<td>Using the &quot;generate sample findings&quot; option in GuardDuty causes CloudWatch events to not be linebroken.</td>
</tr>
<tr>
<td>2018-04-25</td>
<td>ADDON-17576</td>
<td>Timestamp for VPC flow logs are based on record's arrival timestamp and are inaccurate.</td>
</tr>
</tbody>
</table>

Known issues

Version 1.2.0 of the Splunk Add-on for Amazon Kinesis Firehose contains the following known issues.

If no issues appear below, no issues have yet been reported.

Third-party software attributions

Version 1.2.0 of the Splunk Add-on for Amazon Kinesis Firehose does not incorporate any third-party software or libraries.

Release history for the Splunk Add-on for Amazon Kinesis Firehose

Latest release

The latest version of the Splunk Add-on for Amazon Kinesis Firehose is version 1.2.0. See Release notes for the Splunk Add-on for Amazon Kinesis Firehose for the release notes of this latest version.

Version 1.1.1

Version 1.1.1 of the Splunk Add-on for Amazon Kinesis Firehose was released on January 10, 2018 and has the same compatibility specifications as Version 1.2.0.

New features

Version 1.1.1 of the Splunk Add-on fixes a bug with CloudTrail field extractions.
Fixed issues

Version 1.1.1 of the Splunk Add-on for Amazon Kinesis Firehose does not have any fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-01-10</td>
<td>ADDON-16540</td>
<td>Fails to perform cloudtrail field extractions and transformations</td>
</tr>
</tbody>
</table>

Known issues

Version 1.1.1 of the Splunk Add-on for Amazon Kinesis Firehose contains the following known issues.

If no issues appear below, no issues have yet been reported.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-03-22</td>
<td>ADDON-17576</td>
<td>Timestamp for VPC flow logs are based on record's arrival timestamp and are inaccurate</td>
</tr>
<tr>
<td>2018-02-28</td>
<td>ADDON-17577</td>
<td>Using the &quot;generate sample findings&quot; option in GuardDuty causes CloudWatch events to not be linebroken.</td>
</tr>
</tbody>
</table>

Third-party software attributions

Version 1.1.1 of the Splunk Add-on for Amazon Kinesis Firehose does not incorporate any third-party software or libraries.

Version 1.1.0

Version 1.1.0 of the Splunk Add-on for Amazon Kinesis Firehose was released on December 21, 2017 and has the same compatibility specifications as Version 1.1.1.

Fixed issues

Version 1.1.0 of the Splunk Add-on for Amazon Kinesis Firehose does not have any fixed issues.
**Known issues**

Version 1.1.0 of the Splunk Add-on for Amazon Kinesis Firehose contains the following known issues.

If no issues appear below, no issues have yet been reported.

**Third-party software attributions**

Version 1.1.0 of the Splunk Add-on for Amazon Kinesis Firehose does not incorporate any third-party software or libraries.

**Version 1.0.1**

Version 1.0.1 of the Splunk Add-on for Amazon Kinesis Firehose was released on December 7, 2017 and has the same compatibility specifications as Version 1.1.0.

**Fixed issues**

Version 1.0.1 of the Splunk Add-on for Amazon Kinesis Firehose contains the following fixed issues.

<table>
<thead>
<tr>
<th>Date resolved</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-12-07</td>
<td>ADDON-16233</td>
<td>AWS App is not compatible with CloudTrail Logs ingested from Kinesis Firehose</td>
</tr>
</tbody>
</table>

**Known issues**

Version 1.0.1 of the Splunk Add-on for Amazon Kinesis Firehose contains the following known issues.

If no issues appear below, no issues have yet been reported.

**Third-party software attributions**

Version 1.0.1 of the Splunk Add-on for Amazon Kinesis Firehose does not incorporate any third-party software or libraries.
**Version 1.0.0**

Version 1.0.0 of the Splunk Add-on for Amazon Kinesis Firehose was released on November 20, 2017. It was the first release of this add-on.

**Known issues**

Version 1.0.0 of the Splunk Add-on for Amazon Kinesis Firehose contains the following known issues.

If no issues appear below, no issues have yet been reported.

