Splunk® Supported Add-ons
Splunk Add-on for AWS released

Generated: 3/04/2022 9:24 am

Table of Contents

Table of Contents

Overview

Introduction to the Splunk Add-on for Amazon Web Services

Version	5.2.0
Supported vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, SNS
CIM-compliant vendor products	AWS CloudTrail, AWS CloudWatch, AWS Config and AWS Config Rules, Amazon Inspector, Amazon Virtual Private Cloud
Add-on has a web UI	Yes. This add-on contains views for configuration.

Use the Splunk Add-on for Amazon Web Services (AWS) to collect CloudTrail log, performance, billing, and IT and security data on Amazon Web Service products. See Use cases for the Splunk Add-on for AWS for more information.

This add-on provides modular inputs and CIM-compatible knowledge to use with other Splunk apps, such as the Splunk App for AWS, Splunk Enterprise Security, and Splunk IT Service Intelligence.

Download the Splunk Add-on for Amazon Web Services from Splunkbase. See Deploy the Splunk Add-on for AWS for information about installing and configuring this add-on.

See Release notes for the Splunk Add-on for AWS for a summary of new features, fixed issues, and known issues.

See Questions related to Splunk Add-on for Amazon Web Services on the Splunk Community page.

Use cases for the Splunk Add-on for AWS

Use the Splunk Add-on for Amazon Web Services (AWS) to collect data on Amazon Web Services. The Splunk Add-on for AWS offers pretested add-on inputs for four main use cases, but you can create an input manually for a miscellaneous Amazon Web Service. See Configure miscellaneous inputs for the Splunk Add-on for AWS.

See the following table for use cases and corresponding add-on collection methods:

Use case	Add-on inputs
Use the Splunk Add-on for AWS to calculate the **cost of your Amazon Web Service usage** over different lengths of time.	• Billing (Cost and Usage report) • Billing (Legacy)
Use the Splunk Add-on for AWS to push **CloudTrail log data** to the Splunk platform. CloudTrail allows you to audit your AWS account.	• CloudTrail • Kinesis data • S3 Access Logs
Use the Splunk Add-on for AWS to push **IT and performance data** on your Amazon Web Service into the Splunk platform.	• Amazon CloudWatch data • CloudFront Access Logs • ELB Access Logs

Use case	Add-on inputs
	• Config and Config Rules data • Description data • Kinesis data • S3 Access Logs • SQS-based Access Logs • VPC flow log data
Use the Splunk Add-on for AWS to push **security data** on your Amazon Web Service into the Splunk platform.	• Inspector data • Config and Config Rules data • Description data • Kinesis data • S3 Access Logs • SQS-based Access Logs • VPC flow log data

Consider the Splunk Add-on for Amazon Kinesis Firehose as an alternative to the Splunk Add-on for AWS

See About the Splunk Add-on for Amazon Kinesis Firehose to consider an alternative add-on for pushing AWS data to the Splunk platform. See the following table to understand the differences:

Splunk Add-on for Amazon Kinesis Firehose	Splunk Add-on for AWS
Pushes data.	Pulls data.
For high volume, streaming data.	For low volume, rarely changing data.
If high availability and scale are required for your deployment.	For normal availability and scale.
Sends data directly to indexers so you do not need to manage forwarders.	Unless your deployment is in Splunk Cloud, you must manage the forwarders.

Source types for the Splunk Add-on for AWS

The Splunk Add-on for Amazon Web Services (AWS) provides the index-time and search-time knowledge for alerts, events, and performance metrics. Source types and event types map the Amazon Web Service data to the Splunk **Common Information Model (CIM)**.

See Troubleshoot the Splunk Add-on for AWS to find source types for internal logs.

See the following table for source types and event types for AWS data mapping:

Data type	Source type	Description	Supported input types	Data models
Billing	aws:billing aws:billing:cur	`aws:billing` represents billing reports that you have configured in AWS. `aws:billing:cur` represents cost and usage reports.	Billing (Cost and Usage Report) Billing (Legacy)	• CIM: None • ES Custom: None • ITSI: None

Data type	Source type	Description	Supported input types	Data models
CloudFront Access Logs	aws:cloudfront:accesslogs	Represents CloudFront Access Logs.	SQS-based S3 Generic S3 Incremental S3	• CIM: None • ES Custom: None • ITSI: None
CloudTrail	aws:cloudtrail	Represents AWS API call history from the AWS CloudTrail service.	SQS-based S3 CloudTrail Generic S3 Incremental S3	• CIM: Authentication, Change Analysis • ES Custom: None • ITSI: None
CloudWatch	aws:cloudwatch	Represents performance and billing metrics from the AWS CloudWatch service.	CloudWatch	• CIM: Performance, Databases • ES Custom: None • ITSI: Virtualization
CloudWatch Logs	aws:cloudwatchlogs aws:cloudwatchlogs:vpcflow	`aws:cloudwatchlogs` represents generic data from the CloudWatch Logs service. `aws:cloudwatchlogs:vpcflow` represents VPC flow logs from the CloudWatch Logs service.	Kinesis CloudWatch Logs	• CIM: Network Traffic, but only for `aws:cloudwatchlogs:vpcflow` • ES Custom: None • ITSI: None
Config	aws:config aws:config:notification	`aws:config` represents real time and historical configuration snapshots. `aws:config:notification` represents configuration change notifications.	SQS-based S3 AWS Config	• CIM: Change Analysis • ES Custom: None • ITSI: None
Config Rules	aws:config:rule	Represents compliance details, compliance summary, and evaluation status of your AWS Config Rules.	Config Rules	• CIM: Inventory • ES Custom: None • ITSI: None
Description	aws:description	Descriptions of your AWS EC2 instances, reserved instances, and EBS snapshots.	Description	• CIM: None • ES Custom: Assets and Identities • ITSI: Virtualization
ELB Access Logs	aws:elb:accesslogs	Represents ELB Access Logs.	SQS-based S3 Generic S3 Incremental S3	• CIM: None • ES Custom: None • ITSI: None
Inspector	aws:inspector	Represents assessments, runs, and findings data from the Amazon Inspector service.	Inspector	• CIM: Inventory, Alerts • ES Custom: None • ITSI: None

Data type	Source type	Description	Supported input types	Data models
S3	aws:s3	Represents generic log data from your S3 buckets.	Generic S3 Incremental S3 SQS-based S3	• CIM: None • ES Custom: None • ITSI: None
S3 Access Logs	aws:s3:accesslogs	Represents S3 Access Logs.	SQS-based S3 Generic S3 Incremental S3	• CIM: Web • ES Custom: None • ITSI: None
SQS	aws:sqs	Represents generic data from SQS.	SQS	• CIM: None • ES Custom: None • ITSI: None

Hardware and software requirements for the Splunk Add-on for AWS

To install and configure the Splunk Add-on for Amazon Web Services (AWS), you must have admin or sc_admin role permissions.

AWS account prerequisites

To set up your AWS configuration to work with your Splunk platform instance, make sure you have the following AWS account privileges:

- A valid AWS account with permissions to configure the AWS services that provide your data.
- Permission to create Identity and Access Management (IAM) roles and users. This lets you set up AWS account IAM roles or Amazon Elastic Compute Cloud (EC2) IAM roles to collect data from your AWS services.

When configuring your AWS account to send data to your Splunk platform deployment, the best practice is that you should not allow "*" (all resource) statements as part of action elements. This level of access could potentially grant unwanted and unregulated access to anyone given this policy document setting. The best practice is to write a refined policy describing the specific action allowed by specific users or specific accounts, or required by the specific policy holder. For more information, see the Basic examples of Amazon SQS policies topic in the Amazon Simple Queue Service Developer Guide.

AWS region limitations

The Splunk Add-on for AWS supports all services offered by AWS in each region. To learn which worldwide geographic regions support which AWS services, see the Region Table in the AWS global infrastructure documentation.

In the AWS China region, the add-on supports only the services that AWS supports in that region. For an up-to-date list of what products and services are supported in this region, see https://www.amazonaws.cn/en/products/.

For an up-to-date list of what services and endpoints are supported in AWS GovCloud region, see https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-services.html.

Network configuration requirements

The Splunk Add-on for AWS makes REST API calls using HTTPS on port 443. Data inputs for this add-on use large amounts of memory. See Sizing, performance, and cost considerations for the Splunk Add-on for AWS for more information.

AWS encryption requirements

Amazon Web Services supports the following server-side encryption types:

- Server-side encryption with Amazon S3-managed encryption keys (SSE-S3). For SSE-S3 configurations, the unique key is used for encrypting each object)
- Server-side encryption with AWS Key Management Service (SSE-KMS). SSE-KMS will manage encryption. AWS will manage the master key.
- Server-side encryption with customer-provided encryption keys (SSE-C). KMS service will manage encryption/ The client needs to provide a custom master key.

The Splunk Add-on for AWS supports all server-side encryptions. Client-side encryption is not supported. Server side encryption is handled by AWS. AWS SDK for Python does not support client-side encryption.

Splunk platform requirements

There are no Splunk platform requirements specific to the Splunk Add-on for AWS.

For Splunk Enterprise system requirements, see System requirements for use of Splunk Enterprise on-premises in the Splunk Enterprise *Installation Manual*.

For information about installation locations and environments, see Install the Splunk Add-on for AWS.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

Sizing, performance, and cost considerations for the Splunk Add-on for AWS

Before you configure the Splunk Add-on for Amazon Web Services (AWS), review these sizing, performance, and cost considerations.

General

See the following table for the recommended maximum daily indexing volume on a clustered indexer for different AWS source types. This information is based on a generic Splunk hardware configuration. Adjust the number of indexers in your cluster based on your actual system performance. Add indexers to a cluster to improve indexing and search retrieval performance. Remove indexers to a cluster to avoid within-cluster data replication traffic.

Source type	Daily indexing volume per indexer (GB)
aws:cloudwatchlogs:vpcflow	25-30

Source type	Daily indexing volume per indexer (GB)
aws:s3:accesslogs	80- 20
aws:cloudtrail	150-200
aws:billing	50- 00

These sizing recommendations are based on the Splunk platform hardware configurations in the following table. You can also use the System requirements for use of Splunk Enterprise on-premises in the *Splunk Enterprise Installation Manual* as a reference.

Splunk platform type	CPU cores	RAM	EC2 instance type
Search head	8	16 GB	c4.xlarge
Indexer	16	64 GB	m4.4xlarge

Input configuration screens require data transfer from AWS to populate the services, queues, and buckets available to your accounts. If your network to AWS is slow, data transfer might be slow load. If you encounter timeout issues, you can manually type in resource names.

Performance for the Splunk Add-on for AWS data inputs

The rate of data ingestion for this add-on depends on several factors: deployment topology, number of keys in a bucket, file size, file compression format, number of events in a file, event size, and hardware and networking conditions.

See the following tables for measured throughput data achieved under certain operating conditions. Use the information to optimize the Splunk Add-on for AWS add-on in your own production environment. Because performance varies based on user characteristics, application usage, server configurations, and other factors, specific performance results cannot be guaranteed. Contact Splunk Support for accurate performance tuning and sizing.

The Kinesis input for the Splunk Add-on for AWS has its own performance data. See Configure Kinesis inputs for the Splunk Add-on for AWS.

Reference hardware and software environment

Throughput data and conclusions are based on performance testing using Splunk platform instances (dedicated heavy forwarders and indexers) running on the following environment:

Instance type	M4 Double Extra Large (m4.4xlarge)
Memory	64 GB
Compute Units (ECU)	53.5
vCPU	16
Storage (GB)	0 (EBS only)
Arch	64-bit
EBS optimized (max bandwidth)	2000 Mbps
Network performance	High

The following settings are configured in the outputs.conf file on the heavy forwarder:

```
useACK = true
```

```
maxQueueSize = 15MB
```

Measured performance data

The throughput data is the maximum performance for each single input achieved in performance testing under specific operating conditions and is subject to change when any of the hardware and software variables changes. Use this data as a rough reference only.

Single-input max throughput

Data input	Source type	Max throughput (KBs)	Max EPS (events)	Max throughput (GB/day)
Generic S3	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	17,000	86,000	1,470
Generic S3	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	11,000	35,000	950
Incremental S3	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	11,000	43,000	950
Incremental S3	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	7,000	10,000	600
SQS-based S3	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	12,000	50,000	1,000
SQS-based S3	aws:elb:accesslogs (gz, syslog, event size 250 B, S3 key size 2 MB)	24,000	100,000	2,000
SQS-based S3	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	13,000	19,000	1,100
CloudWatch logs [1]	aws:cloudwatchlog:vpcflow	1,000	6,700	100
CloudWatch (ListMetric, 10,000 metrics)	aws:cloudwatch	240 (Metrics)	NA	NA
CloudTrail	aws:cloudtrail (gz, json, sqs=1,000, 9,000 events/key)	5,000	7,000	400
Kinesis	aws:cloudwatchlog:vpcflow (json, 10 shards)	15,000	125,000	1,200
SQS	aws:sqs (json, event size 2,800)	N/A	160	N/A

[1] API throttling error occurs if input streams are greater than 1,000.

Multi-inputs max throughput

The following throughput data was measured with multiple inputs configured on a heavy forwarder in an indexer cluster distributed environment.

Consolidate AWS accounts during add-on configuration to reduce CPU usage and increase throughput performance.

Data input	Source type	Max throughput (KBs)	Max EPS (events)	Max throughput (GB/day)
Generic S3	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	23,000	108,000	1,980
Generic S3	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	45,000	130,000	3,880
Incremental S3	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	34,000	140,000	2,930
Incremental S3	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	45,000	65,000	3,880
SQS-based S3 [1]	aws:elb:accesslogs (plain text, syslog, event size 250 B, S3 key size 2 MB)	35,000	144,000	3,000
SQS-based S3 [1]	aws:elb:accesslogs (gz, syslog, event size 250 B, S3 key size 2 MB)	42,000	190,000	3,600
SQS-based S3 [1]	aws:cloudtrail (gz, json, event size 720 B, S3 key size 2 MB)	45,000	68,000	3,900
CloudWatch logs	aws:cloudwatchlog:vpcflow	1,000	6,700	100
CloudWatch (ListMetric)	aws:cloudwatch (10,000 metrics)	240 (metrics/s)	NA	NA
CloudTrail	aws:cloudtrail (gz, json, sqs=100, 9,000 events/key)	20,000	15,000	1,700
Kinesis	aws:cloudwatchlog:vpcflow (json, 10 shards)	18,000	154,000	1,500
SQS	aws:sqs (json, event size 2.8K)	N/A	670	N/A

[1] Performance testing of the SQS-based S3 input indicates that optimal performance throughput is reached when running four inputs on a single heavy forwarder instance. To achieve higher throughput performance beyond this bottleneck, you can further scale out data collection by creating multiple heavy forwarder instances each configured with up to four SQS-based S3 inputs to concurrently ingest data by consuming messages from the same SQS queue.

Max inputs benchmark per heavy forwarder

The following input number ceiling was measured with multiple inputs configured on a heavy forwarder in an indexer cluster distributed environment. CPU and memory resources were utilized to their fullest.

It is possible to configure more inputs than the maximum number indicated in the table if you have a smaller event size, fewer keys per bucket, or more available CPU and memory resources in your environment.

Data input	Sourcetype	Format	Number of keys/bucket	Event size	Max inputs
S3	aws:s3	zip, syslog	100,000	100 B	300
S3	aws:cloudtrail	gz, json	1,300,000	1 KB	30

Data input	Sourcetype	Format	Number of keys/bucket	Event size	Max inputs
Incremental S3	aws:cloudtrail	gz, json	1,300,000	1 KB	20
SQS-based S3	aws:cloudtrail, aws:config	gz, json	1,000,000	1 KB	50

Memory usage benchmark for generic S3 inputs

Event size	Number of events per key	Total number of keys	Archive type	Number of inputs	Memory used
1,000	1,000	10,000	zip	20	20 G
1,000	1,000	1,000	zip	20	12 G
1,000	1,000	10,000	zip	10	18 G
100 B	1,000	10,000	zip	10	15 G

If you do not achieve the expected AWS data ingestion throughput, see Troubleshoot the Splunk Add-on for AWS.

CloudTrail

The following table provides general guidance on sizing, performance, and cost considerations for the CloudTrail data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	Using CloudTrail itself does not incur charges, but standard S3, SNS, and SQS charges apply. See https://aws.amazon.com/pricing/services/.

Config

The following table provides general guidance on sizing, performance, and cost considerations for the Config data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	Using Config incurs charges from AWS. See http://aws.amazon.com/config/pricing/. In addition, standard S3, SNS, and SQS charges apply. See http://aws.amazon.com/pricing/services/.

Config Rules

The following table provides general guidance on sizing, performance, and cost considerations for the Config Rules data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	None.

CloudWatch

The following table provides general guidance on sizing, performance, and cost considerations for the CloudWatch data input:

Consideration	Notes
Sizing and performance	The smaller the granularity you configure, the more events you collect. Create separate inputs that match your needs for different regions, services, and metrics. For each input, configure a granularity that matches the precision that you require, setting a larger granularity value in cases where indexing fewer, less-granular events is acceptable. You can increase granularity temporarily when a problem is detected. AWS rate-limits the number of free API calls against the CloudWatch API. With a period of 300 and a polling interval of 1,800, collecting data for 2 million metrics does not, by itself, exceed the current default rate limit, but collecting 4 million metrics does exceed it. If you have millions of metrics to collect in your environment, consider paying to have your API limit raised, or remove less essential metrics from your input and configure larger granularities in order to make fewer API calls.
AWS cost	Using CloudWatch and making requests against the CloudWatch API incurs charges from AWS. See https://aws.amazon.com/cloudwatch/pricing/.

CloudWatch Logs (VPC Flow Logs)

The following table provides general guidance on sizing, performance, and cost considerations for the CloudWatch Logs (VPC Flow Logs) data input:

Consideration	Notes
Sizing and performance	AWS limits each account to 10 requests per second, each of which returns no more than 1 MB of data. In other words, the data ingestion and indexing rate is no more than 10 MB/s. The add-on modular input can process up to 4,000 events per second in a single log stream. Best practices: • If volume is a concern, configure the `only_after` parameter to limit the amount of historical data you collect. • If you have high volume VPC Flow Logs, configure one or more Kinesis inputs to collect them instead of using the CloudWatch Logs input.
AWS cost	Using CloudWatch Logs incurs charges from AWS. See https://aws.amazon.com/cloudwatch/pricing/. Transferring data out of CloudWatch Logs incurs charges from AWS. See https://aws.amazon.com/ec2/pricing/.

Inspector

The following table provides general guidance on sizing, performance, and cost considerations for the Inspector data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	Using Amazon Inspector incurs charges from AWS. See https://aws.amazon.com/inspector/pricing/.

Kinesis

The following table provides general guidance on sizing, performance, and cost considerations for the Kinesis data input:

Consideration	Notes
Sizing and performance	See Performance reference for the Kinesis input in the Splunk Add-on for AWS.
AWS cost	Using Amazon Kinesis incurs charges from AWS. See https://aws.amazon.com/kinesis/streams/pricing/.

S3

The following table provides general guidance on sizing, performance, and cost considerations for the S3 data input:

Consideration	Notes
Sizing and performance	AWS throttles S3 data collection at the bucket level, so expect some delay before all data arrives in your Splunk platform. You can configure multiple S3 inputs for a single S3 bucket to improve performance. The Splunk platform dedicates one process for each data input, so provided that your system has sufficient processing power, performance improves with multiple inputs. See Performance reference for the S3 input in the Splunk Add-on for AWS.
AWS cost	Using S3 incurs charges from AWS. See https://aws.amazon.com/s3/pricing/.

Billing

The following table provides general guidance on sizing, performance, and cost considerations for the Billing data input:

Consideration	Notes
Sizing and performance	Detailed billing reports can be very large in size, depending on your environment. If you configure the add-on to collect detailed reports, it collects all historical reports available in the bucket by default. In addition, for each newly finalized monthly and detailed report, the add-on collects new copies of the same report once per interval until the etag is unchanged. Configure separate inputs for each billing report type that you want to collect. Use the regex and interval parameters in the input configuration page of the add-on to limit the number of reports that you collect with each input.
AWS cost	Billing reports themselves do not incur charges, but standard S3 charges apply. See https://aws.amazon.com/s3/pricing/.

