Integrating Cribl Stream with AWS Security Data Lake

Setting up Cribl Stream to send data in OCSF Format to AWS

# Table of Contents

[Table of Contents 2](#_Toc119502844)

[Overview of Integration 3](#_Toc119502845)

[Setup Cribl Stream 3](#_Toc119502846)

[Download 3](#_Toc119502847)

[Cribl Cloud 3](#_Toc119502848)

[Pack Install 3](#_Toc119502849)

[Setup Pipeline 4](#_Toc119502850)

[Modify the Pipeline 5](#_Toc119502851)

[Architecture 8](#_Toc119502852)

[Private Cloud and On-premises Setup 8](#_Toc119502853)

[IAM Roles and Trust 8](#_Toc119502854)

[Mechanics of the Integration 9](#_Toc119502855)

[Troubleshooting 10](#_Toc119502856)

[Contacting Support 10](#_Toc119502857)

# Overview of Integration

Cribl Stream allows customers to send their data from any source to AWS Security Data Lake in OCSF schema. Customers will setup their Cribl instance and then download the Cribl Pack for OCSF from the Cribl Pack Dispensary and install the pack.

# Setup Cribl Stream

Customers have the option to run Cribl Stream locally, in their private cloud or on our AWS based SaaS Cribl Cloud service.

## Download

Cribl Stream can be downloaded from <https://cribl.io/download/> and run locally on a Linux based machine. Customers can also use our docker container images to run Cribl Stream locally. The free version will allow up-to 1TB of data to be processed daily.

## Cribl Cloud

Customers can leverage our SaaS offering on <https://cribl.cloud> to setup and deploy Cribl Stream. The free version will allow up-to 1TB of data to be processed daily.

## Pack Install

Navigate to <https://packs.cribl.io> and find the Cribl Pack for OCSF. The pack can also be installed from within the product by navigating to **Packs** under **Processing**:

Graphical user interface, application

Description automatically generated

From there, select **New Pack** and **Add from Dispensary**:

Graphical user interface, text, application, email

Description automatically generated

Add the Pack from within the Cribl UI:

Graphical user interface, text, application

Description automatically generated

## Setup Pipeline

Once installed, you should see the pack in your Cribl Stream instance:Graphical user interface, application, Teams

Description automatically generated

Click on the Pack and navigate to the Pipelines. Here you will see a list of Pipelines that are tied to the OCSF Asset Classes:

Table

Description automatically generated

## Modify the Pipeline

Select the pipeline and you can start modifying them to comply with your sources. Each pipeline will have specific instructions on how to modify the field mapping for your specific events.

Graphical user interface, text, application, email

Description automatically generated

Fields that have the EDIT ME setting should be opened and modified with your specific fields. These should match the guidelines posted in the OCSF guidelines <https://schema.ocsf.io> .

Graphical user interface, text, application, email

Description automatically generated

## Pack Updates

Cribl will maintain updates to the content pack via the Cribl Stream UI :

Graphical user interface, application

Description automatically generated

Architecture

### Private Cloud and On-premises Setup

Setup Cribl for collection of events from on-premises or private cloud deployments to send events into AWS Security Data Lake in OCSF format.

Diagram

Description automatically generated

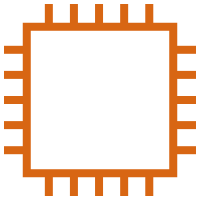
### IAM Roles and Trust

AWS Cloud



**2**

VPC – Cribl Cloud



Cribl Stream

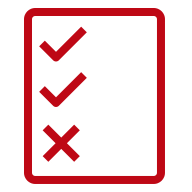
Worker Node

IAM Role



Trust Cribl Cloud

Permission



VPC – Customer Cloud



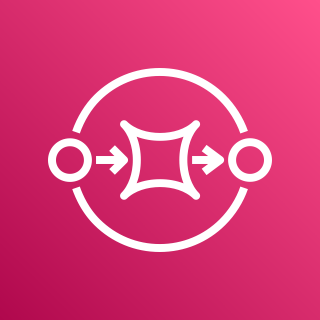
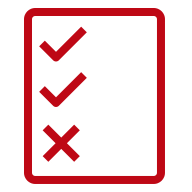
**3**

**1**

IAM Role



Assume Allow Permissions



Amazon SQS



Amazon S3

1. Create the IAM Role with the permissions for access to S3 and SQS within the Customer Account.
2. Create a trust relationship between Cribl Cloud Account and the Customer IAM role.
3. Access the S3 buckets between the two AWS Accounts.

## Mechanics of the Integration

Graphical user interface

Description automatically generated[Link to Diagram in Cribl Docs](https://docs.cribl.io/stream/event-processing-order)

Package as parquet

Transform to OCSF

Cribl Stream will collect the events from the source and then transform the data into OCSF by using the Cribl Pack for OCSF. Once the data has been transformed, it will then be delivered to the destination (AWS Security Data Lake S3) as a parquet formatted file.

## 

## Troubleshooting

When you run your data through Cribl Stream, make sure that you are sending the events to your AWS Security Data Lake in parquet format. Make sure that your permissions are set properly for your IAM role to write into the S3 bucket.

## Contacting Support

Support for Cribl can be engaged through our [Cribl Slack Community](https://cribl.io/community/), [Cribl Curious](https://curious.cribl.io/), and paid support via the support portal <https://cribl.io/support> .

Cribl also offers free training and education through our site:

* <https://sandbox.cribl.io>
* <https://cribl.io/university/>

## Use Cases for Cribl

Cribl Stream can take the native data formats for existing solutions like Palo Alto Networks or Azure NSG Logs and tranform them into OCSF compliant schemas. Any non-AWS native security sources of data can be sent through Cribl Stream Pack for OCSF and mapped to the schema.