<table>
<thead>
<tr>
<th>Date filed</th>
<th>Issue number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-11-20</td>
<td>ADDON-16233</td>
<td>AWS App is not compatible with CloudTrail Logs ingested from Kinesis Firehose</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Workaround: Use AWS Add-On to ingest CloudTrail Logs using the aws:cloudtrail sourcetype.</td>
</tr>
</tbody>
</table>

**Third-party software attributions**

Version 1.0.0 of the Splunk Add-on for Amazon Kinesis Firehose does not incorporate any third-party software or libraries.
Before you install

Hardware and software requirements for the Splunk Add-on for Amazon Kinesis Firehose

Splunk platform requirements

The Splunk Add-on for Amazon Kinesis Firehose requires Splunk platform version 6.6.X or later.

This add-on is supported in the following Splunk platform environments:

- managed Splunk Cloud
- Splunk Enterprise running in an AWS VPC
- Splunk Enterprise running in your own internal network with SSL certificates installed on each indexer. Self-signed certificates are not supported, you must use a CA-signed certificate.

This add-on is not supported in self-service Splunk Cloud at this time.

If you plan to run this add-on entirely in managed Splunk Cloud, there are no additional Splunk platform requirements.

If you plan to run this add-on in a self-managed AWS instance, see Splunk Enterprise, self-managed in the Cloud for sizing considerations specific to AWS.

If you are running this add-on on Splunk Enterprise in your own internal network, see System Requirements in the Splunk Enterprise Installation Manual.

SSL requirements

Amazon Kinesis Firehose requires HTTP Event Collector (HEC) endpoint to be terminated with a valid CA-signed certificate matching the DNS hostname used to connect to your HEC endpoint.

You must use a trusted CA-signed certificate. Self-signed certificates are not supported.

If you are sending data directly into Splunk Enterprise indexers in your own internal network or AWS VPC, a CA-signed certificate must be installed to each
of the indexers. If you are using an ELB to send data, you must install a CA-signed certificate on the load balancer.

Managed Splunk Cloud users are provided an ELB with a proper CA-signed certificate and a hostname for each stack. For ELB users on distributed Splunk Enterprise deployments, see Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose for information on how to configure an ELB with proper SSL certifications.

**Splunk admin requirements**

To install the Splunk Add-on for Amazon Kinesis Firehose, you must be a member of the admin or sc_admin role.

**Amazon Kinesis Firehose requirements**

The Splunk Add-on for Amazon Kinesis Firehose requires specific configuration in Amazon Kinesis Firehose. See What is Amazon Kinesis Firehose? in the AWS documentation.

**Event formatting requirements**

The Splunk Add-on for Amazon Kinesis Firehose supports data collection using either of the two HTTP Event Collector endpoint types: raw and event. If you collect data using the raw endpoint, no special formatting is required for most source types. The `aws:cloudwatchlogs:vpcflow` contains a nested events JSON array that cannot be parsed by the HTTP Event Collector. Prepare this data for the Splunk platform using an AWS Lambda function that extracts the nested JSON events correctly into a newline-delimited set of events. All other source types can be sent directly to the raw endpoint without any preprocessing.

If you collect data using the event endpoint, format your events into the JSON format expected by HTTP Event Collector before sending them from Amazon Kinesis Firehose to the Splunk platform. You can apply an AWS Lambda blueprint to preprocess your events into the JSON structure and set event-specific fields, which allows you greater control over how your events are handled by the Splunk platform. For example, you can create and apply a Lambda blueprint that sends data from the same Firehose stream to different indexes depending on event type.

For information about the required JSON structure, see Format events for HTTP Event Collector on the Splunk developer portal.
Installation and configuration overview for the Splunk Add-on for Amazon Kinesis Firehose

The way that you install and configure your environment to use the Splunk Add-on for Amazon Kinesis Firehose depends on your deployment of the Splunk platform. Follow the instructions that match your Splunk platform deployment.

- Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment
- Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment
- Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment

Deploying this add-on to self-service Splunk Cloud deployments is not supported at this time. If you are not sure whether you have a managed or self-service Splunk Cloud deployment, see Types of Splunk Cloud deployment.
Install and configure on a managed Splunk Cloud deployment

Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment

Follow these steps to use the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment. If you are not on a managed Splunk Cloud deployment, see Installation and configuration for the Splunk Add-on for Amazon Kinesis Firehose to find the instructions that match your Splunk platform deployment type.

1. Install and configure the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment.
2. Configure Amazon Kinesis Firehose to send data to the Splunk platform.