SQS

The following table provides general guidance on sizing, performance, and cost considerations for the SQS data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	Using SQS incurs charges from AWS. See https://aws.amazon.com/sqs/pricing/.

SNS

The following table provides general guidance on sizing, performance, and cost considerations for the SNS data input:

Consideration	Notes
Sizing and performance	None.
AWS cost	Using SNS incurs charges from AWS. See https://aws.amazon.com/sns/pricing/.

Deploy the Splunk Add-on for AWS

Complete the following steps to configure the Splunk Add-on for AWS:

1. Install the Splunk Add-on for AWS.
2. Manage accounts for the Splunk Add-on for AWS.
3. Find your particular input(s) from the *Input Configuration Details* section:
    1. Configure Billing inputs for the Splunk Add-on for AWS
    2. Configure Cost and Usage Report inputs for the Splunk Add-on for AWS

3. Configure CloudTrail inputs for the Splunk Add-on for AWS
4. Configure CloudWatch inputs for the Splunk Add-on for AWS
5. Configure CloudWatch Log inputs for the Splunk Add-on for AWS
6. Configure Config inputs for the Splunk Add-on for AWS
7. Configure Config Rules inputs for the Splunk Add-on for AWS
8. Configure Description inputs for the Splunk Add-on for AWS
9. Configure Generic S3 inputs for the Splunk Add-on for AWS
10. Configure Incremental S3 inputs for the Splunk Add-on for AWS
11. Configure Inspector inputs for the Splunk Add-on for AWS
12. Configure Kinesis inputs for the Splunk Add-on for AWS
13. Configure SQS inputs for the Splunk Add-on for AWS
14. Configure SQS-based S3 inputs for the Splunk Add-on for AWS
15. Configure miscellaneous inputs for the Splunk Add-on for AWS

Deployment

Installation overview for the Splunk Add-on for AWS

1. Download the Splunk Add-on for AWS from Splunkbase or Splunk Web.
2. Use the tables in this topic to determine where to install this add-on.
3. Perform any prerequisite steps specified in the tables before installing.
4. Use the links in the Installation walkthrough section to perform the installation.

Distributed deployments

Use the following tables to install the Splunk Add-on for AWS in a deployment that uses forwarders to get data in, such as a distributed deployment. You might need to install the add-on in multiple places.

Where to install this add-on

Unless otherwise noted, you can safely install all supported add-ons to all tiers of a distributed Splunk platform deployment. See Where to install Splunk add-ons in *Splunk Add-ons* for more information.

This table provides a reference for installing this specific add-on to a distributed deployment of the Splunk platform:

Splunk platform component	Supported	Required	Comments
Search heads	Yes	No	Data inputs for this add-on require large amounts of memory. See Hardware and software requirements for the Splunk Add-on for AWS.
Indexers	Yes	No	Not required as the parsing operations occur on the heavy forwarders.
Heavy forwarders	Yes	Yes	This add-on requires heavy forwarders to perform data collection through modular inputs and to perform the setup and authentication with AWS in Splunk Web.
Universal forwarders	No	No	This add-on requires heavy forwarders.

Distributed deployment compatibility

This table provides a quick reference for the compatibility of this add-on with Splunk distributed deployment features:

Distributed deployment feature	Supported	Comments
Search head clusters	Yes	You can install this add-on on a search head cluster for all search-time functionality, but configure inputs on forwarders to avoid duplicate data collection. Before installing this add-on to a cluster, make the following changes to the add-on package: #Remove the eventgen.conf files and all files in the samples folder. 1. Remove the inputs.conf file.
Indexer clusters	Yes	Before installing this add-on to a cluster, make the following changes to the add-on package: 1. Remove the eventgen.conf files and all files in the samples folder. 2. Remove the inputs.conf file.
Deployment server	No	Deployment servers support deploying unconfigured add-ons only.

Distributed deployment feature	Supported	Comments
		• Using a deployment server to deploy the configured add-on to multiple forwarders acting as data collectors causes duplication of data. • The add-on uses the credential vault to secure your credentials, and this credential management solution is incompatible with the deployment server.

Installation walkthroughs

See the following links, or About installing Splunk add-ons in the *Splunk Add-Ons* manual, for an installation walkthrough specific to your deployment scenario:

- Install the Splunk Add-on for AWS in a Splunk Cloud deployment
- Install the Splunk Add-on for AWS in a single-instance Splunk Enterprise deployment
- Install the Splunk Add-on for AWS in a distributed Splunk Enterprise deployment

Install the Splunk Add-on for AWS in a Splunk Cloud Deployment

Install the Splunk Add-on for Amazon Web Services (AWS) to your free trial instance of Splunk Cloud using the app browser in Splunk Cloud:

1. From the Splunk Web home screen, click on the gear icon next to **Apps** in the navigation bar.
2. Click **Browse more apps**.
3. Find the Splunk Add-on for AWS, then click **Install**.
4. Follow the on-screen prompts to complete your installation.
5. Install the Splunk Add-on for AWS to an Inputs Data Manager. Request that Splunk Cloud Support installs the Splunk add-on for AWS on your Splunk Cloud instance.

Install the Splunk Add-on for AWS in a single-instance Splunk Enterprise deployment

Follow these steps to install the Splunk add-on for Amazon Web Services (AWS) in a single-instance deployment:

1. From the Splunk Web home screen, click the gear icon next to **Apps** in the navigation bar.
2. Click **Install app from file**.
3. Locate the downloaded file and click **Upload**.
4. If Splunk Enterprise prompts you to restart, do so.
5. Verify that the add-on appears in the list of apps and add-ons. You can also find it on the server at `$SPLUNK_HOME/etc/apps/Splunk_TA_AWS`.

Install the Splunk Add-on for AWS in a distributed Splunk Enterprise deployment

If you are using a distributed Splunk Enterprise deployment, follow the instructions in each of the following sections to deploy the Splunk Add-on for Amazon Web Services (AWS) to your search heads, indexers, and forwarders. You must install Splunk add-on for AWS on a heavy forwarder. You cannot use this add-on with a universal forwarder. You can install this add-on onto search heads and indexers.

Heavy forwarders

To install the Splunk Add-on for AWS to a heavy forwarder, follow these steps:

1. Download the Splunk Add-on for AWS from Splunkbase, if you have not already done so.
2. From the Splunk Web home screen on your heavy forwarder, click the gear icon next to **Apps**.
3. Click **Install app from file**.
4. Locate the downloaded file and click **Upload**.
5. If the forwarder prompts you to restart, do so.
6. Verify that the add-on appears in the list of apps and add-ons. You can also find it on the server at `$SPLUNK_HOME/etc/apps/Splunk_TA_AWS`.

Search heads

To install the Splunk Add-on for AWS to a search head, follow these steps:

1. Download the Splunk Add-on for AWS from Splunkbase, if you have not already done so.
2. From the Splunk Web home screen, click the gear icon next to **Apps**.
3. Click **Install app from file**.
4. Locate the downloaded file and click **Upload**.
5. If Splunk Enterprise prompts you to restart, do so.
6. Verify that the add-on appears in the list of apps and add-ons.

Make sure the add-on is not visible. If the Visible column for the add-on is set to "'Yes'", edit the properties and change the visibility to "'No.'" Disable visibility of add-ons on search heads to avoid inputs from being created on search heads. Data collection for search heads might conflict with users' search activity.

You can also find the add-on on the server at `$SPLUNK_HOME/etc/apps/Splunk_TA_AWS`.

Search head clusters

Before deploying the Splunk Add-on for AWS to a search head cluster, make the following changes to the add-on package:

1. Remove the eventgen.conf files and all files in the samples folder.
2. Remove the inputs.conf and inputs.conf.spec files. If you are collecting data locally from the machines running your search head nodes, keep these files.
3. Use the deployer to deploy an add-on to the search head cluster members.

See Use the deployer to distribute apps and configuration updates in the Splunk Enterprise *Distributed Search* manual.

Indexers

To install the Splunk Add-on for AWS to an indexer, follow these steps:

1. Download the Splunk Add-on for AWS from Splunkbase, if you have not already done so.
2. Unpack the .tgz package.
3. Place the resulting `Splunk_TA_AWS` folder in the `$SPLUNK_HOME/etc/apps` directory on your indexer.
4. Restart the indexer.

Indexer clusters

1. Remove the eventgen.conf files and all files in the samples folder.
2. Remove the inputs.conf and inputs.conf.spec files. If you are collecting data locally from the machines running your indexer nodes, keep these files.
3. Deploy add-ons to peer nodes on indexer clusters using a master node.

For more information about using a master node to deploy to peer nodes of an indexer cluster, see Manage app deployment across all peers in *Managing Indexers and Clusters of Indexers*.

Upgrade the Splunk Add-on for AWS

Upgrade to the latest version of the Splunk Add-on for Amazon Web Services (AWS). Upgrades to version 5.2.0 are possible only from version 5.0.3 or higher. For upgrading the Splunk Add-on for AWS on Splunk Cloud deployments, contact your Splunk Cloud administrator.

Starting in version 5.0.1 of the Splunk Add-on for AWS, Python 2 support is removed, and only Python 3 is supported.

1. Verify that you are running version 8.0.0 or later of the Splunk platform.
2. (Optional) Plan your Splunk Enterprise upgrade to work with the Python 3 migration.
3. Disable all running inputs.
4. Delete the pycache directory found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/pycache`.
5. Upgrade to version 5.0.3 of the Splunk Add-on for AWS, if you have not done so already.
6. Download version 5.2.0 of the Splunk Add-on for AWS from Splunkbase.
7. Install the latest version of the Splunk Add-on for AWS.
8. Restart your Splunk platform deployment.
9. Visit http://<url or host_ip>:<web_port>/<locale_string>/_bump and click on the "Bump Version" button to apply upgraded JS file changes. See Localization Files for more information on <locale_string>.
10. Click the **Bump Version** button to apply the upgraded `.js` file changes.
11. Enable all inputs.

Manage accounts for the Splunk Add-on for AWS

The Splunk Add-on for Amazon Web Services (AWS) can only access the data in your AWS account if your account has an IAM AWS Identity Account Management (IAM) role. Read the following sections to do the following:

1. Create an IAM role and assign it to your AWS account.
2. Find an IAM role within your Splunk platform instance.

Before you can configure Splunk Cloud or Splunk Enterprise to work with your AWS data, you must set up accounts in Amazon Web Services.

Create an IAM role and assign it to your AWS account

To configure AWS accounts and permissions, you must have administrator rights in the AWS Management Console. If you do not have administrator access, work with your AWS admin to set up the accounts with the required permissions.

- To let the Splunk Add-on for Amazon Web Services access the data in your AWS account, you assign an IAM role to one or more AWS accounts. You then grant those roles the permissions that are required by the AWS account.
- If you run this add-on on a Splunk platform instance in your own managed Amazon Elastic Compute Cloud (EC2), then assign that EC2 to a role and give that role the IAM permissions listed here.

Manage IAM policies

There are three ways to manage policies for your IAM roles:

- Use the AWS Policy Generator tool to collect all permissions into one centrally managed policy. You can apply the policy to the IAM group that is used by the user accounts or the EC2s that the Splunk Add-on for AWS uses to connect to your AWS environment.
- Create multiple different users, groups, and roles with permissions specific to the services from which you plan to collect data.
- Copy and paste the sample policies provided on this page and apply them to an IAM Group as custom inline policies. To further specify the resources to which the policy grants access, replace the wildcards with the exact Amazon Resource Names (ARNs) of the resources in your environment.

For more information about working with inline policies, see Managing IAM Policies in the AWS documentation.

Create and configure roles to delegate permissions to IAM users

The Splunk Add-on for AWS supports the AWS Security Token Service (AWS STS)Â AssumeRoleÂ API action that lets you use IAM roles to delegate permissions to IAM users to access AWS resources.

The AssumeRole API returns a set of temporary security credentials consisting of an access key ID, a secret access key, and a security token that an AWS account can use to access AWS resources that it might not normally have access to.Â

To assume a role, your AWS account must be trusted by the role. The trust relationship is defined in the role's trust policy when the role is created. That trust policy states which user accounts are allowed to delegate access to this account's role.

The user who wants to access the role must also have permissions delegated from the role's administrator. If the user is in a different account than the role, then the user's administrator must attach a policy that allows the user to call AssumeRole on the ARN of the role in the other account. If the user is in the same account as the role, then you can either attach a policy to the user identical to the previous different account user, or you can add the user as a principal directly in the role's trust policy.

To create an IAM role, see Creating a Role to Delegate Permissions to an IAM User in the AWS documentation.

After creating the role, use the AWS Management Console to modify the trust relationship to allow the IAM user to assume the newly created role. The following example shows a trust relationship that allows a role to be assumed by an IAM user namedÂ johndoe:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": "arn:aws:iam::123456789012:user/johndoe"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Next, grant your IAM user permission to assume the role. The following example shows an AWS IAM policy that allows an IAM user to assume the s3admin role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::123456789012:role/s3admin"
    }
  ]
}
```

Find an IAM role within your Splunk platform instance

Collecting data using an auto-discovered EC2 IAM role is not supported in the AWS China region.

1. Follow IAM roles for Amazon EC2 in the AWS documentation to set up an IAM role for your EC2.
2. Ensure that this role has adequate permissions. If you do not give this role all of the permissions required for all inputs, configure AWS accounts specific to inputs not covered by the permissions for this role.
3. On the Splunk Web home page, click **Splunk Add-on for AWS** in the left navigation bar.
4. Click **Configuration** in the app navigation bar. By default, the add-on displays the Account tab.
5. Look for the EC2 IAM role in the **Autodiscovered IAM Role** column. If you are in your own managed AWS environment and have an EC2 IAM role configured, it appears in this account list automatically.

You can also configure AWS accounts if you want to use both EC2 IAM roles and user accounts to ingest your AWS data.

You cannot edit or delete EC2 IAM roles from the add-on.

Add and manage AWS accounts

Perform the following steps to add an AWS account:

1. In the Splunk Web home page, click **Splunk Add-on for AWS** in the left navigation bar.
2. Click **Configuration** in the app navigation bar. The add-on displays the Account tab.
3. Click **Add**.
4. Name the AWS account. You cannot change this name once you configure the account.
5. Enter the **Key ID** and **Secret Key** credentials for the AWS account that the Splunk platform uses to access your AWS data. The accounts that you configure must have the necessary permissions to access the AWS data that you want to collect.
6. Select the **Region Category** for the account. The most common category is **Global**.
7. Click **Add**.

Edit existing accounts by clicking **Edit** in the Actions column.

Delete an existing account by clicking **Delete** in the Actions column. You cannot delete accounts that are associated with any inputs, even if those inputs are disabled. To delete an account, delete the inputs or edit them to use a different account and then delete the account.

To use custom commands and alert actions, you must set up at least one AWS account on your Splunk platform deployment search head or search head cluster.

Add and manage private AWS accounts

Private account configurations are for users who want to use regional/private endpoints for account validation.

Perform the following steps to add a private AWS account:

1. In the Splunk Web home page, click **Splunk Add-on for AWS** in the left navigation bar.
2. Click **Configuration** in the app navigation bar. The add-on displays the Account tab.
3. Click the **Private Account** tab.
4. Click **Add**.
5. Name the AWS private account. You cannot change this name once you configure the account.
6. Enter the **Key ID** and **Secret Key** credentials for the AWS account that the Splunk platform uses to access your AWS data. The accounts that you configure must have the necessary permissions to access the AWS data that you want to collect.
7. Select the **Region Category** for the private account. The most common category is **Global**.
8. Select the **Region** which will be used for regional endpoints to authenticate account credentials.
9. (Optional) To use private endpoints for account validation, click the **Use Private Endpoints** checkbox and enter the private endpoint URL of your AWS Security Token Service (**STS**). This step is only required if you have specific requirements for your private endpoints.
10. Click **Add**.

Edit existing private accounts by clicking **Edit** in the **Actions** column of the **Private Account** tab.

Delete an existing private account by clicking **Delete** in the **Actions** column. You cannot delete private accounts that are associated with any inputs, even if those inputs are disabled. To delete a private account, delete the inputs or edit them to use a different account or private account and then delete the private account.

Add and manage IAM roles

Use the Configuration menu in the Splunk Add-on for AWS to manage AWS IAM roles that can be assumed by IAM users. Adding IAM roles lets the Splunk Add-on for AWS access the following AWS resources:

- Generic S3
- Incremental S3
- SQS-based S3
- Billing
- Description
- Metadata
- CloudWatch
- Kinesis

Add an IAM role

Use the following steps to add an IAM role:

1. On the Splunk Web home page, click **Splunk Add-on for AWS** in the left navigation bar.
2. Click **Configuration** in the app navigation bar, and then click the **IAM Role** tab.
3. Click **Add**.
4. In the **Name** field, name the role to be assumed by authorized AWS accounts managed on the Splunk platform. You cannot change the name once you configure the role.
5. In the ARN field, enter the role's Amazon Resource Name in the valid format: `arn:aws:iam::<aws_resource_id>:role/<role_name>`.
6. Click **Add**.

Click **Edit** in the Actions column to edit existing IAM roles.

Click **Delete** in the Actions column to delete an existing role. You cannot delete roles associated with any inputs, even if those inputs are disabled. To delete an account, delete the inputs or edit them to use a different assumed role and then delete the role.

Configure a proxy connection

1. On the Splunk Web home page, click **Splunk Add-on for AWS** in the left navigation bar.
2. Click **Configuration** in the app navigation bar.
3. Click the **Proxy** tab.
4. Select the **Enable** box to enable the proxy connection and fill in the fields required for your proxy.
5. Click **Save**.

To disable your proxy but save your configuration, uncheck the **Enable** box. The add-on stores your proxy configuration so that you can enable it later.

To delete your proxy configuration, delete the values in the fields.

Input configuration

Configure Billing inputs for the Splunk Add-on for AWS

Complete the steps to configure Billing inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Billing input.
3. Configure AWS permissions for the Billing input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Billing inputs either through Splunk Web or configuration files.

If you want to collect both a Monthly report and a Detailed report, configure two billing inputs: one for the Monthly report and another for the Detailed report. This way, you can configure the interval and the report_file_match_regex values for a specific report type rather than having the values you enter there apply to both report types.

After you configure your Billing inputs, see Access billing data for the Splunk Add-on for AWS for more information about data collection behavior and how to access the preconfigured reports included in the add-on.

Configure AWS services for the Billing input

The Splunk Add-on for AWS collects Billing Metrics through CloudWatch and Billing Reports by collecting them from an S3 bucket.

To enable AWS to produce Billing Metrics in CloudWatch, turn on **Receive Billing Alerts** in the Preferences section of the Billing and Cost Management console.

To enable Billing Reports, turn on **Receive Billing Reports** in the Preferences section of the Billing and Cost Management console. Verify your S3 bucket in the Billing and Cost Management console and select the report types that you want to collect.

For more details on managing your AWS Billing Reports, see https://docs.aws.amazon.com/cur/latest/userguide/detailed-billing.html.

Configure AWS permissions for the Billing input

You need these required permissions for the S3 bucket to collect your Billing Reports:

- `Get*`
- `List*`

In the Resource section of the policy, specify the Amazon Resource Names (ARNs) of the S3 buckets that contain billing reports for your accounts. ListAllMyBuckets is required when you use an asterisk (*) character.

See the following sample inline policy to configure Billing input permissions:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": ""arn:aws:s3:::<your bucket name>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-permissions-ref.html.

Configure a Billing input using Splunk Web

To configure inputs using Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > Billing**.
3. Fill out the fields as described in the following table:

Argument in configuration file	Field in Splunk Web	Description
AWS input configuration		
`aws_account`	AWS account	The AWS account or EC2 IAM role the Splunk platform uses to access your Billing data. In Splunk Web, select a drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts that you configured on the Co name of the automatically discovered EC2 IAM role.
`aws_iam_role`	Assume Role	The IAM role to assume, see "Add and manage IAM roles" in the Manage accounts for the Splunk Add-on for AW
`aws_s3_region`	AWS Region (Optional)	The AWS region that contains your bucket. In inputs.conf, enter the region ID. Provide an AWS Region only if you want to use specific regional endpoints instead of public e collection. See the **AWS service endpoints** topic in the AWS General Reference manual for more infor
`bucket_name`	S3 Bucket	The S3 bucket that is configured to hold billing reports.
`monthly_report_type`	Monthly report	The monthly report type that the Splunk platform collects from your AWS account. Enter one of the following valu • None • Monthly report • Monthly cost allocation report
`detail_report_type`		The detailed report type that the Splunk platform collects from your AWS account. Enter one of the following valu

Argument in configuration file	Field in Splunk Web	Description
	Detailed report	• None • Detailed billing report • Detailed billing report with resource and tags
Splunk-related configuration		
`initial_scan_datetime`	Start Date/Time (UTC)	This add-on starts to collect data later than this time. If you leave this field empty, the default value is 90 days be **Note:** Once the input is created, you cannot change this value.
`sourcetype`	Source type	A source type for the events. Specify a value if you want to override the default of `aws:billing`. Event extracti value of source type. If you change the default value, you must update props.conf as well.
`index`	Index	The index name where the Splunk platform puts the billing data. The default is main.
Advanced settings		
`interval`	Interval	Enter the number of seconds to wait before the Splunk platform runs the command again, or enter a valid cron s 86400 seconds (one day). This interval applies differently for Monthly report types and Detailed report types. For interval indicates how often to run the data collection for the current month's monthly report and how often to che monthly report's etag to determine if changes were made. If the etag does not match an already-downloaded ve it downloads that report to get the latest data. For Detailed report types, the interval indicates how often to check detailed report etag to determine if changes were made. If the etag does not match a report already downloaded get the latest data. The present month is never collected until the month has ended. Because AWS Billing Reports are usually not finalized until several days after the last day of the month, you can `0 8-31 * *` to skip data collection for the first seven days of every month to avoid collecting multiple copies of the just-finished month.
`report_file_match_reg`	Regex for report selection	A regular expression that the Splunk platform uses to match reports in AWS. This expression overrides values in `monthly_report_type` and `detail_report_type` arguments. If you want to collect both Monthly and Deta want to use regex to specify the report collection period, configure two separate billing inputs so that the regex y to one of the report types that you want to collect. Use this regex to limit the report collection to a certain time period to avoid collecting data that you do not need. important for the first time that you enable the input. By default, the add-on collects all available reports for all pr collect Detailed reports, which are large in size, the add-on results in collecting a very large amount of data. You many months of past data that you collect. For example, you can use the expression `\d+-aws-billing-detailed-line-items-201[56789]-\d+.csv.zip` to collect only Detailed reports fr or the expression `\d+-aws-billing-detailed-line-items-with-resources-and-tags-2015-((0[4-9])|(10)|(1` `-aws-billing-detailed-line-items-with-resources-and-tags-201[6789]-\d+.csv.zip)` to c billing reports with resources and tags for April 2015 and later.
`temp_folder`	Temp Folder	Full path to a non-default folder with sufficient space for temporarily storing downloaded detailed billing report .zi the estimated size of uncompressed detailed billing report files, which can be much larger than that of zipped file temp folder, the add-on will use the system temp folder by default.

Configure a Billing input using a configuration file

To configure inputs in inputs.conf, create a stanza using the following template and add it to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf`. If the file or path does not exist, create it.