Install and configure the Splunk Add-on for Amazon Kinesis Firehose on a managed Splunk Cloud deployment

Follow these steps to install and configure the Splunk Add-on for Amazon Kinesis Firehose in your managed Splunk Cloud deployment.

If your managed Splunk Cloud deployment has a search head cluster, you will need additional assistance from Splunk Support to perform this configuration. See Managed Splunk Cloud with a search head cluster.

If your managed Splunk Cloud instance does not have a search head cluster, follow this procedure.

1. Decide what index you want to use to collect your Amazon Kinesis Firehose data. Ensure that this index is enabled and active. Sending data to a disabled or deleted index results in dropped events. If you need to create a new index, see Manage Splunk Cloud indexes.
2. Install the add-on to your Splunk Cloud deployment. For step-by-step instructions, see Install apps in your Splunk Cloud deployment.
3. Submit a case on the Splunk Support Portal. In the case, ask Splunk Support to enable HTTP event collector and create or modify an elastic load balancer to use with this add-on.

4. Wait for Splunk Support to perform the necessary setup and confirm with you once the HTTP event collector is enabled and your elastic load balancer is ready for use. Splunk Support will confirm the URL that you should use for your HTTP event collector endpoint. It should match this format: https://http-inputs-firehose-<your unique cloud hostname here>.splunkcloud.com:443.

5. Create an HTTP event collector token with indexer acknowledgments enabled. For step-by-step instructions, see Configure HTTP Event Collector on managed Splunk Cloud. During the configuration:
   1. Specify a Source type for your incoming data. See Source types for the Splunk Add-on for Amazon Kinesis Firehose for the source types supported by this add-on.
   2. Select the Index to which Amazon Kinesis Firehose will send data.
   3. Check the box next to Enable indexer acknowledgement.

6. Save the token that Splunk Web provides. You need this token when you configure Amazon Kinesis Firehose.

7. Repeat steps 5 and 6 for each source type from which you want to collect data. Each source type requires a unique HTTP event collector token.

Next step
Configure Amazon Kinesis Firehose to send data to the Splunk platform

Managed Splunk Cloud with a search head cluster

If your managed Splunk Cloud deployment has a search head cluster, follow this procedure.

1. Decide what index you want to use to collect your Amazon Kinesis Firehose data. Ensure that this index is enabled and active. Sending data to a disabled or deleted index results in dropped events. If you need to create a new index, see Manage Splunk Cloud indexes.

2. Submit a case on the Splunk Support Portal. In the case, ask Splunk Support to:
   1. Install the Splunk Add-on for Amazon Kinesis Firehose to your Splunk Cloud deployment
   2. Enable HTTP event collector and create or modify an elastic load balancer for use with this add-on.
   3. Create an HTTP event collector token with indexer acknowledgement enabled for each source type from which you plan to collect data from Amazon Kinesis Firehose. For each of the
tokens you request, ask Splunk Support to specify the following parameters:

◊ The **Source type** for your incoming data. See [Source types for the Splunk Add-on for Amazon Kinesis Firehose](#) for the source types supported by this add-on.
◊ The **Index** to which Amazon Kinesis Firehose will send data.
◊ **Enable indexer acknowledgement** should be true.

3. Wait for Splunk Support to perform the necessary setup and provide you with the following information:

♦ The full URL that you should use for your HTTP event collector endpoint. It should match this format:


♦ A token for each source type that you requested.

4. Save the tokens and the URL that Splunk Support provides. You need this information when you configure Amazon Kinesis Firehose.

**Next step**

Configure Amazon Kinesis Firehose to send data to the Splunk platform
Install and configure on a distributed Splunk Enterprise deployment

Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment

Follow these steps to use the Splunk Add-on for Amazon Kinesis Firehose on a distributed deployment of Splunk Enterprise. If you are not on a distributed Splunk Enterprise deployment, see Installation and configuration for the Splunk Add-on for Amazon Kinesis Firehose to find the instructions that match your Splunk platform deployment type.

1. Select and prepare your distributed Splunk Enterprise deployment for the Splunk Add-on for Amazon Kinesis Firehose
2. If your indexers are in an AWS virtual private cloud, Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose.
3. Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed deployment of Splunk Enterprise.
4. Configure HTTP Event Collector for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment.
5. Configure Amazon Kinesis Firehose to send data to the Splunk platform.