```
[aws_billing://<name>]
aws_account = <value>
aws_iam_role=<value>
aws_s3_region = <value>
interval = <value>
initial_scan_datetime = <value>
```

```
bucket_name = <value>
detail_report_type = <value>
monthly_report_type = <value>
report_file_match_reg = <value>
sourcetype = <value>
index = <value>
host_name = s3.amazonaws.com
```

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_billing]
bucket_name =
aws_account =
monthly_report_type = Monthly cost allocation report
detail_report_type = Detailed billing report with resources and tags
report_file_match_reg =
interval = 86400
sourcetype = aws:billing
host_name = s3.amazonaws.com
```

The previous values correspond to the default values in Splunk Web. If you choose to copy this stanza to the `/local` directory and use it as a starting point to configure your inputs.conf manually, change the stanza title from `aws_billing` to `aws_billing://<name>`.

Configure Cost and Usage Report inputs for the Splunk Add-on for AWS

Complete the steps to configure Cost and Usage Report inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Cost and Usage Report input.
3. Configure AWS permissions for the Cost and Usage Report input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure Cost and Usage Report inputs either through Splunk Web or configuration files.

Enable prefixes so that AWS delivers the reports into a folder with the name of the prefix. Timestamps and report names can be used to filter results if you do not want to ingest all the reports.

After you configure your Cost and Usage Report inputs, see Access billing data for the Splunk Add-on for AWS for more information about data collection behavior and how to access the preconfigured reports included in the add-on.

See the Cost and Usage Report section of the AWS documentation for more information on AWS-side configuration steps.

Configure AWS permissions for the Cost and Usage Report input

You need these required permissions for the S3 bucket to collect your Cost and Usage Reports:

- `Get*`

- List*

In the Resource section of the policy, specify the Amazon Resource Names (ARNs) of the S3 buckets that contain billing reports for your accounts. ListAllMyBuckets is required when you use an asterisk (*) character.

See the following sample inline policy to configure Billing input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*",
      ],
      "Resource": ""arn:aws:s3:::<your bucket name>"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-permissions-ref.html.

Configure a Cost and Usage Report input using Splunk Web

To configure inputs using Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > Billing > Billing (Cost and Usage Report)**.
3. Fill out the fields as described in the following table:

Argument in configuration file	Field in Splunk Web	Description
AWS input configuration		
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Billing data. In Splunk Web, select an account from the drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.
`aws_iam_role`	Assume Role	The IAM role to assume. Verify that your IAMAssume role has enough permission to access your S3 buckets. For more information, see **Add and manage IAM roles** in the Manage accounts for the Splunk Add-on for AWS topic.
`aws_s3_region`	AWS Region	The AWS region that contains your bucket. In inputs.conf, enter the region ID.

Argument in configuration file	Field in Splunk Web	Description
	(Optional)	Provide an AWS Region only if you want to use specific regional endpoints instead of public endpoints for data collection. See the **AWS service endpoints** topic in the AWS General Reference manual for more information.

`s3_private_endpoint_url`	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.amazonaws.com`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3.<region_id>.vpce.amazonaws.com`

`sts_private_endpoint_url`	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws.com`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<region_id>.vpce.amazonaws.com`

`bucket_name`	S3 Bucket	The S3 bucket that is configured to hold Billing Reports.
`private_endpoint_enabled`	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Cloud Storage (S3) services for authentication and data collection. In inputs.conf, enter `0` or `1` to respectively disable or enable use of private endpoints.
`report_prefix`	Report Prefix	Prefixes used to allow AWS to deliver the reports into a specified folder.
`report_names`	Report Name Pattern	A regular expression used to filter reports by name.
Splunk-related configuration		
`start_date`	Start Date	This add-on starts to collect data later than this time. If you leave this field empty, the default value is 90 days before the input is configured. Once the input is created, you cannot change its value.
`sourcetype`	Source type	A source type for the events. Specify a value if you want to override the default of `aws:billing`. Event extraction relies on the default value of source type. If you change the default value, you must update props.conf as well.
`index`	Index	The index name where the Splunk platform puts the billing data. The default is main.
Advanced settings		
`interval`	Interval	Enter the number of seconds to wait before the Splunk platform runs the command again, or enter a valid cron schedule. The default is 86,400 seconds (one day). This interval applies differently for Monthly report types and Detailed report types. For Monthly report types, the interval indicates how often to run the data collection for the current month's monthly report and how often to check the previous month's monthly report's etag to determine if changes were made. If the etag does not match an already-downloaded version of the monthly report, it downloads that report to get the latest data. For Detailed report types, the interval

Argument in configuration file	Field in Splunk Web	Description
		indicates how often to check the previous month's detailed report etag to determine if changes were made. I the etag does not match a report already downloaded, it downloads that report to get the latest data. The present month is never collected until the month has ended. Because AWS Billing Reports are usually not finalized until several days after the last day of the month, you can use the cron expression `0 0 8-31 * *` to skip data collection for the first seven days of every month to avoid collecting multiple copies of not-yet-finalized reports for the just-finished month.
`temp_folder`	Temp folder	Full path to a non-default folder with sufficient space for temporarily storing downloaded detailed billing report .zip files. Take into account the estimated size of uncompressed detailed billing report files, which can be much larger than that of zipped files. If you do not specify a temp folder, the add-on will use the system temp folder by default.

Configure a Cost and Usage Report input using configuration files

To configure inputs in inputs.conf, create a stanza using the following template and add it to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf`. If the file or path does not exist, create it.

```
[aws_billing_cur://<name>]
start_by_shell = true
aws_account = <value>
aws_iam_role = <value>
aws_s3_region = <value>
bucket_name = <value>
bucket_region = <value>
private_endpoint_enabled = <value>
report_names = <value>
report_prefix = <value>
s3_private_endpoint_url = <value>
start_date = <value>
sts_private_endpoint_url = <value>
temp_folder = <value>
host_name = s3.amazonaws.com
```

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_billing_cur]
start_by_shell = false
aws_account = <value>
aws_iam_role = <value>
bucket_name = <value>
bucket_region = <value>
report_names = <value>
report_prefix = <value>
start_date = <value>
temp_folder = <value>
```

The previous values correspond to the default values in Splunk Web. If you choose to copy this stanza to `/local` and use it as a starting point to configure your inputs.conf manually, change the stanza title from `aws_billing:cur` to `aws_billing:cur://<name>`.

Configure Config inputs for the Splunk Add-on for AWS

Complete the steps to configure Config inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Config input.
3. Configure AWS permissions for the Config input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Config inputs either through Splunk Web or configuration files.

Best practices for configuring inputs

- Configure Simple Queue Service (SQS)-based S3 inputs to collect AWS data.
- Configure an AWS Config input for the Splunk Add-on for Amazon Web Services on your data collection node through Splunk Web. This data source is available only in a subset of AWS regions, which does not include China. See http://docs.aws.amazon.com/general/latest/gr/rande.html#awsconfig_region for a full list of supported regions.
- Configure a single enabled Config modular input for each unique SQS. Multiple enabled modular inputs can cause conflicts when trying to delete SQS messages or S3 records that another modular input is attempting to access and parse.
- Disable or delete testing configurations before releasing your configuration in production.

Configure AWS services for the Config input

The Splunk Add-on for AWS collects events from a SQS that subscribes to the Simple Notification Service (SNS) notification events from AWS Config. Configure AWS Config to produce SNS notifications, and then create the SQS that the add-on can access. See http://aws.amazon.com/config/.

1. Enable AWS Config. See http://docs.aws.amazon.com/config/latest/developerguide/setting-up.html.
2. Specify a new S3 bucket to save the data and an SNS Topic to which Splunk software streams Config notifications. Do not use an existing bucket or SNS.
3. Verify that you completed the setup process. If you used the AWS console, the Resource Lookup page displays.
4. Create a new SQS.
5. Subscribe the SQS exclusively to the SNS Topic that you created.
6. Grant IAM permissions to access the S3 bucket and SQS to the AWS account that the add-on uses to connect to your AWS environment.

Configure AWS permissions for the Config input

Set the following permissions in your AWS configuration:

- For the S3 bucket that collects your Config logs:
  - `GetObject`
  - `GetBucketLocation`
  - `ListBucket`
  - `ListAllMyBuckets`
- For the SQS subscribed to the SNS Topic that collects Config notifications:

    - GetQueueAttributes
    - ListQueues
    - ReceiveMessage
    - GetQueueUrl
    - SendMessage
    - DeleteMessage

- For the Config snapshots: `DeliverConfigSnapshot`
- For the IAM user to get the Config snapshots: `GetUser`

See the following sample inline policy to configure Config input permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:ListQueues",
                "sqs:ReceiveMessage",
                "sqs:GetQueueAttributes",
                "sqs:SendMessage",
                "sqs:GetQueueUrl",
                "sqs:DeleteMessage"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeliverConfigSnapshot"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetUser"
            ],
            "Resource": [
                "*"
            ]
        }
```

```
    ]
}
```

For more information and sample policies, see the following AWS documentation:

- For SQS, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/UsingIAM.html.
- For S3, see http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html.

Configure a Config input using Splunk Web

To configure inputs using Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input** > **Config** > **Config**.
3. Fill out the fields as described in the table:

Field in Splunk Web	Description
AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Config data. In Splunk Web, select an account from the drop-down list.
AWS Region	The AWS region that contains the log notification SQS queue. Enter the region ID. See http://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.
SQS queue name	The name of the queue to which AWS sends new Config notifications. Select a queue from the drop-down list, or enter the queue name manually. The queue name is the final segment of the full queue URL. For example, if your SQS queue URL is `http://sqs.us-east-1.amazonaws.com/123456789012/testQueue`, then your SQS queue name is `testQueue`.
Source type	A source type for the events. Enter a value only if you want to override the default of `aws:config`. Event extraction relies on the default value of source type. If you change the default value, you must update props.conf as well. The Splunk platform indexes AWS Config events using three variations of this source type: • Configuration snapshots are indexed as `sourcetype=aws:config`. • Configuration change notifications are indexed as `sourcetype=aws:config:notification`. • Logs from `aws_config.log` are indexed as `sourcetype=aws:config:log`.
Index	The index name where the Splunk platform puts the Config data. The default is main.
Interval	The number of seconds to wait before the Splunk platform runs the command again. The default is 30 seconds.

Configure a Config input using configuration files

To configure inputs manually in inputs.conf, create a stanza using the following template and add it to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf`. If the file or path does not exist, create it.

```
[aws_config://<name>]
aws_account = <value>
aws_region = <value>
sqs_queue = <value>
interval = <value>
sourcetype = <value>
index = <value>
```

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_config]
aws_account =
sourcetype = aws:config
queueSize = 128KB
persistentQueueSize = 24MB
interval = 30
```
The previous values correspond to the default values in Splunk Web as well as some internal values that are not exposed in Splunk Web for configuration. If you choose to copy this stanza to `/local` and use it as a starting point to configure your inputs.conf manually, change the stanza title from `aws_config` to `aws_config://<name>` and add the additional parameters that you need.

Configure Config Rules inputs for the Splunk Add-on for AWS

Complete the steps to configure Config Rules inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Config Rules input.
3. Configure AWS permissions for the Config Rules input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Config Rules inputs either through Splunk Web or configuration files.

Configure AWS services for the Config Rules input

1. Enable AWS Config for all regions for which you want to collect data in the add-on. Follow the steps in the AWS documentation. See http://docs.aws.amazon.com/config/latest/developerguide/setting-up.html.
2. Set up AWS Config Rules by following the instructions in the AWS Config documentation. See http://docs.aws.amazon.com/config/latest/developerguide/evaluate-config_set-up.html.
3. Grant the necessary permissions to the AWS account used for this input. See Configure AWS permissions for details.

Configure AWS permissions for the Config Rules input

You need these required permissions for Config:

- `DescribeConfigRules`
- `DescribeConfigRuleEvaluationStatus`
- `GetComplianceDetailsByConfigRule`
- `GetComplianceSummaryByConfigRule`

See the following sample inline policy to configure Config Rules input permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "config:DescribeConfigRules",
                "config:DescribeConfigRuleEvaluationStatus",
```

```
                "config:GetComplianceDetailsByConfigRule",
                "config:GetComplianceSummaryByConfigRule"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/config/latest/developerguide/example-policies.html

Configure a Config Rules input using Splunk Web

To configure inputs using Splunk Web:

- Click **Splunk Add-on for AWS** in the left navigation bar on Splunk Web home.
- Click **Create New Input > Config Rules**.
- Fill out the fields as described in the table:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Config Rules data. In Splunk Web, select an account from the drop-down list.
`region`	Region	The AWS region that contains the Config Rules. See the AWS documentation for more information.
`rule_names`	Config Rules	Config Rules names in a comma-separated list. Leave blank to collect all rules.
`sourcetype`	Source Type	A source type for the events. Enter a value only if you want to override the default of `aws:config:rule`. Event extraction relies on the default value of source type. If you change the default value, you must update `props.conf` as well.
`index`	Index	The index name where the Splunk platform puts the Config Rules data. The default is main.
`polling_interval`	Polling Interval	The data collection interval, in seconds. The default is 300 seconds.

Configure a Config Rules input using configuration files

To configure the input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_config_rule_tasks.conf` using the following template:

```
[<name>]
account = <value>
region = <value>
rule_names = <value>
sourcetype = <value>
polling_interval = <value>
index = <value>
```

Here is an example stanza that collects Config Rules data for just two rules:

```
[splunkapp2:us-east-1]
account = splunkapp2
region = us-east-1
rule_names=required-tags,restricted-common-ports
```

```
sourcetype = aws:config:rule
polling_interval = 300
index = aws
```

Configure CloudTrail inputs for the Splunk Add-on for AWS

Complete the steps to configure CloudTrail inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the CloudTrail input.
3. Configure AWS permissions for the CloudTrail input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for SQS, STS and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure CloudTrail inputs either through Splunk Web or configuration files.

The CloudTrail input type supports the collection of CloudTrail data (source type: aws:cloudtrail). However, you might want to configure SQS-based S3 inputs to collect this type of data. See Configure SQS-based S3 inputs for the Splunk Add-on for AWS

Before you begin configuring your CloudTrail inputs, be aware of the following behaviors:

- Create a single enabled CloudTrail modular input for each unique Simple Queue Service (SQS) > Simple Notification Service (SNS) > S3 bucket path. Multiple enabled modular inputs can cause conflicts when trying to delete SQS messages or S3 records that another modular input is attempting to access and parse. Be sure to disable or delete testing configurations before going to production.

- If you have multiple AWS regions from which you want to gather CloudTrail data, the Amazon Web Services best practice is that you configure a trail that applies to all regions in the AWS partition in which you are working. You can then set up one CloudTrail input to collect data from the centralized S3 bucket where log files from all the regions are stored.

Configure AWS services for the CloudTrail input

The Splunk Add-on for AWS collects events from an SQS that subscribes to the SNS notification events from CloudTrail. Configure CloudTrail to produce these notifications, then create an SQS in each region for the add-on to access them. The best practice for creating one CloudTrail configuration in one region in order to collect SQS messages of CloudTrail data from all regions, is to perform one of the following tasks:

- Configure one CloudTrail S3 bucket, separate SNS and SQS paths for each region, and configure S3 Event Notification to send to SNS.
- Configure a global CloudTrail, skip steps 3 through 6 below, and configure a Generic S3 input on the add-on to collect data directly from your AWS deployment's S3 bucket.

Configure AWS services

1. Enable CloudTrail. Follow the instructions in the AWS documentation. See http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-and-update-a-trail.html.
2. Create an S3 bucket in which to store the CloudTrail events. Follow the AWS documentation to ensure the permissions for this bucket are correct. See

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/create-s3-bucket-policy-for-cloudtrail.html.
3. Enable SNS notifications. See: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/getting_notifications_top_level.html.
4. Create a new SQS.
5. If you are in the China region, explicitly grant `DeleteMessage` and `SendMessage` permissions to the SQS that you just created. This step is not necessary in commercial regions.
6. Subscribe the SQS to the SNS notifications that you enabled in step 3.
7. Grant IAM permissions to access the AWS account that the add-on uses to connect to your AWS environment. See Manage accounts for the Splunk Add-on for AWS for details.

Configure AWS permissions for the CloudTrail input

Required permissions for the S3 bucket that collects your CloudTrail logs:

- `Get*`
- `List*`
- `Delete*`

Granting the delete permission is required to support the option to remove log files when done collecting them with the add-on. If you set this parameter to `false`, you do not need to grant delete permissions.

Required permissions for the SQS subscribed to the S3 bucket that collects CloudTrail logs:

- `GetQueueAttributes`
- `ListQueues`
- `ReceiveMessage`
- `GetQueueUrl`
- `DeleteMessage`

In the Resource section of the policy, specify the ARNs of the S3 buckets and SQS queues from which you want to collect data.

See the following sample inline policy to configure CloudTrail input permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:ListQueues",
                "sqs:ReceiveMessage",
                "sqs:GetQueueUrl",
                "sqs:DeleteMessage",
                "s3:Get*",
                "s3:List*",
                "s3:Delete*"
            ],
            "Resource": [
               "*"
            ]
        }
    ]
}
```

For more information and sample policies, see these resources in the AWS documentation:

- For SQS, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/UsingIAM.html.
- For S3, see http://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html.