Select and prepare your distributed Splunk Enterprise deployment for the Splunk Add-on for Amazon Kinesis Firehose

Before you install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise, review the supported deployment topologies below. The diagrams show where the Splunk Add-on for Amazon Kinesis Firehose should be installed for data collection in the supported distributed deployment topologies. The add-on is also installed on search heads for search-time functionality, but that is not shown in the diagrams.

Choose the deployment topology that works best for your situation.
Indexers in AWS VPC

If your indexers are on AWS Virtual Private Cloud, use an elastic load balancer to send data to your indexers.

**Next step**

Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose

Indexers not in an AWS VPC

If your indexers are not in an AWS VPC, but are accessible from AWS Firehose via public IPs, install a CA-signed SSL certificate on each indexer, then send data directly to your indexers.
Prepare your indexers before you proceed:

1. Install a CA-signed SSL certificate on each indexer. For instructions, see Configure your indexer to use your certificates in *Securing Splunk Enterprise*.
2. Create a DNS name that resolves to the set of indexers that you plan to use to collect data from Amazon Kinesis Firehose. You will need this DNS name in a later step.

**Next step**

*Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment*

---

**Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose**

If your indexers are in an AWS Virtual Private Cloud, send your Amazon Kinesis Firehose data to an Elastic Load Balancer (ELB) with **sticky sessions enabled** and **cookie expiration disabled**. Follow the directions on this page to configure an ELB that can integrate with the Splunk HTTP event collector.

If your indexers are not in an AWS Virtual Private Cloud, this procedure does not apply to you. See *Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment*.

You must use an ELB. Application load balancers and network load balancers are not supported.

**Create an elastic load balancer**

Follow these steps to configure your ELB properly to receive data. For more detailed information about Elastic Load Balancers, see Elastic Load Balancing Documentation in the AWS documentation.

**Prerequisites**

- **Amazon Kinesis Firehose requires the HEC endpoint to be terminated with a valid CA-signed SSL certificate.** Import your valid CA-signed SSL certificates to AWS Certificate Manager or AWS IAM before creating or modifying your elastic load balancer. See Configure Security Settings in the AWS documentation.
Steps

1. Open the Amazon EC2 console.
2. On the navigation pane, under **Load balancing**, select **Load Balancers**.
3. Create a classic load balancer with the following parameters:

<table>
<thead>
<tr>
<th>Field in Amazon Web Services ELB UI</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select load balancer type</td>
<td>Classic load balancer</td>
</tr>
<tr>
<td>Load balancer name</td>
<td>Name of your load balancer</td>
</tr>
<tr>
<td>Load balancer protocol</td>
<td>HTTPS. Use the default or change the load balancer port.</td>
</tr>
<tr>
<td>Assign or select a security group</td>
<td>The chosen security group needs to allow inbound traffic from load balancer to HTTP event collector port on indexers.</td>
</tr>
<tr>
<td>Configure security settings</td>
<td>Select your CA-signed SSL certificate that you imported in the prerequisites step.</td>
</tr>
<tr>
<td>Health Check settings</td>
<td>Ping protocol: HTTPS</td>
</tr>
<tr>
<td></td>
<td>Ping port: 8088</td>
</tr>
<tr>
<td></td>
<td>Ping path: HTTPS:8088/services/collector/health/1.0</td>
</tr>
<tr>
<td></td>
<td>Timeout: 5 seconds</td>
</tr>
<tr>
<td></td>
<td>Interval: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Unhealthy threshold: 2</td>
</tr>
<tr>
<td></td>
<td>Healthy threshold: 10</td>
</tr>
<tr>
<td>Add EC2 instances</td>
<td>Add all indexers that you are using to index data with this add-on.</td>
</tr>
</tbody>
</table>

4. Click **Review and create**, and verify in the following review page that your load balancer details are correct. After creating your elastic load balancer, modify the **port configuration** and the **attributes** as described below.

**Modify an existing load balancer with the proper settings**

**Prerequisites**
- An elastic load balancer that has been configured with the correct basic settings. This includes setting the load balancer protocol to HTTPS and uploading a valid CA-signed SSL certificate.

Steps

1. From the **Load balancers** page in the EC2 console, select your elastic load balancer with the basic settings already configured.