Configure a CloudTrail input using Splunk Web

To configure inputs in Splunk Web:

1. Click on **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > CloudTrail**.
3. Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your CloudTrail data. In Splunk Web, select an account from the drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.
`aws_region`	AWS Region	The AWS region that contains the log notification SQS queue. In inputs.conf, enter the region ID. See http://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.
`private_endpoint_enabled`	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Cloud Storage (S3) services for authentication and data collection. In inputs.conf, enter `0` or `1` to respectively disable or enable use of private endpoints.

`s3_private_endpoint_url`	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.amazonaws.com`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3.<region_id>.vpce.amazonaws.com`

`sts_private_endpoint_url`	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws.com`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<region_id>.vpce.amazonaws.com`

`sqs_queue`	SQS queue name	The name of the queue to which AWS sends new CloudTrail log notifications. In Splunk Web, you can select a queue from the drop-down list, if your account permissions allow you to list queues, or enter the queue name manually. The queue name is the final segment of the full queue URL. For example, if your SQS queue URL is `http://sqs.us-east-1.amazonaws.com/123456789012/testQueue`, then your SQS queue name is `testQueue`.
`sqs_private_endpoint_url`	Private Endpoint	Private Endpoint (Interface VPC Endpoint) of your SQS service, which can be configured from your AWS console.

Argument in configuration file	Field in Splunk Web	Description
	URL (SQS)	Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.sqs.<region_id>.vpce.amazonaws.com <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sqs.<region_id>.vpce.amazonaws.com
remove_files_when_done	Remove logs when done	A Boolean value indicating whether the Splunk platform should delete log files from the S3 bucket after indexing is complete. The default is false.
exclude_describe_events	Exclude events	A Boolean value indicating whether or not to exclude certain events, such as read-only events that can produce a high volume of data. The default is true.
blacklist	Deny list for exclusion	A PCRE regular expression that specifies event names to exclude if exclude_describe_events is set to true. Leave blank to use the default regex ^(?:Describe|List|Get).
excluded_events_index	Excluded events index	The name of the index in which the Splunk platform puts excluded events. The default is empty, which discards the events.
interval	Interval	The number of seconds to wait before the Splunk platform runs the command again. The default is 30 seconds.
log_partitions	n/a	Configure partitions of a log file to be ingested. This add-on searches the log files for <Region ID> and <Account ID>. For example, log_partitions = AWSLogs/<Account ID>/CloudTrail/<Region>.
sourcetype	Source type	A source type for the events. Enter a value only if you want to override the default of aws:cloudtrail. Event extraction relies on the default value of source type. If you change the default value, you must update props.conf as well.
index	Index	The index name where the Splunk platform puts the CloudTrail data. The default is main.

Configure a CloudTrail input using configuration files

To configure inputs manually in inputs.conf, create a stanza using the following template and add it to $SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf. If the file or path does not exist, create it.

```
[aws_cloudtrail://<name>]
aws_account = <value>
aws_region = <value>
private_endpoint_enabled = <value>
sqs_queue = <value>
sqs_private_endpoint_url = <value>
s3_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
exclude_describe_events = <value>
remove_files_when_done = <value>
blacklist = <value>
excluded_events_index = <value>
interval = <value>
sourcetype = <value>
index = <value>
```

Some of these settings have default values that can be found in $SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf:

```
[aws_cloudtrail]
aws_account =
sourcetype = aws:cloudtrail
exclude_describe_events = true
remove_files_when_done = false
queueSize = 128KB
persistentQueueSize = 24MB
interval = 30
```

The values in default/inputs.conf correspond to the default values in Splunk Web as well as some internal values that are not exposed in Splunk Web for configuration. If you choose to copy this stanza to `/local` and use it as a starting point to configure your inputs.conf manually, change the stanza title from `aws_cloudtrail` to `aws_cloudtrail://<name>`.

Switch from a CloudTrail input to an SQS-based S3 input

The SQS-based S3 input is a more fault-tolerant and higher-performing alternative to the CloudTrail input for collecting CloudTrail data. If you are already collecting CloudTrail data using a CloudTrail input, you can configure an SQS-based S3 input and seamlessly switch to the new input for CloudTrail data collection with little disruption.

1. Disable the CloudTrail input you are using to collect CloudTrail data.
2. Set up a Dead-Letter Queue (DLQ) and the SQS visibility timeout setting for the SQS queue from which you are collecting CloudTrail data. See Configure SQS-based S3 inputs for the Splunk Add-on for AWS.
3. Create an SQS-based S3 input, pointing to the SQS queue you configured in the last step. Configure SQS-based S3 inputs for the Splunk Add-on for AWS for the detailed configuration steps.

Once configured, the new SQS-based S3 input replaces the old CloudTrail input to collect CloudTrail data from the same SQS queue.

Configure CloudWatch inputs for the Splunk Add-on for AWS

Complete the steps to configure CloudWatch inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the CloudWatch input.
3. Configure AWS permissions for the CloudWatch input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS, monitoring, ELB, EC2, Autoscaling, Lambda and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. Configuration of all service endpoints is not required. Configure only those endpoints which are required for each specific metric. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure CloudWatch inputs either through Splunk Web or configuration files.

Configure separate CloudWatch inputs for each metric or set of metrics that have different minimum granularities, based on the sampling period that AWS allows for that metric. For example, CPUUtilization has a sampling period of 5 minutes, whereas Billing Estimated Charge has a sampling period of 4 hours. If you configure a granularity that is smaller than the minimum sampling period available in AWS, the input wastes API calls.

For more information, see Sizing, performance, and cost considerations for the Splunk Add-on for AWS.

Configure AWS services for the CloudWatch input

To enable AWS to produce billing metrics in CloudWatch, turn on **Receive Billing Alerts** in the Preferences section of the Billing and Cost Management console.

The CloudWatch service is automatically enabled to collect free metrics for your AWS services and requires no additional configuration for the Splunk Add-on for AWS.

Configure CloudWatch permissions

Required permissions for CloudWatch: `Describe*, Get*, List*`

Required permissions for Autoscaling: `Describe*`

Required permissions for EC2: `Describe*`

Required permissions for S3: `List*`

Required permissions for SQS: `List*`

Required permissions for SNS: `List*`

Required permissions for Lambda: `List*`

Required permissions for ELB: `Describe*`

See the following sample inline policy to configure CloudWatch input permissions:

```
{
  "Statement": [{
    "Action": [
      "cloudwatch:List*",
      "cloudwatch:Get*",
      "autoscaling:Describe*",
      "ec2:Describe*",
      "s3:List*",
      "sqs:List*",
      "sns:List*",
      "lambda:List*",
      "elasticloadbalancing:Describe*"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }],
  "Version": "2012-10-17"
}
```

For more information and sample policies, see:
http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/UsingIAM.html

Configure a CloudWatch input using Splunk Web

To configure inputs in Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > CloudWatch**.
3. Click **Advanced** to edit **Metrics Configuration**.
4. Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your CloudWatch data. from the drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts tha page or the name of the automatically discovered EC2 IAM role.
`aws_iam_role`	Assume Role	The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.
`aws_region`	AWS Regions	The AWS region name or names. In Splunk Web, select one or more regions from the drop-do more valid AWS region IDs, separated by commas. See http://docs.aws.amazon.com/general/ information.
`interval`	Interval	The number of seconds to wait before the Splunk platform runs the command again. Set pollin parameter according to your requirements in the inputs.conf file. Default value is 300 or 5 mins
Metrics Configuration arguments		
`metric_dimensions`	Dimensions	CloudWatch metric dimensions display as a JSON array, with strings as keys and regular expr automatically populates correctly formatted JSON objects to collect all metric dimensions in th you want, you can customize the JSON object to limit the collection to just the dimensions you SQS namespace, you can collect only the metrics for queue names that start with "splunk" and `[{"QueueName": ["\"splunk.*_current\\\\s\""]}]`. You can set multiple dimensions in one data input. If you use a JSON array, the dimension ma array is matched. A JSON object has strings as keys and values that are either a regex or an a for AWS supports one JSON object per JSON array. For example, `[{"key1": "regex1"},` supported. A dimension is matched to the object if it meets these two conditions: • It has the same key set to the object • In the value of each key, there is one or more elements matched by every regex in th object. For example, `[{"key":["val.*", ".*lue"]}]` matches `{"key":"value"}` and `{` `{"key":"value", "key2":"value2"}`. The BucketName dimension does not support wildcards or arrays with length g collect metrics from the AWS S3 namespace, configure separate CloudWatch example, `{"StorageType": ["StandardStorage"], "BucketName": ["my_favor`
`metric_names`	Metrics	CloudWatch metric names in JSON array. For example, `["CPUUtilization","DiskReadOps","StatusCheckFailed_System"]`. Splunk Web formatted JSON objects for all metric names in the namespace you have selected. Edit the JS do not want to collect. Collecting metrics you do not need results in unnecessary API calls.
`metric_namespace`	Namespace	The metric namespace. For example, `AWS/EBS`. In Splunk Web, click **+ Add Namespace** and drop-down list or manually enter it. If you manually enter a custom namespace, you need to ty

Argument in configuration file	Field in Splunk Web	Description
		for the remaining fields. In inputs.conf, enter a valid namespace for the region you specified. Y namespace per input.
metric_expiration	Metric Expiration	Duration of time the discovered metrics are cached for, measured in seconds.
index	Index	The index name where the Splunk platform puts the CloudWatch data. The default is main.
period	Period	The granularity, in seconds, of the returned data points. For metrics with regular resolution, a p (1 minute) and must be a multiple of 60. Different AWS metrics can support different minimum period that AWS allows for that metric. For example, CPUUtilization has a sampling period of 5 Charge has a sampling period of 4 hours. Do not configure a granularity that is less than the a selected metric, or else the reported granularity reflects the sampling granularity but is labeled resulting in inconsistent data. The smaller your granularity, the more precise your metrics data becomes. Co useful when you want to do precise analysis of metrics and you are not concer volume. Configure a larger granularity when a broader view is acceptable or yo data you collect from AWS.
private_endpoint_enabled	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS for authentication and data collection. In inputs.conf, enter 0 or 1 to respectively disable or ena
sts_private_endpoint_url	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.ama <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts _id>.vpce.amazonaws.com
monitoring_private_endpoint_url	Private Endpoint URL (Monitoring)	Private Endpoint (Interface VPC Endpoint) of your monitoring service, which can be configured Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.monitoring.<region_id>. <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.mon _id>.vpce.amazonaws.com
elb_private_endpoint_url	Private Endpoint URL (ELB)	Private Endpoint (Interface VPC Endpoint) of your Elastic Load Balancer (ELB) service, which console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.elasticloadbalancing.<r <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.ela _id>.vpce.amazonaws.com
ec2_private_endpoint_url	Private Endpoint URL (EC2)	Private Endpoint (Interface VPC Endpoint) of your Elastic Compute Cloud (EC2) service, whic console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.ec2.<region_id>.vpce.ama

Argument in configuration file	Field in Splunk Web	Description
		<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.ec2 _id>.vpce.amazonaws.com
autoscaling_private_endpoint_url	Private Endpoint URL (Autoscaling)	Private Endpoint (Interface VPC Endpoint) of your Autoscaling service, which can be configure Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.autoscaling.<region_id> <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.aut _id>.vpce.amazonaws.com
lambda_private_endpoint_url	Private Endpoint URL (Lambda)	Private Endpoint (Interface VPC Endpoint) of your Lambda service, which can be configured fr Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.lambda.<region_id>.vpce <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.lam _id>.vpce.amazonaws.com
s3_private_endpoint_url	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from y Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.ama <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3. _id>.vpce.amazonaws.com
query_window_size	Query Window Size	Window of time used to determine how far back in time to go in order to retrieve data points, m
statistics	Metric statistics	The metric statistics you want to request. Choose from Average, Sum, SampleCount, Ma this list must be JSON encoded. For example: ["Average","Sum","SampleCount","Max
sourcetype	Source type	A source type for the events. Enter a value if you want to override the default of aws:cloudwa default value of source type. If you change the default value, you must update props.conf as w

Configure a CloudWatch input using configuration files

To configure inputs manually in inputs.conf, create a stanza using the following template and add it to $SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf. If the file or path does not exist, create it.

```
[aws_cloudwatch://<name>]
aws_account = <value>
aws_iam_role=<value>
aws_region = <value>
metric_namespace = <value>
metric_names = <value>
metric_dimensions = <value>
private_endpoint_enabled = <value>
sts_private_endpoint_url = <value>
s3_private_endpoint_url = <value>
autoscaling_private_endpoint_url = <value>
ec2_private_endpoint_url = <value>
elb_private_endpoint_url = <value>
```

```
monitoring_private_endpoint_url = <value>
lambda_private_endpoint_url = <value>
statistics = <value>
period = <value>
sourcetype = <value>
index = <value>
metric_expiration = <value>
query_window_size = <value>
```

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_cloudwatch]
start_by_shell = false
sourcetype = aws:cloudwatch
use_metric_format = false
metric_expiration = 3600
query_window_size = 24
interval = 300
python.version = python3
```

The previous values correspond to the default values in Splunk Web as well as some internal values that are not exposed in Splunk Web for configuration. If you choose to copy this stanza to `/local` and use it as a starting point to configure your inputs.conf manually, change the stanza title from `aws_cloudwatch` to `aws_cloudwatch://<name>`.

> If you want to change the interval, copy the [aws_cloudwatch] stanza to the local/inputs.conf file then set the interval value as you want. It will override the default value set in default/inputs.conf

.

Send CloudWatch events to a metrics index

Configure the Splunk Add-on for AWS to collect CloudWatch events and send them to a metrics index.

Prerequisites

- Splunk Enterprise version 7.2 and higher.
- An existing metrics index. See Get started with metrics in the Splunk Enterprise *Metrics* manual to learn more about creating a metrics index.

1. In Splunk Web, click **Splunk Add-on for AWS** in the left navigation bar on Splunk Web home.
2. Click **Create New Input > CloudWatch**.
3. In the **AWS Input Configuration** section, populate the **Name**, **AWS Account**, **Assume Role**, and **AWS Regions** fields, using the previous table as a reference.
4. Navigate to the **Splunk-related Configuration** section.
5. In the **Source Type** field, type `aws:cloudwatch:metric`.
6. Click on the **Index** dropdown menu, and type the name of your metrics index.
7. Click **Save**.

Configure CloudWatch Log inputs for the Splunk Add-on for AWS

Complete the steps to configure CloudWatch Log inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the CloudWatch Log input.
3. Configure AWS permissions for the CloudWatch Log input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS and logs services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure CloudWatch Log inputs either through Splunk Web or configuration files.

Due to rate limitations, don't use the Splunk Add-on for AWS to collect CloudWatch Log data which has the source type aws:cloudwatchlogs:*. Instead, use the Splunk Add-on for Amazon Kinesis Firehose to collect CloudWatch Log and VPC Flow Logs. The Splunk Add-on for Amazon Kinesis Firehose includes index-time logic to perform the correct knowledge extraction for these events through the Kinesis input as well.

Configure AWS permissions for the CloudWatch Log input

Required permissions for Logs:

- `DescribeLogGroups`
- `DescribeLogStreams`
- `GetLogEvents`
- `s3:GetBucketLocation`

See the following sample inline policy to configure CloudWatch Log input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:GetLogEvents",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

You must also ensure that your role has a trust relationship that allows the flow logs service to assume the role. While viewing the IAM role, choose **Edit Trust Relationship** and replace that policy with this one:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

Configure a CloudWatch Logs input using Splunk Web

To configure inputs using Splunk Web, click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home, then choose one of the following menu paths depending on the data type you want to collect:

- **Create New Input > VPC Flow Logs > CloudWatch Logs**
- **Create New Input > Others > CloudWatch Logs**

Fill out the fields as described in the table:

Argument in configuration file	Field in Splunk Web	Description
`account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your CloudWatch Logs data. In Splu Web, select an account from the drop-down list. In `aws_cloudwatch_logs_tasks.conf`, enter the frien name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.
`region`	AWS Region	The AWS region that contains the data. In `aws_cloudwatch_logs_tasks.conf`, enter the region ID.
`private_endpoint_enabled`	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Clou Storage (S3) services for authentication and data collection. In inputs.conf, enter `0` or `1` to respectively disa or enable use of private endpoints.

`logs_private_endpoint_url`	Private Endpoint URL (Logs)	Private Endpoint (Interface VPC Endpoint) of your logs service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.logs.<region_id>.vpce.amazonaws.c`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.logs.<region _id>.vpce.amazonaws.com`

`sts_private_endpoint_url`	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws.co`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<region _id>.vpce.amazonaws.com`

`groups`	Log group	A comma-separated list of log group names. Do not use wildcards.
`only_after`	Only After	GMT time string in '%Y-%m-%dT%H:%M:%S' format. If set, only events after this time are queried and indexed. Defaults to 1970-01-01T00:00:00.
`stream_matcher`	Stream Matching Regex	REGEX to strictly match stream names. Defaults to `.*`
`interval`	Interval	

Argument in configuration file	Field in Splunk Web	Description
		The number of seconds to wait before the Splunk platform runs the command again. The default is 600 seconds.
`sourcetype`	Source type	A source type for the events. Enter `aws:cloudwatchlogs:vpcflow` if you are indexing VPC Flow Log data. Enter `aws:cloudwatchlogs` if you are collecting any other CloudWatch Logs data.
`index`	Index	The index name where the Splunk platform puts the CloudWatch Logs data. The default is main.

Configure a CloudWatch Logs input using configuration files

To configure the input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_cloudwatch_logs_tasks.conf` using the following template:

```
[<name>]
account = <value>
groups = <value>
index = <value>
interval = <value>
only_after = <value>
region = <value>
private_endpoint_enabled = <value>
logs_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
sourcetype = <value>
stream_matcher = <value>
```

Here is an example stanza that collects VPC Flow Log data from two log groups:

```
[splunkapp2:us-west-2]
account = splunkapp2
groups = SomeName/DefaultLogGroup, SomeOtherName/SomeOtherLogGroup
index = default
interval = 600
only_after = 1970-01-01T00:00:00
region = us-west-2
sourcetype = aws:cloudwatchlogs:vpcflow
stream_matcher = eni.*
```

Configure Description inputs for the Splunk Add-on for AWS

> The Description input will be deprecated in a future release. The Metadata input has been added as a replacement. The best practice is to begin moving your workloads to the Metadata input.

Complete the steps to configure Description inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Description input.
3. Configure AWS permissions for the Description input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Description inputs either through Splunk Web or configuration files.

Configure Description permissions

Required permissions for EC2 resources: `DescribeInstances, DescribeReservedInstances, DescribeSnapshots, DescribeRegions, DescribeKeyPairs, DescribeNetworkAcls, DescribeSecurityGroups, DescribeSubnets, DescribeVolumes, DescribeVpcs, DescribeImages, DescribeAddresses`

Required permissions for Lambda: `ListFunctions`

Required permissions for RDS: `DescribeDBInstances`

Required permissions for CloudFront, if you are in a region that supports CloudFront: `ListDistributions`

Required permissions for ELB: `DescribeLoadBalancers, DescribeInstanceHealth, DescribeTags, DescribeTargetGroups, DescribeTargetHealth`

Required permissions for S3: `ListAllMyBuckets, GetAccelerateConfiguration, GetBucketCORS, GetLifecycleConfiguration, GetBucketLocation, GetBucketLogging, GetBucketTagging`

See the following sample inline policy to configure Description input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeRegions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "lambda:ListFunctions",
        "rds:DescribeDBInstances",
        "cloudfront:ListDistributions",
        "iam:GetUser",
        "iam:ListUsers",
        "iam:GetAccountPasswordPolicy",
        "iam:ListAccessKeys",
        "iam:GetAccessKeyLastUsed",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "s3:ListAllMyBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketCORS",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
```

```
        "s3:GetBucketTagging"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Configure a Description input using Splunk Web

To configure inputs in Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > Description > Description**.
3. Fill out the fields as described in the following table:

Argument in configuration file	Field in Splunk Web	Description
`account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Description data. In Splunk Web, select an a In `aws_description_tasks.conf`, enter the friendly name of one of the AWS accounts that you configured on the Co of the automatically discovered EC2 IAM role.
`aws_iam_role`	Assume Role	The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.
`regions`	AWS Regions	The AWS regions for which you are collecting Description data. In Splunk Web, select one or more regions from the drop aws_description_tasks.conf, enter one or more valid AWS region IDs, separated by commas. See https://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.
`apis`	APIs/Interval (seconds)	APIs you want to collect data from, and intervals for each API, in the format of <api name>/<api interval in seconds>,<api seconds>. The default value in Splunk Web is `ec2_volumes/3600,ec2_instances/3600,ec2_reserved_instances/3600,ebs_snapshots/3600,elasti /3600,vpcs/3600,vpc_network_acls/3600,cloudfront_distributions/3600,vpc_subnets/3600,rds_ _pairs/3600,ec2_security_groups/3600` . This value collects from all of the APIs supported in this release. Set your intervals to 3,600 seconds (1 hour) or longer t
`sourcetype`	Source type	A source type for the events. Enter `aws:description`.
`index`	Index	The index name where the Splunk platform puts the Description data. The default is main.

Configure a Description input using configuration files

To configure a Description input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_description_tasks.conf` using the following template:

```
[<name>]
account = <value>
aws_iam_role=<value>
apis = <value>
index = <value>
regions = <value>
sourcetype = <value>
```

Here is an example stanza that collects description data from all supported APIs:

```
[desc:splunkapp2]
account = splunkapp2
```

```
apis = ec2_volumes/3600, ec2_instances/3600, ec2_reserved_instances/3600, ebs_snapshots/3600,
classic_load_balancers/3600, application_load_balancers/3600, vpcs/3600, vpc_network_acls/3600,
cloudfront_distributions/3600, vpc_subnets/3600, rds_instances/3600, ec2_key_pairs/3600,
ec2_security_groups/3600, ec2_images/3600, ec2_addresses/3600, lambda_functions/3600, s3_buckets/3600,
iam_users/3600
index = default
regions = us-west-2
sourcetype = aws:description
```

Configure Incremental S3 inputs for the Splunk Add-on for AWS

Complete the steps to configure Incremental S3 inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Incremental S3 input.
3. Configure AWS permissions for the Incremental S3 input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure Incremental S3 inputs either through Splunk Web or configuration files.

From version 4.3.0 and higher, the Splunk Add-on for AWS provides the Simple Queue Service (SQS)-based S3 input, which is a more scalable and higher-performing alternative to the generic S3 and incremental S3 input types for collecting various types of log files from S3 buckets. For new inputs for collecting a variety of predefined and custom data types, consider using the SQS-based S3 input instead.

The incremental S3 input only lists and retrieves objects that have not been ingested from a bucket by comparing datetime information included in filenames against checkpoint record, which significantly improves ingestion performance.

Configure AWS services for the Incremental S3 input

To collect access logs, configure logging in the AWS console to collect the logs in a dedicated S3 bucket. See the AWS documentation for more information on how to configure access logs:

- For S3 access logs, see http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html.
- Enable ELB access logs, see http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/enable-access-logs.html.
- Enable CloudFront access logs, see http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html.

See http://docs.aws.amazon.com/gettingstarted/latest/swh/getting-started-create-bucket.html for more information about how to configure S3 buckets and objects.

Configure S3 permissions

Required permissions for S3 buckets and objects:

- `ListBucket`
- `GetObject`
- `ListAllMyBuckets`
- `GetBucketLocation`

Required permissions for KMS:

- `Decrypt`

In the Resource section of the policy, specify the Amazon Resource Names (ARNs) of the S3 buckets from which you want to collect S3 Access Logs, CloudFront Access Logs, ELB Access Logs, or generic S3 log data.

See the following sample inline policy to configure S3 input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html.

Configure an Incremental S3 input using Splunk Web

To configure inputs in Splunk Web, click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home, then choose one of the following menu paths depending on which data type you want to collect:

- **Create New Input > CloudTrail > Incremental S3**
- **Create New Input > CloudFront Access Log > Incremental S3**
- **Create New Input > ELB Access Logs > Incremental S3**
- **Create New Input > S3 Access Logs > Incremental S3**

Make sure you choose the right menu path corresponding to the data type you want to collect. The system automatically sets the appropriate source type and may display slightly different field settings in the subsequent configuration page based on the menu path.

Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access the keys in your S3 buckets. In Splunk Web, select an account from the drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.

Argument in configuration file	Field in Splunk Web	Description
		If the region of the AWS account you select is **GovCloud**, you may encounter errors, such as "Failed to load options for S3 Bucket". You need to manually add **AWS GovCloud Endpoint** in the **S3 Host Name** field. See http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-govcloud-endpoints.htm for more information.
`aws_iam_role`	Assume Role	The IAM role to assume, see The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS
`aws_s3_region`	AWS Region (Optional)	The AWS region that contains your bucket. In inputs.conf, enter the region ID. Provide an AWS Region only if you want to use specific regional endpoints instead of public endpoints for data collection. See the **AWS service endpoints** topic in the AWS General Reference manual for more information.
`bucket_name`	S3 Bucket	The AWS bucket name.
`log_file_prefix`	Log File Prefix	Configure the prefix of the log file, which along with other path elements, forms the URL under which the Splunk Add-on for AWS searches the log files. The locations of the log files are different for each S3 incremental log type: • **cloudtrail**: The Splunk Add-on for AWS searches for the CloudTrail logs under `<bucket_name>/<log_file_prefix>/AWSLogs/<Account ID>/CloudTrail/<Region ID>/<YYYY/MM/DD>/<file_name>.json.gz`. • **elb**: The Splunk Add-on for AWS searches the elb access logs under `<bucket_name>/<log_file_prefix>/AWSLogs/<Account ID>/elasticloadbalancing/<Region ID>/<YYYY/MM/DD>/<file_name>.log.gz`. • **S3**: The Splunk Add-on for AWS searches the S3 access logs under `<bucket_name>/<log_file_prefix><YYYY-mm-DD-HH-MM-SS><UniqueString>`. • **cloudfront**: The Splunk Add-on for AWS searches the CloudFront access logs under `<bucket_name>/<log_file_prefix><distributionID><YYYY/MM/DD>.<UniqueID>.g` Under one AWS account, to ingest logs in different prefixed locations in the bucket, you need to configure multiple AWS data inputs, one for each prefix name. Alternatively, you can configure one data input but use different AWS accounts to ingest logs in different prefixed locations in the bucket.
`log_type`	Log Type	The type of logs to ingest. Available log types are `cloudtrail`, `elb:accesslogs`, `cloudfront:accesslogs`, and `s3:accesslogs`. This value is automatically set based on the menu path you chose to access this configuration page.
`log_start_date`	Log Start Date	The start date of the log.
`distribution_id`	Distribution ID	CloudFront distribution ID. This field is displayed only when you access the input configuration page through the **Create New Input > CloudFront Access Log > Incremental S3** menu path.
`sourcetype`	Source Type	Source type for the events. This value is automatically set for the type of logs you want to collect based on the menu path you chose to access this configuration page.
`index`	Index	The index name where the Splunk platform puts the S3 data. The default is main.

Argument in configuration file	Field in Splunk Web	Description
interval	Interval	The number of seconds to wait before splunkd checks the health of the modular input so that it can trigger a restart if the input crashes. The default is 30 seconds.
private_endpoint_enabled	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Cloud Storage (S3) services for authentication and data collection. In inputs.conf, enter 0 or 1 to respectively disable or enable use of private endpoints.
s3_private_endpoint_url	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from your AWS console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.amazonaws.com <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3.<region_id>.vpce.amazonaws.com
sts_private_endpoint_url	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AWS console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws.com <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<region_id>.vpce.amazonaws.com

Configure an Incremental S3 input using a configuration file

When you configure inputs manually in inputs.conf, create a stanza using the following template and add it to $SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf. If the file or path does not exist, create it.

```
[splunk_ta_aws_logs://<name>]
log_type =
aws_account =
[splunk_ta_aws_logs://<name>]
aws_s3_region = <value>
host_name =
bucket_name =
bucket_region =
log_file_prefix =
log_start_date =
log_name_format =
aws_iam_role = AWS IAM role that to be assumed.
max_retries = @integer:[-1, 1000]. default is -1. -1 means retry until success.
max_fails = @integer: [0, 10000]. default is 10000. Stop discovering new keys if the number of failed files
exceeded the max_fails.
max_number_of_process = @integer:[1, 64]. default is 2.
max_number_of_thread = @integer:[1, 64]. default is 4.
private_endpoint_enabled = <value>
s3_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
```

Configure Inspector inputs for the Splunk Add-on for AWS

Complete the steps to configure Inspector inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Inspector input.
3. Configure AWS permissions for the Inspector input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Inspector inputs either through Splunk Web or configuration files.

Configure Amazon Inspector permissions

You need these required permissions for Inspector:

- `Describe*`
- `List*`

See the following sample inline policy to configure Inspector input permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector:Describe*",
                "inspector:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

For more information, see http://docs.aws.amazon.com/IAM/latest/UserGuide/list_inspector.html.

Configure an Inspector input using Splunk Web

To configure inputs using Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > Inspector**.
3. Use the following table to complete the fields for the new input in Splunk Web or in the .conf file:

Argument in configuration file	Field in Splunk Web	Description
`account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Inspector findings. In Splunk Web, select an account from the drop-down list. In aws_inspector_tasks.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.
`regions`	AWS Region	The AWS region that contains the data. In aws_inspector_tasks.conf, enter region IDs in a comma-separated list.

Argument in configuration file	Field in Splunk Web	Description
`sourcetype`	Source type	A source type for the events. Enter a value only if you want to override the default of `aws:inspector`. Event extraction relies on the default value of source type. If you change the default value, you must update props.conf as well.
`index`	Index	The index name where the Splunk platform puts the Inspector findings. The default is main.
`polling_interval`	Pooling interval	The number of seconds to wait before the Splunk platform runs the command again. The default is 300 seconds.

Configure an Inspector input using configuration files

To configure the input using the configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_inspector_tasks.conf` using the following template:

```
[<name>]
account = <value>
region = <value>
index = <value>
polling_interval = <value>
sourcetype = <value>
```

Here is an example stanza that collects Inspector findings:

```
[splunkapp2:us-west-2]
account = splunkapp2
region = us-west-2
index = default
polling_interval = 300
sourcetype = aws:inspector
```

Configure Kinesis inputs for the Splunk Add-on for AWS

Complete the steps to configure Kinesis inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Kinesis input.
3. Configure AWS permissions for the Kinesis input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS and Kinesis services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure Kinesis inputs either through Splunk Web or configuration files.

You can see the "Performance for the Kinesis input in the Splunk Add-on for AWS" section of this page for reference data to enhance the performance of your own Kinesis data collection task.

Kinesis is the recommended input type for collecting VPC Flow Logs. This input type also supports the collection of custom data types through Kinesis streams.

This data source is available only in a subset of AWS regions. For a full list of supported regions, see https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/.

The Kinesis data input only supports gzip compression or plaintext data. It cannot ingest data with other encodings, nor can it ingest data with a mix of gzip and plaintext in the same input. Create separate Kinesis inputs for gzip data and plaintext data.

Configure AWS permissions for the Kinesis input

Required permission for Amazon Kinesis:

- `Get*`
- `DescribeStream`
- `ListStreams`

See the following sample inline policy to configure Kinesis input permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:Get*",
                "kinesis:DescribeStream",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

Configure a Kinesis input using Splunk Web

To configure inputs in Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Choose one of the following menu paths depending on which data type you want to collect:

- **Create New Input > VPC Flow Logs > Kinesis**
- **Create New Input > Others > Kinesis**

Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Kinesis data. In Splunk We an account from the drop-down list. In aws_kinesis_tasks.conf, enter the friendly name of one of the AW accounts that you configured on the Configuration page or the name of the automatically discovered EC role.
`aws_iam_role`		The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.

Argument in configuration file	Field in Splunk Web	Description
	Assume Role	
region	AWS Region	The AWS region that contains the Kinesis streams. In aws_kinesis_tasks.conf, enter the region ID. See https://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.
private_endpoint_enabled	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Storage (S3) services for authentication and data collection. In inputs.conf, enter 0 or 1 to respectively enable use of private endpoints.
kinesis_private_endpoint_url	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your Kinesis service, which can be configured from your A console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.kinesis.<region_id>.vpce.amazo <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.kinesis.<r _id>.vpce.amazonaws.com
sts_private_endpoint_url	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AW Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws
stream_names	Stream Names	Stream names in a comma-separated list. Each stream_name must be unique to each region. If a stream_name is the same for two different regions, it fails. Leave blank to collect all streams.
encoding	Encoding	The encoding of the stream data. Set to gzip or leave blank, which defaults to Base64. All stream data collect in a single input must have the same encoding. If you are collecting VPC Flow Logs data throug input, encoding is typically gzip.
init_stream_position	Initial Stream Position	LATEST or TRIM_HORIZON. LATEST starts data collection from the point the input is enabled. TRIM_ starts collecting with the oldest data record.
format	Record Format	CloudWatchLogs or none. If you choose CloudWatchLogs, this add-on parses the data in CloudWatchL format.
sourcetype	Source type	A source type for the events. Enter aws:cloudwatchlogs:vpcflow if you are indexing VPC Flow L through Kinesis. Enter aws:kinesis if you are collecting any other Kinesis data.
index	Index	The index name where the Splunk platform puts the Kinesis data. The default is main.

Configure a Kinesis input using configuration files

To configure the input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_kinesis_tasks.conf` using the following template:

```
[<name>]
account = <value>
aws_iam_role=<value>
region = <value>
private_endpoint_enabled = <value>
kinesis_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
stream_names = <value>
```

```
encoding = <value>
init_stream_position = <value>
format = <value>
sourcetype = <value>
index = <value>
```
Here is an example stanza that collects Kinesis data for all streams available in the region:

```
[splunkapp2:us-east-1]
account = splunkapp2
region = us-east-1
encoding =
init_stream_position = LATEST
index = aws
format = CloudWatchLogs
sourcetype = aws:kinesis
```

Performance for the Kinesis input in the Splunk Add-on for AWS

This page provides the reference information about the performance testing of the Kinesis input in Splunk Add-on for AWS. The testing was performed on version 4.0.0, when the Kinesis input was first introduced. You can use this information to enhance the performance of your own Kinesis data collection tasks.

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

Summary

While results in different environments will vary, the performance testing of the Kinesis input showed the following:

- Each Kinesis input can handle up to 6 MB/s of data, with a daily ingestion volume of 500 GB.
- More shards can slightly improve the performance. Three shards are recommended for large streams.

Testing architecture

Splunk tested the performance of the Kinesis input using a single-instance Splunk Enterprise 6.4.0 on an m4.4xlarge AWS EC2 instance to ensure CPU, memory, storage, and network did not introduce any bottlenecks. See the following instance specs:

Instance type	M4 Quadruple Extra Large (m4.4xlarge)
Memory	64 GB
ECU	53.5
Cores	16
Storage	0 GB (EBS only)
Architecture	64-bit
Network performance	High
EBS Optimized: Max Bandwidth	250 MB/s

Test scenario

Splunk tested the following parameters to target the use case of high-volume VPC flow logs ingested through a Kinesis stream:

- Shard numbers: 3, 5, and 10 shards
- Event size: 120 bytes per event
- Number of events: 20,000,000
- Compression: gzip
- Initial stream position: TRIM_HORIZON

AWS reports that each shard is limited to 5 read transactions per second, up to a maximum read rate of 2 MB per second. Thus, with 10 shards, the theoretical upper limit is 20 MB per second.

Test results

Splunk observed a data ingestion rate of 6 million events per minute at peak, which is 100,000 events per second. Because each event is 120 bytes, this indicates a maximum throughput of 10 MB/s.

Splunk observed an average throughput of 6 MB/s for a single Kinesis modular input, or a daily ingestion throughput of approximately 500 GB.

After reducing the shard number from 10 shards to 3 shards, Splunk observed a throughput downgrade of approximately 10%.

During testing, Splunk observed the following resource usage on the instance:

- Normalized CPU usage of approximately 30%
- Python memory usage of approximately 700 MB

The indexer is the largest consumer of CPU, and the modular input is the largest consumer of memory.

AWS throws a ProvisionedThroughputExceededException if a call returns 10 MB of data and subsequent calls are made within the next 5 seconds. Splunk observed this error while testing with three shards only every 1 to 5 minutes.

Configure Generic S3 inputs for the Splunk Add-on for AWS

Complete the steps to configure Generic S3 inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Generic S3 input.
3. Configure AWS permissions for the Generic S3 input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure Generic S3 inputs either through Splunk Web or configuration files.

The Generic S3 input lists all the objects in the bucket and examines each file's modified date every time it runs to pull uncollected data from an S3 bucket. When the number of objects in a bucket is large, this can be a very time-consuming process with low throughput.

Before you begin configuring your Generic S3 inputs, be aware of the following expected behaviors:

1. You cannot edit the initial scan time parameter of an S3 input after you create it. If you need to adjust the start time of an S3 input, delete it and recreate it.
2. The S3 data input is not intended to read frequently modified files. If a file is modified after it has been indexed, the Splunk platform indexes the file again, resulting in duplicated data. Use key, blocklist, and allowlist options to instruct the add-on to index only those files that you know will not be modified later.
3. The S3 data input processes compressed files according to their suffixes. Use these suffixes only if the file is in the corresponding format, or data processing errors occur. The data input supports the following compression types:

   - single file in ZIP, GZIP, TAR, or TAR.GZ formats
   - multiple files with or without folders in ZIP, TAR, or TAR.GZ format

Expanding compressed files requires significant operating system resources. The Splunk platform automatically detects the character set used in your files among these options:

- The Splunk platform auto-detects the character set used in your files among these options:

  - UTF-8 with or without BOM
  - UTF-16LE/BE with BOM
  - UTF-32BE/LE with BOM.

  If your S3 key uses a different character set, you can specify it in inputs.conf using the `character_set` parameter and separate out this collection job into its own input. Mixing non-autodetected character sets in a single input causes errors..
- If your S3 bucket contains a very large number of files, you can configure multiple S3 inputs for a single S3 bucket to improve performance. The Splunk platform dedicates one process for each data input, so provided that your system has sufficient processing power, performance improves with multiple inputs. See "Performance for the Splunk Add-on for AWS data inputs" in Sizing, Performance, and Cost Considerations for the Splunk Add-on for AWS for details.

To prevent indexing duplicate data, verify that multiple inputs do not collect the same S3 folder and file data.

- As a best practice, archive your S3 bucket contents when you no longer need to actively collect them. AWS charges for list key API calls that the input uses to scan your buckets for new and changed files so you can reduce costs and improve performance by archiving older S3 keys to another bucket or storage type.
- After configuring an S3 input, you may need to wait for a few minutes before new events are ingested and can be searched. The wait time depends on the number of files in the S3 buckets from which you are collecting data. The larger the quantity files, the longer the delay. Also, more verbose logging levels causes longer data digestion time.

Configure AWS services for the Generic S3 input

To collect access logs, configure logging in the AWS console to collect the logs in a dedicated S3 bucket. See the AWS documentation for more information on how to configure access logs:

- For S3 access logs, see http://docs.aws.amazon.com/AmazonS3/latest/dev/ServerLogs.html.

- For ELB access logs, see http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/enable-access-logs.html.
- For CloudFront access logs, see http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html.

See http://docs.aws.amazon.com/gettingstarted/latest/swh/getting-started-create-bucket.html for more information about how to configure S3 buckets and objects.

Refer to the AWS S3 documentation for more information about how to configure S3 buckets and objects: http://docs.aws.amazon.com/gettingstarted/latest/swh/getting-started-create-bucket.html

Configure S3 permissions

Required permissions for S3 buckets and objects:

- `ListBucket`
- `GetObject`
- `ListAllMyBuckets`
- `GetBucketLocation`

Required permissions for KMS:

- `Decrypt`

In the Resource section of the policy, specify the Amazon Resource Names (ARNs) of the S3 buckets from which you want to collect S3 Access Logs, CloudFront Access Logs, ELB Access Logs, or generic S3 log data.

See the following sample inline policy to configure S3 input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetObject",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html.

Configure a Generic S3 input using Splunk Web

To configure inputs in Splunk Web, click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home, then choose one of the following menu paths depending on which data type you want to collect:

- **Create New Input > CloudTrail > Generic S3**

- **Create New Input > CloudFront Access Log > Generic S3**
- **Create New Input > ELB Access Logs > Generic S3**
- **Create New Input > S3 Access Logs > Generic S3**
- **Create New Input > Custom Data Type > Generic S3**

Make sure you choose the right menu path corresponding to the data type you want to collect. The system automatically sets the appropriate source type and may display slightly different field settings in the subsequent configuration page based on the menu path.

Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access the keys in your S3 buckets. In Splunk Web, select an account from the drop-down list. In inputs.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role. If the region of the AWS account you select is **GovCloud**, you might encounter errors suc as "Failed to load options for S3 Bucket". You need to manually add **AWS GovCloud Endpoint** in the **S3 Host Name** field. See http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-govcloud-endpoints.htm for more information.
`aws_iam_role`	Assume Role	The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.
`aws_s3_region`	AWS Region (Optional)	The AWS region that contains your bucket. In inputs.conf, enter the region ID. Provide an AWS Region only if you want to use specific regional endpoints instead of public endpoints for data collection. See the **AWS service endpoints** topic in the AWS General Reference manual for more information.
`private_endpoint_enabled`	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Cloud Storage (S3) services for authentication and data collection. In inputs.conf, enter `0` or `1` to respectively disable or enable use of private endpoints.

`s3_private_endpoint_url`	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from your AWS console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.amazonaws.com`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3.<region_id>.vpce.amazonaws.com`

`sts_private_endpoint_url`	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AWS console. Supported Formats : `<http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaws.co`

Argument in configuration file	Field in Splunk Web	Description
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<region_id>.vpce.amazonaws.com`
`bucket_name`	S3 Bucket	The AWS bucket name.
`log_file_prefix`	Log File Prefix/S3 Key Prefix	Configure the prefix of the log file. This add-on searches the log files under this prefix. This argument is titled **Log File Prefix** in incremental S3 field inputs, and is titled **S3 Key Prefix** in generic S3 field inputs.
`log_start_date`	Start Date/Time	The start date of the log.
`log_end_date`	End Date/Time	The end date of the log.
`sourcetype`	Source Type	A source type for the events. Specify only if you want to override the default of `aws:s3`. You can select a source type from the drop-down list or type a custom source type yourself. To index access logs, enter `aws:s3:accesslogs`, `aws:cloudfront:accesslogs`, or `aws:elb:accesslogs`, depending on the lo types in the bucket. To index CloudTrail events directly from an S3 bucket, change the source type to `aws:cloudtrail`.
`index`	Index	The index name where the Splunk platform puts the S3 data. The default is main.
`ct_blacklist`	CloudTrail Event Blacklist	Only valid if the source type is set to `aws:cloudtrail`. A Pearl Compatible Regex Expression (PCRE) regular expression that specifies event names to exclude. The default regex is `^$` to exclude events that car produce a high volume of data. Leave it blank if you want all data to be indexed.
`blacklist`	CloudTrail Event Blacklist	\.bin$).
`polling_interval`	Polling Interval	The number of seconds to wait before the Splunk platform runs the command again. The default is 1,800 seconds.

Configure a Generic S3 input using configuration files

When you configure inputs manually in `inputs.conf`, create a stanza using the following template and add it to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf`. If the file or path does not exist, create it.