2. Modify your load balancer with the following parameters:

<table>
<thead>
<tr>
<th>Field in Amazon Web Services ELB UI</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Check settings</td>
<td>Ping protocol: HTTPS</td>
</tr>
<tr>
<td></td>
<td>Ping port: 8088</td>
</tr>
<tr>
<td></td>
<td>Ping path: HTTPS:8088/services/collector/health/1.0</td>
</tr>
<tr>
<td></td>
<td>Timeout: 5 seconds</td>
</tr>
<tr>
<td></td>
<td>Interval: 30 seconds</td>
</tr>
<tr>
<td></td>
<td>Unhealthy threshold: 2</td>
</tr>
<tr>
<td></td>
<td>Healthy threshold: 10</td>
</tr>
<tr>
<td>Port configuration</td>
<td>Under Edit stickiness, select <strong>Enable load balancer generated cookie stickiness</strong>.</td>
</tr>
<tr>
<td></td>
<td>Leave <strong>expiration period</strong> blank.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Under Edit idle timeout, enter <strong>600 seconds</strong>.</td>
</tr>
</tbody>
</table>

**Next step**
Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment

**Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment**

**Prerequisite**
Select and prepare your distributed Splunk Enterprise deployment for the Splunk Add-on for Amazon Kinesis Firehose

**Steps**
1. Get the Splunk Add-on for Amazon Kinesis Firehose by downloading it from https://splunkbase.splunk.com/app/3719 or browsing to it using the app browser within Splunk Web.

2. Install the add-on on all search heads where Amazon Kinesis Firehose knowledge management is required and on one or more indexers. See Install an add-on in a distributed Splunk Enterprise deployment in *Splunk Add-Ons* for detailed instructions describing how to install a Splunk add-on in a distributed deployment.

Next step
Configure HTTP Event Collector for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment

Configure HTTP event collector for the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment

Prerequisites

- Install the Splunk Add-on for Amazon Kinesis Firehose on a distributed Splunk Enterprise deployment
- If your indexers are in an Amazon VPC, Configure an Elastic Load Balancer for the Splunk Add-on for Amazon Kinesis Firehose
- For optimal performance, set `ackIdleCleanup` to `true` in `inputs.conf` located in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local/inputs.conf` for *nix users and `%SPLUNK_HOME%\etc\apps\splunk_httpinput\local\inputs.conf` for Windows users.

Steps

1. Decide what index you want to use to collect your Amazon Kinesis Firehose data. Ensure that this index is enabled and active. Sending data to a disabled or deleted index results in dropped events. If you need to create a new index, see Create custom indexes in *Managing Indexers and Clusters of Indexers*.

2. Set up the HTTP Event Collector on your distributed deployment. For instructions on how to configure the HTTP Event Collector and create a server class using the deployment server, see Setting up distributed deployment of HTTP Event Collector data on the Splunk developer portal. When you define the server class, specify all indexers that you want to
use to collect Amazon Kinesis Firehose data.

3. Enable the deployment server and push the configuration to the clients.
4. On the deployment server, confirm that the Enable SSL box is checked in your HTTP Event Collector global settings.
5. Create a new HTTP event collector token with indexer acknowledgments enabled. For a detailed walkthrough, see Create an Event Collector token in Getting Data In. During the token configuration:
   1. Specify a Source type for your incoming data. See Source types for the Splunk Add-on for Amazon Kinesis Firehose for the source types supported by this add-on.
   2. Select the Index to which Amazon Kinesis Firehose will send data.
   3. Check the box next to Enable indexer acknowledgement.

6. Save the token that Splunk Web provides. You need this token when you configure Amazon Kinesis Firehose.
7. Repeat steps 5 and 6 for each additional source type from which you want to collect data. Each source type requires a unique HTTP event collector token.

**Next step**
Configure Amazon Kinesis Firehose to send data to the Splunk platform
Install and configure on a single-instance Splunk Enterprise deployment

Installation steps for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment

Follow these steps to use the Splunk Add-on for Amazon Kinesis Firehose on single-instance Splunk Enterprise. If you are not on a single-instance Splunk Enterprise deployment, see Installation and configuration for the Splunk Add-on for Amazon Kinesis Firehose to find the instructions that match your Splunk platform deployment type.

1. Install the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment.
2. Configure HTTP Event Collection for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment.
3. Configure Amazon Kinesis Firehose to send data to the Splunk platform.

Install the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment

Install the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment.

1. Download the Splunk Add-on for Amazon Kinesis Firehose from https://splunkbase.splunk.com/app/3719 or browsing to it using the app browser within Splunk Web.
2. Install the add-on to your Splunk Enterprise instance. For step-by-step instructions, see Install an add-on in a single-instance Splunk Enterprise deployment.
3. If you have not already done so, install an SSL certificate on your Splunk Enterprise instance. For instructions, see Configure your indexer to use your certificates in Securing Splunk Enterprise.
Next step
Configure HTTP event collector for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment

Configure HTTP event collector for the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment

Prerequisite

- Install the Splunk Add-on for Amazon Kinesis Firehose on a single-instance Splunk Enterprise deployment
- For optimal performance, set `ackIdleCleanup` to true in `inputs.conf` located in `$SPLUNK_HOME/etc/apps/splunk_httpinput/local/inputs.conf` for *nix users and `%SPLUNK_HOME%\etc\apps\splunk_httpinput\local\inputs.conf` for Windows users.

Steps

1. Decide what index you want to use to collect your Amazon Kinesis Firehose data. Ensure that this index is enabled and active. Sending data to a disabled or deleted index results in dropped events. If you need to create a new index, see Create custom indexes in Managing Indexers and Clusters of Indexers.
2. Go to Settings > Data inputs > HTTP Event Collector click Global Settings.
3. Check the box next to Enable SSL, then click Save.
4. Create an HTTP event collector token with indexer acknowledgments enabled. For a detailed walkthrough, see Set up and use the HTTP Event Collector in Getting Data In. During the configuration:
   1. Specify a Source type for your incoming data. See Source types for the Splunk Add-on for Amazon Kinesis Firehose for the source types supported by this add-on.
   2. Select an Index to which Firehose will send data.
   3. Check the box next to Enable indexer acknowledgement.
5. Save the token that Splunk Web provides. You need this token when you configure Amazon Kinesis Firehose.
6. Repeat steps 4 and 5 for each additional source type from which you want to collect data. Each source type requires a unique HTTP event collector token.
Next step
Configure Amazon Kinesis Firehose to send data to the Splunk platform
Configure Amazon Kinesis Firehose

Configure Amazon Kinesis Firehose to send data to the Splunk platform

Prerequisite
Before you configure Amazon Kinesis Firehose to send data to the Splunk platform, you need to prepare the Splunk platform to receive the data. If you have not already done so, see Installation and configuration overview for the Splunk Add-on for Amazon Kinesis Firehose and follow the directions for your Splunk platform deployment type.

Go to the AWS Management Console to configure Amazon Kinesis Firehose to send data to the Splunk platform. See Choose Splunk for Your Destination in the AWS documentation for step-by-step instructions. Repeat this process for each token that you configured in the HTTP event collector, or that Splunk Support configured for you.

When prompted during the configuration, enter the following information:

<table>
<thead>
<tr>
<th>Field in Amazon Kinesis Firehose configuration page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>Select <strong>Splunk</strong>.</td>
</tr>
<tr>
<td><strong>Splunk cluster endpoint</strong></td>
<td>If you are using managed Splunk Cloud, enter your ELB URL in this format: <a href="https://http-inputs-firehose-">https://http-inputs-firehose-</a>&lt;your unique cloud hostname here&gt;.splunkcloud.com:443. For example, if your Splunk Cloud URL is <a href="https://mydeployment.splunkcloud.com">https://mydeployment.splunkcloud.com</a>, enter <a href="https://http-inputs-firehose-mydeployment.splunkcloud.com:443">https://http-inputs-firehose-mydeployment.splunkcloud.com:443</a>. If you are on a distributed Splunk Enterprise deployment, enter the URL and port of your data receiver node. For example, if you have an ELB that proxies traffic to your indexers with DNS name example-test-123456789.us-east-1.elb.amazonaws.com and port 443, enter</td>
</tr>
</tbody>
</table>
If you want to send data directly to multiple Splunk indexers acting as your data collection nodes, you need a URL that resolves to multiple IP addresses (one for each node) with the port enabled for HTTP event collector on those nodes. For example, if the hostname that resolves to your indexers is examples.example-deployment.com, enter https://inputs.example-deployment.com:8088.