```
[aws_s3://<name>]
is_secure = <whether use secure connection to AWS>
host_name = <the host name of the S3 service>
aws_account = <AWS account used to connect to AWS>
aws_s3_region = <value>
private_endpoint_enabled = <value>
s3_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
bucket_name = <S3 bucket name>
polling_interval = <Polling interval for statistics>
key_name = <S3 key prefix>. For example, key_name = cloudtrail. This value does not accept regex.
recursion_depth = <For folder keys, -1 == unconstrained>
initial_scan_datetime = <Splunk relative time>
terminal_scan_datetime = <Only S3 keys which have been modified before this datetime will be considered.
Using datetime format: %Y-%m-%dT%H:%M:%S%z (for example, 2011-07-06T21:54:23-0700).>
log_partitions = AWSLogs/<Account ID>/CloudTrail/<Region>
max_items = <Max trackable items.>
max_retries = <Max number of retry attempts to stream incomplete items.>
whitelist = <Override regex for blacklist when using a folder key.>. For example, whitelist =
```

```
^.\/cloudtrail2\/.$. Regex should match the full path.
blacklist = <Keys to ignore when using a folder key.>. Regex should match the full path.
character_set = <The encoding used in your S3 files. Default to 'auto' meaning that file encoding will be
detected automatically amoung UTF-8, UTF8 without BOM, UTF-16BE, UTF-16LE, UTF32BE and UTF32LE. Notice that
once one specified encoding is set, data input will only handle that encoding.>
ct_blacklist = <The blacklist to exclude cloudtrail events. Only valid when manually set
sourcetype=aws:cloudtrail.>
ct_excluded_events_index = <name of index to put excluded events into. default is empty, which discards the
events>
aws_iam_role = <AWS IAM role to be assumed>
```

Under one AWS account, to ingest logs in different prefixed locations in the bucket, you need to configure multiple AWS data inputs, one for each prefix name. Alternatively, you can configure one data input but use different AWS accounts to ingest logs in different prefixed locations in the bucket.

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_s3]
aws_account =
sourcetype = aws:s3
initial_scan_datetime = default
log_partitions = AWSLogs/<Account ID>/CloudTrail/<Region>
max_items = 100000
max_retries = 3
polling_interval=
interval = 30
recursion_depth = -1
character_set = auto
is_secure = True
host_name = s3.amazonaws.com
ct_blacklist = ^(?:Describe|List|Get)
ct_excluded_events_index =
```

Configure SQS inputs for the Splunk Add-on for AWS

Complete the steps to configure SQS inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the SQS input.
3. Configure AWS permissions for the SQS input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure SQS inputs either through Splunk Web or configuration files.

Configure AWS services for the SQS input

If you plan to use the SQS input, you must perform the following:

- Set up a dead-letter queue for the SQS queue to be used for the input for storing invalid messages. For information about SQS dead-letter queues and how to configure it, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-dead-letter-queues.html.
- Configure the SQS visibility timeout to prevent multiple inputs from receiving and processing messages in a queue more than once. Set your SQS visibility timeout to 5 minutes or longer. If the visibility timeout for a message is reached before the message is fully processed by the SQS input, the message reappears in the queue and is retrieved and processed again, resulting in duplicate data.

For information about SQS visibility timeout and how to configure it, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/sqs-visibility-timeout.html.

Configure AWS permissions for the SQS input

Required permissions for Amazon SQS:

- `GetQueueAttributes`
- `ListQueues`
- `ReceiveMessage`
- `GetQueueUrl`
- `SendMessage`
- `DeleteMessage`.

See the following sample inline policy to configure SQS input permissions:

```
{
â  â  "Version": "2012-10-17",
â  â  "Statement": [
â  â  â  â  {
â  â  â  â  â  â  "Effect": "Allow",
â  â  â  â  â  â  "Action": [
â  â  â  â  â  â  â  â  "sqs:GetQueueAttributes",
â  â  â  â  â  â  â  â  "sqs:ListQueues",
â  â  â  â  â  â  â  â  "sqs:ReceiveMessage",
â  â  â  â  â  â  â  â  "sqs:GetQueueUrl",
â  â  â  â  â  â  â  â  "sqs:SendMessage",
â  â  â  â  â  â  â  â  "sqs:DeleteMessage"
â  â  â  â  â  â  ],
â  â  â  â  â  â  "Resource": [
â  â  â  â  â  â  â  â  "*"
â  â  â  â  â  â  ]
â  â  â  â  }
â  â  ]
}
```

Configure an SQS input using Splunk Web

To configure inputs using Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.
2. Click **Create New Input > Custom Data Type > SQS**.
3. Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your SQS data. In Splunk Web, select an account from the drop-down list. In aws_sqs_tasks.conf, enter the friendly name of one of the AWS accounts that you configured on the Configuration page or the name of the automatically discovered EC2 IAM role.
`aws_region`	AWS Region	The AWS region that contains the log notification SQS queue. In aws_sqs_tasks.conf, enter the region code. For example, the region code for the US East region is us-east-2. See https://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.

Argument in configuration file	Field in Splunk Web	Description
`sqs_queues`	SQS queues	The name of the queue to which AWS sends new SQS log notifications. In Splunk Web, you can select a queue from the drop-down list, if your account permissions allow you to list queues, or enter the queue name manually. The queue name is the final segment of the full queue URL. For example, if your SQS queue URL is `http://sqs.us-east-1.amazonaws.com/123456789012/testQueue`, then your SQS queue name is `testQueue`. You can add multiple queues separated by commas.
`sourcetype`	Source type	A source type for the events. Enter a value only if you want to override the default of `aws:sqs`. Event extraction relies on the default value of source type. If you change the default value, you must update props.conf as well.
`index`	Index	The index name where the Splunk platform puts the SQS data. The default is main.
`interval`	Interval	The number of seconds to wait before the Splunk platform runs the command again. The default is 30 seconds.

Configure an SQS input using configuration files

To configure the input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_sqs_tasks.conf` using the following template:

```
[<name>]
aws_account = <value>
aws_region = <value>
sqs_queues = <value>
index = <value>
sourcetype = <value>
interval = <value>
```

Configure SQS-based S3 inputs for the Splunk Add-on for AWS

Complete the steps to configure SQS-based S3 inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the SQS-based S3 input.
3. Configure AWS permissions for the SQS-based S3 input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. (Optional) Configure VPC Interface Endpoints for STS, SQS, and S3 services from your AWS Console if you want to use private endpoints for data collection and authentication. For more information, see the **Interface VPC endpoints (AWS PrivateLink)** topic in the Amazon Virtual Private Cloud documentation.
5. Configure SQS-based S3 inputs either through Splunk Web or configuration files.

Configure AWS services for the SQS-based S3 input

Configure SQS-based S3 inputs to collect the following events:

- CloudFront Access Logs
- Config
- ELB Access logs
- CloudTrail
- S3 Access Logs

- Custom data types

Before you configure SQS-based S3 inputs, perform the following tasks:

- Configure S3 to send notifications to SQS. This lets S3 notify the add-on that new events were written to the S3 bucket.
- Subscribe to the corresponding SNS Topic.

Keep the following in mind as you configure your inputs:

- The SQS-based S3 input only collects in AWS service logs that meet the following criteria:
  - Near-real time
  - Newly created
  - Stored into S3 buckets
  - Has event notifications sent to SQS

Events that occurred in the past, or events with no notifications sent through SNS to SQS end up in the Dead Letter Queue (DLQ), and no corresponding event is created by the Splunk Add-on for AWS. To collect historical logs stored into S3 buckets, use the generic S3 input instead. The S3 input lets you set the initial scan time parameter to collect data generated after a specified time in the past.

- To collect the same types of logs from multiple S3 buckets, even across regions, set up one input to collect data from all the buckets. To do this, configure these buckets to send notifications to the same SQS queue from which the SQS-based S3 input polls message.
- To achieve high throughput data ingestion from an S3 bucket, configure multiple SQS-based S3 inputs for the S3 bucket to scale out data collection.
- After configuring an SQS-based S3 input, you might need to wait for a few minutes before new events are ingested and can be searched. Also, a more verbose logging level causes longer data digestion time. Debug mode is extremely verbose and is not recommended on production systems.
- The SQS-based input allows you to ingest data from S3 buckets by optimizing the API calls made by the add-on and relying on SQS/SNS to collect events upon receipt of notification.
- The SQS-based S3 input is stateless, which means that when multiple inputs are collecting data from the same bucket, if one input goes down, the other inputs continue to collect data and take over the load from the failed input. This lets you enhance fault tolerance by configuring multiple inputs to collect data from the same bucket.

- The SQS-based S3 input supports signature validation. If S3 notifications are set up to send through SNS, AWS will create a signature for every message. The SQS-based S3 input will validate each message with the associated certificate, provided by AWS. For more information, see the *Verifying the signatures of Amazon SNS messages* topic in the AWS documentation.
- If any messages with a signature are received, all following messages will require valid SNS signatures, no matter your input's SNS signature setting.
- Set up a Dead Letter Queue for the SQS queue to be used for the input for storing invalid messages. For information about SQS Dead Letter Queues and how to configure it, see the *Amazon SQS dead-letter queues* topic in the AWS documentation.
- Configure the SQS visibility timeout to prevent multiple inputs from receiving and processing messages in a queue more than once. Set your SQS visibility timeout to 5 minutes or longer. If the visibility timeout for a message is reached before the message is fully processed by the SQS-based S3 input, the message reappears in the queue and is retrieved and processed again, resulting in duplicate data.

For information about SQS visibility timeout and how to configure it, see the *Amazon SQS visibility timeout* topic in the AWS documentation.

Configure AWS permissions for the SQS-based S3 input

Required permissions for SQS:

- `GetQueueUrl`
- `ReceiveMessage`
- `SendMessage`
- `DeleteMessage`
- `GetQueueAttributes`
- `ListQueues`

Required permissions for S3 buckets and objects:

- `GetObject`

Required permissions for KMS:

- `Decrypt`

See the following sample inline policy to configure Inspector input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sqs:GetQueueUrl",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "s3:GetObject",
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information and sample policies, see http://docs.aws.amazon.com/AmazonS3/latest/dev/using-iam-policies.html.

Configure an SQS-based S3 input using Splunk Web

To configure inputs in Splunk Web, click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home, then choose one of the following menu paths depending on which data type you want to collect:

- **Create New Input > CloudTrail > SQS-based S3**
- **Create New Input > CloudFront Access Log > SQS-based S3**
- **Create New Input > Config > SQS-based S3**
- **Create New Input > ELB Access Logs > SQS-based S3**
- **Create New Input > S3 Access Logs > SQS-based S3**
- **Create New Input > Custom Data Type > SQS-based S3**

You must have the admin_all_objects role enabled in order to add new inputs.

Choose the menu path that corresponds to the data type you want to collect. The system automatically sets the source type and display relevant field settings in the subsequent configuration page.

Use the following table to complete the fields for the new input in the .conf file or in Splunk Web:

Argument in configuration file	Field in Splunk Web	Description
`aws_account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access the keys in your S3 buckets. I Splunk Web, select an account from the drop-down list. In inputs.conf, enter the friendly name of one AWS accounts that you configured on the Configuration page or the name of the automatically discov EC2 IAM role. If the region of the AWS account you select is **GovCloud**, you may encounter errors as"Failed to load options for S3 Bucket". You need to manually add **AWS GovCloud Endpoint** in the **S3 Host Name** field. See http://docs.aws.amazon.com/govcloud-us/latest/UserGuide/using-govcloud-endpoint for more information.
`aws_iam_role`	Assume Role	The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.
`using_dlq`	Force using DLQ (Recommended)	Check the checkbox to remove the checking of DLQ (Dead Letter Queue) for ingestion of specific dat inputs.conf, enter `0` or `1` to respectively disable or enable the checking. (Default value is `1`)
`sqs_queue_region`	AWS Region	AWS region that the SQS queue is in.
`private_endpoint_enabled`	Use Private Endpoints	Check the checkbox to use private endpoints of AWS Security Token Service (STS) and AWS Simple Storage (S3) services for authentication and data collection. In inputs.conf, enter `0` or `1` to respectively disable or enable use of private endpoints.

`sqs_private_endpoint_url`	Private Endpoint URL (SQS)	Private Endpoint (Interface VPC Endpoint) of your SQS service, which can be configured from your A console.
		
		Supported Formats :
		`<http/https>://vpce-<endpoint_id>-<unique_id>.sqs.<region_id>.vpce.amazonaw`
		`<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sqs.<regi _id>.vpce.amazonaws.com`

`sqs_sns_validation`	SNS Signature Validation	SNS validation of your SQS messages, which can be configured from your AWS console. If selected, messages will be validated. If unselected, then messages will not be validated until receiving a signed message. Thereafter, all messages will be validated for an SNS signature. For new SQS-based S3 in this feature is enabled, by default. Supported Formats : `1` is enabled, `0` is disabled. Default is `1`
`s3_private_endpoint_url`	Private Endpoint URL (S3)	Private Endpoint (Interface VPC Endpoint) of your S3 service, which can be configured from your AW console. Supported Formats : `<http/https>://vpce-<endpoint_id>-<unique_id>.s3.<region_id>.vpce.amazonaws`

Argument in configuration file	Field in Splunk Web	Description
		<http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.s3.<regio _id>.vpce.amazonaws.com
sts_private_endpoint_url	Private Endpoint URL (STS)	Private Endpoint (Interface VPC Endpoint) of your STS service, which can be configured from your AW console. Supported Formats : <http/https>://vpce-<endpoint_id>-<unique_id>.sts.<region_id>.vpce.amazonaw <http/https>://vpce-<endpoint_id>-<unique_id>-<availability_zone>.sts.<regi _id>.vpce.amazonaws.com
sqs_queue_url	SQS Queue Name	The SQS queue URL.
sqs_batch_size	SQS Batch Size	The maximum number of messages to pull from the SQS queue in one batch. Enter an integer betwe and 10 inclusive. Set a larger value for small files, and a smaller value for large files. The default SQS size is 10. If you are dealing with large files and your system memory is limited, set this to a smaller va
s3_file_decoder	S3 File Decoder	The decoder to use to parse the corresponding log files. The decoder is set according to the **Data Typ** select. If you select a **Custom Data Type**, choose one from `Cloudtrail`, `Config`, `ELB Access Lo` `Access Logs`, or `CloudFront Access Logs`.
sourcetype	Source Type	The source type for the events to collect, automatically filled in based on the decoder chosen for the in
interval	Interval	The length of time in seconds between two data collection runs. The default is 300 seconds.
index	Index	The index name where the Splunk platform puts the SQS-based S3 data. The default is main.

Configure an SQS based S3 input for CrowdStrike Falcon Data Replicator (FDR) events using Splunk Web

To configure an SQS based S3 input for CrowdStrike Falcon Data Replicator (FDR) events, perform the following steps:

1. On the **Inputs** page, select "Create New Input" > "Custom Data Type" > "SQS-Based S3".
2. Select your AWS Account the account from the dropdown list.
3. Uncheck the check box **Force Using DLQ (Recommended)**.
4. Select the region in which the SQS Queue is present from the **AWS Region** dropdown.
5. In the **SQS Queue Name** box, enter the full SQS queue URL. This will create a option for the SQS queue URL in the dropdown menu.
6. Select the newly created SQS queue URL option from the **SQS Queue Name** dropdown menu.
7. Use the table in the **Configure an SQS-based S3 input using Splunk Web** section of this topic to add any additional configuration file arguments.
8. Save your changes.

Configure an SQS-based S3 input using configuration files

When you configure inputs manually in inputs.conf, create a stanza using the following template and add it to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/inputs.conf`. If the file or path does not exist, create it.

```
[aws_sqs_based_s3://<stanza_name>]
aws_account = <value>
```

```
using_dlq = <value>
private_endpoint_enabled = <value>
sqs_private_endpoint_url = <value>
s3_private_endpoint_url = <value>
sts_private_endpoint_url = <value>
interval = <value>
s3_file_decoder = <value>
sourcetype = <value>
sqs_batch_size = <value>
sqs_queue_region = <value>
sqs_queue_url = <value>
```

Some of these settings have default values that can be found in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/default/inputs.conf`:

```
[aws_sqs_based_s3]
using_dlq = 1
```

The previous values correspond to the default values in Splunk Web, as well as some internal values that are not exposed in Splunk Web for configuration. If you copy this stanza to your `$SPLUNK_HOME/etc/apps/Splunk_TA_aws//local` and use it as a starting point to configure your inputs.conf manually, change the `[aws_sqs_based_s3]` stanza title from `aws_sqs_based_s3` to `aws_sqs_based_s3://<name>` and add the additional parameters that you need for your deployment.

Valid values for `s3_file_decoder` are CloudTrail, Config, S3 Access Logs, ELB Access Logs, CloudFront Access Logs, and CustomLogs.