<table>
<thead>
<tr>
<th>Field in Amazon Kinesis Firehose configuration page</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Splunk endpoint type</td>
<td>If you are on a single-instance Splunk Enterprise deployment, enter the HEC endpoint URL and port. For example, if your HEC endpoint is <a href="https://10.130.33.112:8088">https://10.130.33.112:8088</a>, enter <a href="https://10.130.33.112:8088">https://10.130.33.112:8088</a>.</td>
</tr>
<tr>
<td>Authentication token</td>
<td>Enter your HTTP event collector token that you configured or received from Splunk Support.</td>
</tr>
<tr>
<td>S3 backup mode</td>
<td>Best practice: Backup all events to S3 until you have validated that events are fully processed by the Splunk platform and available in Splunk searches. You can adjust this setting after you have verified data is searchable in the Splunk platform.</td>
</tr>
</tbody>
</table>

After you configure Amazon Kinesis Firehose to send data to the Splunk platform, go to the Splunk search page and search for the source types of the data you are collecting. See Source types for the Splunk Add-on for Amazon Kinesis Firehose for a list of source types that this add-on applies to your Firehose data. Validate that the data is searchable in the Splunk platform before you adjust the S3 backup mode setting in the AWS Management Console.

If you are unable to see your data in the Splunk platform, see troubleshoot the Splunk Add-on for Amazon Kinesis Firehose.
Troubleshooting

Troubleshoot the Splunk Add-on for Amazon Kinesis Firehose

General troubleshooting

For troubleshooting tips that you can apply to all add-ons, see Troubleshoot add-ons in *Splunk Add-ons*. For additional resources, see Support and resource links for add-ons in *Splunk Add-ons*.

Cannot launch add-on

This add-on does not have views and is not intended to be visible in Splunk Web.

For more details about add-on visibility and instructions for turning visibility off, see Troubleshoot add-ons in * Splunk Add-ons*.

Firehose error exceptions

See Data Not Delivered to Splunk in the AWS documentation.

Data delivery errors

You can view the error logs related to Kinesis Firehose data delivery failure using the Kinesis Firehose console or CloudWatch console. See the **Accessing CloudWatch Logs for Kinesis Firehose** section in the Monitoring with Amazon CloudWatch Logs topic from the AWS documentation.

SSL-related data delivery errors

Amazon Kinesis Firehose requires HTTP Event Collector (HEC) endpoint to be terminated with a valid CA-signed certificate matching the DNS hostname used to connect to your HEC endpoint. If you are seeing an error message "Could not connect to the HEC endpoint. Make sure that the HEC endpoint URL is valid and reachable from Kinesis Firehose," then your SSL certificate might not be valid.

Test if your SSL certificate is valid by opening your HEC endpoint in a web browser. If you are using a self-signed certificate, you will receive an error in your browser. For example, in Google Chrome, the error looks like:
Error: "Received event for unconfigured/disabled/deleted index" but indexer acknowledgement is returning positives

If you see this error in messages or logs, edit your HEC token configurations to send data to an index that is able to accept data.

If indexer acknowledgment for your Amazon Kinesis Firehose data is successful but your data is not successfully indexed, the data may have been dropped by the parsing queue as an unparsable event. This is expected behavior when data is processed successfully in the input phase but cannot be parsed due to a logical error. For example, if the HTTP event collector is routing data to an index that has been deleted or disabled, the Splunk platform will still accept the data and begin processing it, which triggers indexer acknowledgement to confirm receipt. However, the parsing queue cannot pass the data to the index queue because the specified index is not available, thus the data does not appear in your index. For more information about the expected behavior of the indexer acknowledgement feature, see Indexer acknowledgment on the Splunk Developer Portal.

If you suspect events have been dropped, search your "last chance" index, if you have one configured. If you are on Splunk Cloud, contact Splunk Support if you do not know the name of your last chance index. If you are on Splunk Enterprise, see the lastChanceIndex setting in indexes.conf for more information about the behavior of the last chance index feature and how to configure it.

Troubleshoot performance with the Splunk Monitoring Console

The Monitoring Console provides prebuilt dashboards with detailed topology and performance information about your Splunk Enterprise deployment.
Queue fill dashboard

If you are experiencing performance issues with your HEC server, you may need to increase the number of HEC-enabled indexers to which your events are sent. Follow these steps to check whether your indexers are at capacity.

Steps

1. Navigate to Monitoring Console > Overview > Queue Fill.
2. From the Queue Fill dashboard, select Indexing queue from the Queue dropdown and 90th percentile from the Aggregation dropdown.
3. (Optional) Set a Platform Alert to get a notification when one or more of your indexer queues reports a fill percentage of 90% or more. This alert can inform you of potential indexing latency.
   ✦ From Managed Splunk Cloud, navigate to Settings > Searches, reports, and alerts and select Monitoring Console in the app filter. Find the SIM Alert - Abnormal State of Indexer Processor platform alert, and click Edit > Enable to enable the alert.
   ✦ From the Splunk Enterprise Monitoring Console Overview page, click Triggered Alerts > Enable or Disable and then click the Enabled checkbox next to the SIM Alert - Abnormal State of Indexer Processor platform alert.

See determine queue fill pattern for an example of a healthy and unhealthy queue.

HTTP Event Collector dashboards

The Monitoring Console also comes with pre-built dashboards for monitoring the HTTP Event Collector. To interpret the HTTP event collector dashboards information panels correctly, be aware of the following:

- The Data Received and Indexed panel shows data as "indexed" even when the data is sent to a deleted or disabled index. Thus, this graph shows the data that is acknowledged by the indexer acknowledgment feature, even if that data is not successfully indexed. See "Error: 'Received event for unconfigured/disabled/deleted index' but indexer acknowledgment is returning positives" for more information about the expected behavior of the indexer acknowledgment feature when the index
The Errors panel is expected to show a steady stream of errors under normal operation. These errors occur because Amazon Kinesis Firehose sends empty test events to check that the authentication token is enabled, and the HTTP event collector cannot parse these empty events. Filter the Errors panel by Reason to help find significant errors.

For more information about the specific HTTP event collector dashboards, see HTTP Event Collector dashboards.

The HTTP event collector dashboards show all indexes, even if they are disabled or have been deleted.

**Troubleshoot with prebuilt panels**

The Splunk Add-on for Amazon Kinesis Firehose has four prebuilt panels that you can use to check if your data is being indexed for each index, indexer, or all indexers. There is also a panel that shows if your data is being properly load balanced across all indexers.

For information on how to use prebuilt panels, see Access prebuilt panels included with add-ons.
Reference

Performance reference for the Splunk Add-on for Amazon Kinesis Firehose

This page provides reference information on performance testing for version 1.1.1 of the Splunk Add-on for Amazon Kinesis Firehose. Use this information to enhance the performance of your own Amazon Kinesis Firehose instance.

Many factors impact performance results, including file size, file compression, event size, deployment architecture, and hardware. These results should be used as reference information and do not represent performance in all environments.

Testing architecture

The throughput data and conclusions provided here are based on performance testing using a managed Splunk Cloud deployment running in the following environment.

<table>
<thead>
<tr>
<th>Instance type</th>
<th>EC2 (c4.8xlarge)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>60 GB</td>
</tr>
<tr>
<td>CPU</td>
<td>36 cores</td>
</tr>
</tbody>
</table>

Results

The following throughput data was measured with a single cluster master with seven indexers and one search head.

This table shows the average throughput for different sourcetypes achieved in performance testing under specific operating conditions and is subject to change when any of the hardware and software variables changes. These numbers are not indicative of Firehose performance but were measured using the backend HEC library that the Splunk Add-on for Amazon Kinesis Firehose uses. Use this data for a very rough reference only.

<table>
<thead>
<tr>
<th>Sourcetype</th>
<th>Throughput (MB/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic single line</td>
<td>142</td>
</tr>
<tr>
<td>CloudTrail</td>
<td>140</td>
</tr>
</tbody>
</table>
[1] We observed close to linear performance with the addition or subtraction of indexers. If you see traffic flowing to your Splunk instance mostly without exception with occasional "Could not connect to the HEC endpoint" errors, your HEC server may be too busy processing other data requests. Increase the number of HEC-enabled indexers to prevent your indexers from being filled. See the **Accessing CloudWatch logs for Kinesis Firehose** in the Monitoring with Amazon CloudWatch Logs documentation for instructions on how to view data delivery error logs.