If you want to ingest custom logs other than the natively supported AWS log types, you must set `s3_file_decoder = CustomLogs`. This setting lets you ingest custom logs into the Splunk platform instance, but it does not parse the data. To process custom logs into meaningful events, you need to perform additional configurations in props.conf and transforms.conf to parse the collected data to meet your specific requirements.

For more information on these settings, see `/README/inputs.conf.spec` under your add-on directory.

Migrate from the Generic S3 input to the SQS-based S3 input

SQS-based S3 is the recommended input type for real-time data collection from S3 buckets because it is scalable and provides better ingestion performance than the other S3 input types.

If you are already using a generic S3 input to collect data, use the following steps to switch to the SQS-based S3 input:

1. Perform prerequisite configurations of AWS services:
    - Set up an SQS queue with a Dead Letter Queue and proper visibility timeout configured. See Documentation:AddOns:AWS:SQS-basedS3.
    - Set up the S3 bucket with the S3 key prefix, if specified, from which you are collecting data to send notifications to the SQS queue. See Configure alerts for the Splunk Add-on for AWS.
2. Add an SQS-based S3 input using the SQS queue you just configured. After the setup, make sure the new input is enabled and starts collecting data from the bucket.

   https://docs.splunk.com/Documentation/AddOns/released/AWS/Inspector
3. Edit your old generic S3 input and set the **End Date/Time** field to the current system time to phase it out.
4. Wait until all the task executions of the old input are complete. As a best practice, wait at least double your polling frequency.
5. Disable the old generic S3 input.

6. Run the following searches to delete any duplicate events collected during the transition: For CloudTrail events:

```
index=xxx sourcetype=aws:cloudtrail | streamstats count by source, eventID | search count > 1 | eval
indexed_time=strftime(_indextime, "%+") | eval dup_id=source.eventID.indexed_time | table dup_id |
outputcsv dupes.csv

index=xxx sourcetype=aws:cloudtrail | eval indexed_time=strftime(_indextime, "%+") | eval
dup_id=source.eventID.indexed_time | search [|inputcsv dupes.csv | format "(" "" "" "" "OR" ")"] |
delete
```

   For S3 access logs:

```
index=xxx sourcetype=aws:s3:accesslogs | streamstats count by source, request_id | search count > 1
| eval indexed_time=strftime(_indextime, "%+") | eval dup_id=source.request_id.indexed_time | table
dup_id | outputcsv dupes.csv

index=xxx sourcetype=aws:s3:accesslogs | eval indexed_time=strftime(_indextime, "%+") | eval
dup_id=source.request_id.indexed_time | search [|inputcsv dupes.csv | format "(" "" "" "" "OR" ")"]
| delete
```

   For CloudFront access logs:

```
index=xxx sourcetype=aws:cloudfront:accesslogs | streamstats count by source, x_edge_request_id |
search count > 1 | eval indexed_time=strftime(_indextime, "%+") | eval
dup_id=source.x_edge_request_id.indexed_time | table dup_id | outputcsv dupes.csv

index=xxx sourcetype=aws:cloudfront:accesslogs | eval indexed_time=strftime(_indextime, "%+") | eval
dup_id=source.x_edge_request_id.indexed_time | search [|inputcsv dupes.csv | format "(" "" "" ""
"OR" ")"] | delete
```

   For classic load balancer (elb) access logs:

   Because events do not have unique IDs, use the hash function to remove duplication.

```
index=xxx sourcetype=aws:elb:accesslogs | eval hash=sha256(_raw) | streamstats count by source, hash
| search count > 1 | eval indexed_time=strftime(_indextime, "%+") | eval
dup_id=source.hash.indexed_time | table dup_id | outputcsv dupes.csv

index=xxx sourcetype=aws:elb:accesslogs | eval hash=sha256(_raw) | eval
indexed_time=strftime(_indextime, "%+") | eval dup_id=source.hash.indexed_time | search [|inputcsv
dupes.csv | format "(" "" "" "" "OR" ")"] | delete
```

7. Optionally, delete the old generic S3 input.

Automatically scale data collection with SQS-based S3 inputs

With the SQS-based S3 input type, you can take full advantage of the auto-scaling capability of the AWS infrastructure to scale out data collection by configuring multiple inputs to ingest logs from the same S3 bucket without creating duplicate events. This is particularly useful if you are ingesting logs from a very large S3 bucket and hit a bottleneck in your data collection inputs.

1. Create an AWS auto scaling group for your heavy forwarder instances where the SQS-based S3 inputs is running.
   To create an auto-scaling group, you can either specify a launch configuration or create an AMI to provision new EC2 instances that host heavy forwarders, and use bootstrap script to install the Splunk Add-on for AWS and configure SQS-based S3 inputs. For detailed information about the auto-scaling group and how to create it, see

http://docs.aws.amazon.com/autoscaling/latest/userguide/AutoScalingGroup.html.
2. Set CloudWatch alarms for one of the following Amazon SQS metrics:
    - **ApproximateNumberOfMessagesVisible**: The number of messages available for retrieval from the queue.
    - **ApproximateAgeOfOldestMessage**: The approximate age (in seconds) of the oldest non-deleted message in the queue.

   For instructions on setting CloudWatch alarms for Amazon SQS metrics, see http://docs.aws.amazon.com/AWSSimpleQueueService/latest/SQSDeveloperGuide/SQS_AlarmMetrics.html.
3. Use the CloudWatch alarm as a trigger to provision new heavy forwarder instances with SQS-based S3 inputs configured to consume messages from the same SQS queue to improve ingestion performance.

Configure miscellaneous inputs for the Splunk Add-on for AWS

You can configure miscellaneous Amazon Web Services (AWS) if they integrate with an input that the Splunk Add-on for AWS provides. For example, GuardDuty integrates with CloudWatch. You can index GuardDuty data through the Splunk Add-on for AWS CloudWatch input. Check to see if your intended AWS service integrates with CloudWatch, CloudWatch Logs, or Kinesis. See the following examples:

- https://www.splunk.com/en_us/blog/cloud/how-to-easily-stream-aws-cloudwatch-logs-to-splunk.html
- https://www.splunk.com/en_us/blog/tips-and-tricks/how-to-ingest-any-log-from-aws-cloudwatch-logs-via-firehose.html
- https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html

Configure Metadata inputs for the Splunk Add-on for AWS

The Description input will be deprecated in a future release. The Metadata input has been added as a replacement. The best practice is to begin moving your workloads to the Metadata input.

Complete the steps to configure Metadata inputs for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for the Metadata input.
3. Configure AWS permissions for the Metadata input. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Configure Metadata inputs either through Splunk Web or configuration files.

Configure Metadata permissions

Required permissions for EC2 resources: `DescribeInstances, DescribeReservedInstances, DescribeSnapshots, DescribeRegions, DescribeKeyPairs, DescribeNetworkAcls, DescribeSecurityGroups, DescribeSubnets, DescribeVolumes, DescribeVpcs, DescribeImages, DescribeAddresses`

Required permissions for Lambda: `ListFunctions`

Required permissions for RDS: `DescribeDBInstances`

Required permissions for CloudFront, if you are in a region that supports CloudFront: `ListDistributions`

Required permissions for ELB: `DescribeLoadBalancers, DescribeInstanceHealth, DescribeTags, DescribeTargetGroups, DescribeTargetHealth`

Required permissions for S3: `ListAllMyBuckets, GetAccelerateConfiguration, GetBucketCORS, GetLifecycleConfiguration, GetBucketLocation, GetBucketLogging, GetBucketTagging`

See the following sample inline policy to configure Metadata input permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeReservedInstances",
        "ec2:DescribeSnapshots",
        "ec2:DescribeRegions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:DescribeVpcs",
        "ec2:DescribeImages",
        "ec2:DescribeAddresses",
        "lambda:ListFunctions",
        "rds:DescribeDBInstances",
        "cloudfront:ListDistributions",
        "iam:GetUser",
        "iam:ListUsers",
        "iam:GetAccountPasswordPolicy",
        "iam:ListAccessKeys",
        "iam:GetAccessKeyLastUsed",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeListeners",
        "s3:ListAllMyBuckets",
        "s3:GetAccelerateConfiguration",
        "s3:GetBucketCORS",
        "s3:GetLifecycleConfiguration",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketTagging"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Configure a Metadata input using Splunk Web

To configure inputs in Splunk Web:

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web home.

2. Click **Create New Input > Description > Metadata**.
3. Fill out the fields as described in the following table:

Argument in configuration file	Field in Splunk Web	Description
`account`	AWS Account	The AWS account or EC2 IAM role the Splunk platform uses to access your Metadata data. In Splunk Web, select an acc In `aws_metadata_tasks.conf`, enter the friendly name of one of the AWS accounts that you configured on the Config the automatically discovered EC2 IAM role.
`regions`	AWS Regions	The AWS regions for which you are collecting Metadata data. In Splunk Web, select one or more regions from the drop-d aws_metadata_tasks.conf, enter one or more valid AWS region IDs, separated by commas. See https://docs.aws.amazon.com/general/latest/gr/rande.html#d0e371.
`apis`	APIs/Interval (seconds)	APIs you want to collect data from, and intervals for each API, in the format of <api name>/<api interval in seconds>,<api seconds>. The default value in Splunk Web is `ec2_volumes/3600,ec2_instances/3600,ec2_reserved_instances/3600,ebs_snapshots/3600,elasti /3600,vpcs/3600,vpc_network_acls/3600,cloudfront_distributions/3600,vpc_subnets/3600,rds_ _pairs/3600,ec2_security_groups/3600` . This value collects from all of the APIs supported in this release. Set your intervals to 3,600 seconds (1 hour) or longer t
`aws_iam_role`	Assume Role	The IAM role to assume, see Manage accounts for the Splunk Add-on for AWS.
`sourcetype`	Source type	A source type for the events. Enter `aws:metadata`.
`index`	Index	The index name where the Splunk platform puts the Metadata data. The default is main.

Configure a Metadata input using configuration files

To configure a Metadata input using configuration files, create `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local/aws_metadata_tasks.conf` using the following template:

```
[<name>]
account = <value>
regions = <values split by commas>
apis = <value>
aws_iam_role = <value>
sourcetype = <value>
index = <value>
```

Here is an example stanza that collects metadata data from all supported APIs:

```
[desc:splunkapp2]
account = splunkapp2
regions = us-west-2
apis = ec2_volumes/3600, ec2_instances/3600, ec2_reserved_instances/3600, ebs_snapshots/3600,
classic_load_balancers/3600, application_load_balancers/3600, vpcs/3600, vpc_network_acls/3600,
cloudfront_distributions/3600, vpc_subnets/3600, rds_instances/3600, ec2_key_pairs/3600,
ec2_security_groups/3600, ec2_images/3600, ec2_addresses/3600, lambda_functions/3600, s3_buckets/3600,
iam_users/3600
aws_iam_role = iam_users
sourcetype = aws:metadata
index = default
```

Alert configuration

Configure alerts for the Splunk Add-on for AWS

Complete the steps to configure and use the Simple Notification Service (SNS) alerts for the Splunk Add-on for Amazon Web Services (AWS):

1. You must manage accounts for the add-on as a prerequisite. See Manage accounts for the Splunk Add-on for AWS.
2. Configure AWS services for SNS alerts.
3. Configure AWS permissions for SNS alerts. You can skip this step and configure AWS permissions at once, if you prefer. See Configure AWS permissions for all Splunk Add-on for AWS inputs at once.
4. Create an SNS alert search.
5. Use the alert action.

To use the search commands and alert actions included with the Splunk Add-on for AWS, you must either be an administrator or a user with the appropriate capability:

- `list_storage_passwords` if you are using Splunk Enterprise 6.5.0 or higher.
- `admin_all_objects` if you are using a version of Splunk Enterprise lower than 6.5.0.

This functionality is not supported in Splunk Cloud, due to security policy conflicts.

Configure AWS services for SNS alerts

If you plan to use the SQS-based S3 input, you must enable Amazon S3 bucket events to send notification messages to an SQS queue whenever the events occur. This queue cannot be first-in-first-out. For instructions on setting up S3 bucket event notifications, see the AWS documentation:
https://docs.aws.amazon.com/AmazonS3/latest/UG/SettingBucketNotifications.html
http://docs.aws.amazon.com/AmazonS3/latest/dev/NotificationHowTo.html

Configure AWS permissions for SNS alerts

Required permissions for Amazon SNS:

- `Publish`
- `Get*`
- `List*`

```
See the following sample inline policy to configure SNS alert permissions:
{
â  â  "Version": "2012-10-17",
â  â  "Statement": [
â  â  â  â  {
â  â  â  â  â  â  "Effect": "Allow",
â  â  â  â  â  â  "Action": [
â  â  â  â  â  â  â  â  "sns:Publish",
â  â  â  â  â  â  â  â  "sns:Get*",
â  â  â  â  â  â  â  â  "sns:List*"
```

```
â  â  â  â  â  â  ],
â  â  â  â  â  â  "Resource": "*"
â  â  â  â  }
â  â  ]
}
```

Use the awssnsalert search command

Use the search command, `awssnsalert`, to send alerts to AWS SNS.

The following example search demonstrates how to use this search command:

```
...| eval message="My Message" | eval entity="My Entity" | eval correlation_id="1234567890" | awssnsalert
account=real region="ap-southeast-1" topic_name="ta-aws-sns-ingestion" publish_all=1
```

Use the following table to create an SNS alert search. All attributes are required:

Attribute	Description
`account`	The AWS account name configured in the add-on.
`region`	The AWS region name.
`topic_name`	The alert message is sent to this AWS SNS topic name.
`message`	The message that the Splunk Add-on for AWS sends to AWS SNS.
`publish_all`	You can set `publish_all` to 0 or 1. If you set `publish_all=1`, the add-on sends all the records in this search. If you set `publish_all=0`, the add-on sends only the first result to the search. The default value of this field is 0.

Use the alert action

The Splunk Add-on for AWS supports automatic incident and event creation and incident update from custom alert actions. Custom alert actions are available in Splunk Enterprise version 6.3.0 and higher.

To create a new incident or event from a custom alert action, follow these steps:

1. In Splunk Web, navigate to the **Search & Reporting** app.
2. Write a search string that you want to use to trigger incident or event creation in AWS SNS.

   Click **Save As > Alert**.
3. Fill out the Alert form. Give your alert a unique name and indicate whether the alert is a real-time alert or a scheduled alert. See Getting started with alerts in the *Alerting Manual* for more information.
4. Under Trigger Actions, click **Add Actions**.
5. From the list, select **AWS SNS Alert** if you want the alert to create an event in AWS SNS.
6. Enter values for all required fields, as shown in the following table:

Field	Description
Account	Required. The account name configured in Splunk Add-on for AWS.
Region	Required. The region of AWS SNS the events are sent to. Make sure the region is consistent with AWS SNS.
Topic Name	Required. The name of the topic the events are sent to. Make sure the topic name exists in AWS SNS.
Correlation ID	Optional. The ID that correlates this alert with the other events. If you leave this field empty, it uses `$result.correlation_id$` by default.
Entity	Optional. The object related to the event or alert, such as host, database, or EC2 instance. If you leave this field empty, Splunk Enterprise uses `$result.entity$` by default.

Field	Description
Source	Optional. The source of the event or alert. If you leave this field empty, Splunk Enterprise uses `$result.source$` by default.
Timestamp	Optional. The time of the event occurs. If you leave this field empty, the Splunk Enterprise uses `$result._time$` by default.
Event	Optional. The details of the event. If you leave this field empty, the Splunk Enterprise uses `$result._raw$` by default.
Message	Required. The message that the Splunk Add-on for AWS sends to AWS SNS.

Troubleshooting

Troubleshoot the Splunk Add-on for AWS

Use the following information to troubleshoot the Splunk Add-on for Amazon Web Services (AWS). For helpful troubleshooting tips that you can apply to all add-ons see Troubleshoot add-ons, and Support and resource links for add-ons in the *Splunk Add-ons* manual.

Data collection errors and performance issues

You can choose dashboards from the Health Check menu to troubleshoot data collection errors and performance issues.

The Health Overview dashboard gives you an at-a-glance view of the following data collection errors and performance metrics for all input types:

- Errors count by error category
- Error count over time by input type, host, data input, and error category
- Throughput over time by host, input type, and data input

The S3 Health Details dashboard focuses on the generic, incremental, and SQS-based S3 input types and provides indexing time lag and detailed error information of these multi-purpose inputs.

You can customize the health dashboard. See the About the Dashboard Editor topic in the *Dashboards and Visualizations* manual.

Internal logs

You can directly access internal log data for help with troubleshooting. Data collected with these source types is used in the Health Check dashboards.

Data source	Source type
splunk_ta_aws_cloudtrail_cloudtrail_{input_name}.log.	aws:cloudtrail:log
splunk_ta_aws_cloudwatch.log.	aws:cloudwatch:log
splunk_ta_aws_cloudwatch_logs.log.	aws:cloudwatchlogs:log
splunk_ta_aws_config_{input_name}.log.	aws:config:log
splunk_ta_aws_config_rule.log.	aws:configrule:log
splunk_ta_aws_inspector_main.log, splunk_ta_aws_inspector_app_env.log, splunk_ta_aws_inspector_proxy_conf.log, and splunk_ta_aws_inspector_util.log.	aws:inspector:log
splunk_ta_aws_description.log.	aws:description:log
splunk_ta_aws_billing_{input_name}.log.	aws:billing:log
splunk_ta_aws_generic_s3_{input_name}.	aws:s3:log
splunk_ta_aws_logs_{input_name}.log, each incremental S3 input has one log file with the input name in the log file.	aws:logs:log
splunk_ta_aws_kinesis.log.	aws:kinesis:log

Data source	Source type
splunk_ta_aws_ sqs_based_s3_{input_name} .	aws:sqsbaseds3:log
splunk_ta_aws_sns_alert_modular.log and splunk_ta_aws_sns_alert_search.log.	aws:sns:alert:log
splunk_ta_aws_rest.log, populated by REST API handlers called when setting up the add-on or data input.	aws:resthandler:log
splunk_ta_aws_proxy_conf.log, the proxy handler used in all AWS data inputs.	aws:proxy-conf:log
splunk_ta_aws_s3util.log, populated by the S3, CloudWatch, and SQS connectors.	aws:resthandler:log
splunk_ta_aws_util.log, a shared utilities library.	aws:util:log

Configure log levels

1. Click **Splunk Add-on for AWS** in the navigation bar on Splunk Web.
2. Click **Configuration** in the app navigation bar.
3. Click the **Logging** tab.
4. Adjust the log levels for each of the AWS services as needed by changing the default level of `INFO` to `DEBUG` or `ERROR`.

These log level configurations apply only to runtime logs. Some REST endpoint logs from configuration activity log at DEBUG, and some validation logs log at ERROR. These levels cannot be configured.

Troubleshoot custom sourcetypes for SQS Based S3 inputs

Troubleshoot custom sourcetypes created with an SQS-based S3 input.

- If a custom sourcetype is used (for example, `custom_sourcetype`), it can be replaced. see the following steps:
    1. Navigate to the **Inputs** page of the Splunk Add-on for AWS.
    2. Create a new SQS-Based S3 input, or edit an existing SQS-Based S3 input.
    3. Navigate to the **Source Type** input box, and change the sourcetype name.
    4. Save your changes.
- Adding a custom sourcetype will not split the events. To split events, perform the following steps:
    1. Navigate to `Splunk_TA_aws/local/`.
    2. Open `props.conf` with a text editor.
    3. Add the following stanza:
    ```
    [custom_sourcetype]
    SHOULD_LINEMERGE = false
    ```
    4. Save your changes.

Low throughput for the Splunk Add-on for AWS

If you do not achieve the expected AWS data ingestion throughput, follow these steps to troubleshoot the throughput performance:

1. Identify the problem in your system.
2. Adjust the factors affecting performance.
3. Verify whether performance meets your requirements.

1. Identify the problem in your system that prevents it from achieving a higher level of throughput performance. The problem in AWS data ingestion might be caused one of the following components:
    - The amount of data the Splunk Add-on for AWS can pull in through API calls

- The heavy forwarder's capacity to parse and forward data to the indexer tier, which involves the throughput of the parsing, merging, and typing pipelines
- The index pipeline throughput

To troubleshoot the indexing performance on the heavy forwarder and indexer, refer to Troubleshooting indexing performance in the Capacity Planning Manual.

2. Troubleshoot the performance of the problem component.
   If heavy forwarders or indexers are affecting performance, refer to the Summary of performance recommendations in the Splunk Enterprise *Capacity Planning* Manual.
   If the Splunk Add-on for AWS is affecting performance, adjust the following factors:
   - Parallelization settings
     To achieve optimal throughput performance, set the value of `parallelIngestionPipelines` to 2 in the server.conf file if your resource capacity permits. For information about `parallelIngestionPipelines`, see Parallelization settings in the Splunk Enterprise *Capacity Planning* Manual.
   - AWS data inputs
     If you have sufficient resources, you can increase the number of inputs to improve throughput, but be aware that this also consumes more memory and CPU. Increase the number of inputs to improve throughput until memory or CPU is running short.
     If you are using SQS-based S3 inputs, you can horizontally scale data collection by configuring more inputs on multiple heavy forwarders to consume messages from the same SQS queue.
   - Number of keys in a bucket
     For both the Generic S3 and Incremental S3 inputs, the number of keys or objects in a bucket can impact initial data collection performance. A large number of keys in a bucket requires more memory for S3 inputs in the initial data collection and limits the number of inputs you can configure in the add-on.
     If applicable, you can use log file prefix to subset keys in a bucket into smaller groups and configure different inputs to ingest them separately. For information about how to configure inputs to use log file prefix, see Configure Generic S3 inputs for the Splunk Add-on for AWS.
     For SQS-based S3 inputs, the number of keys in a bucket is not a primary factor since data collection can be horizontally scaled out based on messages consumed from the same SQS queue.
   - File format
     Compressed files consume much more memory than plain text files.
3. When you resolve the performance issue, see if the improved performance meets your requirements. If not, repeat the previous steps to identify the next bottleneck in the system and address it until you're satisfied with the overall throughput performance.

Problem saving during account or input configuration

If you experience errors or trouble saving while configuring your AWS accounts on the setup page, go to `$SPLUNK_HOME/etc/system/local/web.conf` and and change the following timeout setting:

```
[settings]
splunkdConnectionTimeout = 300
```

Problems deploying with a deployment server

If you use a deployment server to deploy the Splunk Add-on for Amazon Web Services to multiple heavy forwarders, you must configure the Amazon Web Services accounts using the Splunk Web setup page for each instance separately because the deployment server does not support sharing hashed password storage across instances.

S3 issues

Troubleshoot the S3 inputs for the Splunk Add-on for AWS.

S3 input performance issues

You can configure multiple S3 inputs for a single S3 bucket to improve performance. The Splunk platform dedicates one process for each data input, so provided that your system has sufficient processing power, you can improve performance with multiple inputs. See Hardware and software requirements for the Splunk Add-on for AWS.

> To prevent indexing duplicate data, don't overlap the S3 key names in multiple inputs against the same bucket.

S3 key name filtering issues

Troubleshoot regex to fix filtering issues.

The deny and allow list matches the full key name, not just the last segment. For example, allow list `.*abc/.*` matches `/a/b/abc/e.gz`.

Your regex should match the full for whitelist and blacklist. For example, if the directory of `example` bucket is `cloudtrail/cloudtrail2`, the desired file is under the path `cloudtrail/cloudtrail2/abc.txt`, and you would like to ingest `abc.txt`, you need to specify the `key_name` and `whitelist`. See the following example, which will ingest any files under the path:
`cloudtrail/cloudtrail2`:

```
key_name = cloudtrail
whitelist = ^.\/cloudtrail2\/.$
```

For more help with regex, see the following resources:

- Watch "All My Regex's Live in Texas" on Splunk Blogs.
- Read "About Splunk regular expressions" in the Splunk Enterprise *Knowledge Manager Manual*.

S3 event line breaking issues

If your indexed S3 data has incorrect line breaking, configure a custom source type in props.conf to control how the lines break for your events.

If S3 events are too long and get truncated, set `TRUNCATE = 0` in props.conf to prevent line truncating.

More more information, see Configure event line breaking in the *Getting Data In* manual.

CloudWatch configuration issues

Troubleshoot your CloudWatch configuration.

API throttling issues

If you have a high volume of CloudWatch data, search `index=_internal Throttling` to determine if you are experiencing an API throttling issue. If you are, contact AWS support to increase your CloudWatch API rate. You can also decrease the number of metrics you collect or increase the granularity of your indexed data in order to make fewer API calls.

Granularity

If the granularity of your indexed data does not match your expectations, check that your configured granularity falls within what AWS supports for the metric you have selected. Different AWS metrics support different minimum granularities, based on the allowed sampling period for that metric. For example, CPUUtilization has a sampling period of 5 minutes, whereas Billing Estimated Charge has a sampling period of 4 hours.

If you configured a granularity that is less than the sampling period for the selected metric, the reported granularity in your indexed data reflects the actual sampling granularity but is labeled with your configured granularity. Clear the `local/inputs.conf` cloudwatch stanza with the problem, adjust the granularity configuration to match the supported sampling granularity so that newly indexed data is correct, and reindex the data.

CloudTrail data indexing problems

If you are not seeing CloudTrail data in the Splunk platform, follow this troubleshooting process.

1. Review the internal logs with the following search: `index=_internal source=*cloudtrail*`
2. Verify that the Splunk platform is connecting to SQS successfully by searching for the string `Connected to SQS`.
3. Verify that the Splunk platform is processing messages successfully. Look for strings that follow the pattern: `X completed, Y failed while processing notification batch`.
4. Verify that the Splunk platform is processing messages successfully. Look for strings that follow the following pattern: `X completed, Y failed while processing notification batch`.
5. Review your Amazon Web Services configuration to verify that SQS messages are being placed into the queue. If messages are being removed and the logs do not show that the input is removing them, then there might be another script or input consuming messages from the queue. Review your data inputs to ensure there are no other inputs configured to consume the same queue.
6. Go to the AWS console to view CloudWatch metrics with the detail set to 1 minute to view the trend. For more details, see https://aws.amazon.com/blogs/aws/amazon-cloudwatch-search-and-browse-metrics-in-the-console/. If you see messages consumed but no Splunk platform inputs are consuming them, check for remote services that might be accessing the same queue.
7. If your AWS deployment contains large S3 buckets with a large number of subdirectories for 60 or more AWS accounts, perform one of the following tasks:
    - Enable SQS notification for each S3 bucket and switch to a SQS S3 input. This lets you add multiple copies of the input for scaling purposes.
    - Split your inputs into one bucket per account and use multiple incremental inputs.

Billing Report issues

Troubleshoot the Splunk Add-on for AWS Billing inputs.

Problems accessing billing reports from AWS

If you have problems accessing billing reports from AWS, ensure that:

- There Billing Reports available on the S3 bucket you select when you configure the billing input,
- The AWS account you specify has the permission to read the files inside that bucket.

Problems understanding the billing report data

If you have problems understanding the billing report data, access the saved searches included with the add-on to analyze billing report data.

Problems configuring the billing data interval

> The default billing data ingestion collection intervals for billing report data is designed to minimize license usage. Review the default behavior and make adjustments with caution.

Configure the interval by which the Splunk platform pulls Monthly and Detailed Billing Reports:

1. In Splunk Web, go to the Splunk Add-on for AWS inputs screen.
2. Create a new **Billing** input or click to edit your existing one.
3. Click the **Settings** tab.
4. Customize the value in the **Interval** field.

SNS alert issues

Because the modular input module is inactive, it cannot check whether the AWS is correctly configured or existing in the AWS SNS. If you cannot send a message to the AWS SNS account, you can perform the following procedures:

- Ensure the SNS topic name exists in AWS and the region ID is correctly configured.
- Ensure the AWS account is correctly configured in Splunk Add-on for AWS.

If you still have the issue, use the following search to check the log for AWS SNS:

```
index=_internal sourcetype=aws:sns:alert:log"
```

Proxy settings for VPC endpoints

You must add each S3 region endpoint to the `no_proxy` setting, and use the correct hostname in your region: `s3.<your_aws_region>.amazonaws.com`. The `no_proxy` setting does not allow for any spaces between the IP addresses.

When using a proxy with VPC endpoints, check the proxy setting defined in the splunk-launch.conf file located at `$SPLUNK_HOME/etc/splunk-launch.conf`. For example:

```
no_proxy = 169.254.169.254,127.0.0.1,s3.amazonaws.com,s3.ap-southeast-2.amazonaws.com
```

Certificate verify failed (_ssl.c:741) error message

If you create a new input, you might receive the following error message:
`certificate verify failed (_ssl.c:741)`
Perform the following steps to resolve the error:

1. Navigate to `$SPLUNK_HOME/etc/auth/cacert.pem` and open the **cacert.pem** file with a text editor.
2. Copy the text from your deployment's proxy server certificate, and paste it into the **cacert.pem** file.
3. Save your changes.

Internet restrictions prevent add-on from collecting AWS data

If your deployment has a security policy that doesn't allow connection to the public internet from AWS virtual private clouds (VPCs), this might prevent the Splunk Add-on for AWS from collecting data from Cloudwatch inputs, S3 inputs, and other inputs which depend on access to AWS services.

To identify this issue in your deployment:

1. Check if you have a policy that restricts outbound access to the public Internet from your AWS VPC.
2. Identify if you have error messages that show that your attempts to connect to sts.amazonaws.com result in a timeout. For example:

```
ConnectTimeout: HTTPSConnectionPool(host='sts.amazonaws.com', port=443): Max retries exceeded
with url: / (Caused by ConnectTimeoutError(<botocore.awsrequest.AWSHTTPSConnection object
at 0x7fdfd97bc350>,
'Connection to sts.amazonaws.com timed out. (connect timeout=60)')) host = si3-splunk1
index = 0014000000kbznqaa1
source = /opt/splunkcoreengine/ce_customers/0014000000KBzNQAA1/1425528/si3-splunk1-sh_ds_
ls_-20190708-190819/log/splunk_ta_aws_aws_cloudwatch.log sourcetype = splunk_ta_
aws_aws_cloudwatch
```

To fix this issue in your deployment:

1. Your VPC endpoint interface needs to be set up in your AWS environment. See the AWS documentation for details regarding VPC endpoints.
2. Update the Splunk instance that is being used for data collection to use your VPC endpoint as a gateway to allow connections to be established to your AWS services:
    1. In your Splunk instance, navigate to `./etc/apps/Splunk_TA_aws/bin/3rdparty/botocore/data/endpoints.json`, and open using a text editor.
    2. Update the `hostname` to use the hostname of your VPC endpoint interface. For example: Before

```
"sts": {
"defaults": {
"credentialScope": {
"region": "us-east-1"
},
"hostname": "sts.amazonaws.com"
```

    After

```
},
"sts" : {
"defaults" : {
"credentialScope" : {
"region" : "us-east-1"
},
"hostname" : "<Enter VPC endpoint Interface DNS name here>"
```

    3. Save your changes.
    4. In your Splunk instance, navigate to `./etc/apps/Splunk_TA_aws/bin/3rdparty/botocore/data/endpoints.json`, and open using a text editor.
    5. Update the `hostname` to use the hostname of your VPC endpoint interface. For example: Before

```
"sts": {
"defaults": {
"credentialScope": {
"region": "us-east-1"
},
"hostname": "sts.amazonaws.com"
```

    After

```
},
"sts" : {
"defaults" : {
```

```
"credentialScope" : {
"region" : "us-east-1"
},
"hostname" : "<Enter VPC endpoint Interface DNS name here>"
```

6. Save your changes.
3. Restart your Splunk instance.
4. Validate that the connection to your VPC has been established.

Failed to load input and configuration page when running the Splunk software on a custom management port

If the Splunk software fails to load input and configuration page while running on the custom management port (for example, `<IP>:<CUSTOM_PORT>`), perform the following troubleshooting steps.

1. Navigate to `$SPLUNK_HOME/etc/`
2. Open `splunk-launch.conf` using a text editor.
3. Add the environment variable `SPLUNK_MGMT_HOST_PORT=<IP>:<CUSTOM_PORT>`
4. Save your changes.
5. Restart your Splunk instance.

Kinesis timestamp issues

If your Kinesis events are ingested with the wrong timestamp, perform the following troubleshooting steps to disable the Splunk software's timestamp extraction feature.

1. Stop your Splunk instance.
2. Navigate to `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/local`.
3. Open the `props.conf` file using a text editor.
4. In the `props.conf` file, locate the stanza for the Kinesis sourcetype. If it doesn't exist, create one with the Kinesis sourcetype.
5. Inside the Kinesis sourcetype stanza, add `DATETIME_CONFIG = NONE`.
6. Save your changes.
7. Restart the Splunk.

Reference

Access billing data for the Splunk Add-on for AWS

Use the billing input in the Splunk Add-on for Amazon Web Services (AWS) to collect your AWS billing reports, then extract useful information from them using pre-built reports included with this add-on. The pre-built reports are based on AWS report formats. You can use these reports as examples of how to use the Splunk platform to explore your other S3 data.

For more information on how to configure Billing inputs for the Splunk Add-on for AWS, see the Configure Billing inputs for the Splunk Add-on for AWS topic in this manual.

> The Billing input does not collect billing reports for your AWS Marketplace charges.

Billing report types

See information about Monthly reports, Monthly cost allocation reports, Detailed billing reports, and Detailed billing reports with resources and tags.

Monthly report

The Monthly report lists AWS usage for each product dimension used by an account and its Identity Access Management (IAM) users in monthly line items. You can download this report from the Bills page of the Billing and Cost Management console.

This report takes the following file name format:

```
<AWS account number>-aws-billing-csv-yyyy-mm.csv
```

This report is small in size, so the add-on pulls the entire report once daily to get the latest snapshot.

Monthly cost allocation report

The Monthly cost allocation report contains the same data as the monthly report as well as any cost allocation tags that you create. Monthly reports have the event type `aws_billing_monthly_report`. You must obtain this report from the Amazon S3 bucket that you specify. Standard AWS storage rates apply.

This report takes the following file name format:

File Name Format: `<AWS account number>-aws-cost-allocation-yyyy-mm.csv`

This report is small in size, so the add-on pulls the entire report once daily to get the latest snapshot.

Detailed billing report

The Detailed billing report lists AWS usage for each product dimension used by an account and its IAM users in hourly line items. Detailed billing reports have the event type `aws_billing_detail_report`. You must obtain this report from the Amazon S3 bucket that you specify. Standard AWS storage rates apply.

This report takes the following file name format:

```
<AWS account number>-aws-billing-detailed-line-items-yyyy-mm.csv.zip
```

This report can grow very large, so the add-on collects the report only after the month has ended. The add-on continues to collect the report once per day until it is finalized by Amazon billing services.

Detailed billing report with resources and tags

The Detailed billing report with resources and tags contains the same data as the detailed billing report, but also includes any cost allocation tags you have created and ResourceIDs for the AWS resources used by your account. You must obtain this report from the Amazon S3 bucket that you specify. Standard AWS storage rates apply.

This report takes the following file name format:

```
<AWS account number>-aws-billing-detailed-line-items-with-resources-and-tags-yyyy-mm.csv.zip
```

This report can be very large, so the add-on collects the report only after the month has ended. The add-on continues to collect the report once per day until it is finalized by Amazon billing services.

Access preconfigured reports

The Splunk Add-on for AWS includes several reports based on the indexed billing report data. You can find these saved reports in Splunk Web by clicking **Home > Reports** and looking for items with the prefix `AWS Bill -` . Some of the saved searches return a table. Others return a single value, such as `AWS Bill - Total Cost till Now`.

The Splunk platform typically indexes multiple monthly report snapshots. To obtain the most recent monthly report snapshot, click **Home > Reports** and open the saved report called `AWS Bill - Monthly Latest Snapshot`. Or, search for it using the search string: `| savedsearch "AWS Bill - Monthly Latest Snapshot"`

You can obtain the most recent detailed report by clicking **Home > Reports** and opening the saved report called `AWS Bill - Daily Cost`. Or, search for it using the search string:

```
| savedsearch "AWS Bill - Daily Cost"
```

.

Searching against detailed reports can be slow due to the volume of data in the report. Accelerate the searches against detailed reports.

Report sources

These saved reports are based on AWS Billing Reports instead of the billing metric data in CloudWatch. By default, Total or Monthly reports are based on data indexed from the AWS Monthly Reports (`*-aws-billing-csv-yyyy-mm.csv` or `*-aws-cost-allocation-yyyy-mm.csv`) on the S3 bucket, while Daily reports are based on AWS Detail Reports (`*-aws-billing-detailed-line-items-yyyy-mm.csv.zip` or `*-aws-billing-detailed-line-items-with-resources-and-tags-yyyy-mm.csv.zip`).

Default index behavior

By default, reports look for data in the default index, `main`. If you changed the default index when you configured the data input, the reports will not work unless you include the index in the default search indexes list or change the two reports so

they filter to the custom index.

To include a custom index in the default search indexes list, perform the following steps:

1. Click **Settings > Users and authentication > Access controls > Roles > [Role that uses the saved searches] > Indexes searched by default**.
2. Add the custom index to the default search indexes list.
3. Repeat for each role that uses the saved searches.

To change the saved searches to filter to a custom index, perform the following steps:

1. Open the saved search `AWS Bill - Monthly Latest Snapshot`.
2. Add a filter to specify the index you configured. For example, `index=new_index`.
3. Save your changes to the saved search.
4. Repeat these steps for the other saved search, `AWS Bill - Detailed Cost`.

API reference for the Splunk Add-on for AWS

See the following sections for API reference information for the Splunk Add-on for AWS.

Account

`https://<host>:<mPort>splunk_ta_aws_aws_account`
API for AWS Account settings.

GET, POST, or DELETE

API for AWS Account settings

Request parameters

Name	Type	Description
name	Boolean `true`	Name
key_id	Boolean `true`	Key ID
secret_key	Boolean `true`	Secret Key
category	Boolean `true`	Region Category
iam	Boolean `false`	Identifies EC2 Instance Role

Config inputs

`https://<host>:<mPort>aws_config_inputs_rh_ucc`
API for the AWS Config input.

GET, POST, or DELETE

API for the AWS Config input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
aws_account	Boolean `true`	AWS Account
aws_region	Boolean `true`	AWS Region
sqs_queue	Boolean `true`	SQS Queue Name
polling_interval	Boolean `true`	Interval
sourcetype	Boolean `true`	Sourcetype API for `aws:config`
index	Boolean `true`	Index
enable_additional_notifications	Boolean `false`	API for enabling additional notifications.

Description input

`https://<host>:<mPort>splunk_ta_aws_aws_description`
API for AWS Description inputs.

GET, POST, or DELETE

API for the AWS Description input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
regions	Boolean `true`	AWS Regions
apis	Boolean `true`	APIs for the following information: `ec2_volumes/3600,ec2_instances/3600,ec2_reserved_instances/3600,ebs_snapshots/3600,classic_load /3600,application_load_balancers/3600,vpcs/3600,vpc_network_acls/3600,cloudfront_distributions/ /3600,rds_instances/3600,ec2_key_pairs/3600,ec2_security_groups/3600,ec2_images/3600,ec2_addres _functions/3600,s3_buckets/3600`
sourcetype	Boolean `true`	Sourcetype API for `aws:description`
index		Index

Name	Type	Description
	Boolean `true`	

IAM role settings

`https://<host>:<mPort>splunk_ta_aws_iam_roles`
API for IAM role settings.

GET, POST, or DELETE

API for IAM role settings

Request parameters

Name	Type	Description
name	Boolean `true`	Name
arn	Boolean `true`	Role ARN

Incremental S3 input

`https://<host>:<mPort>splunk_ta_aws_splunk_ta_aws_logs`
API for the AWS Incremental S3 input.

GET, POST, or DELETE

API for AWS Config inputs

Request parameters

Name	Type	Description
name	Boolean `true`	Name
aws_account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
host_name	Boolean `true`	AWS S3 host name
bucket_name	Boolean `true`	S3 bucket

Name	Type	Description
log_type	Boolean `true`	Log type information for the following sourcetypes: `Log Type: cloudtrail, s3:accesslogs, cloudfront:accesslogs and elb:accesslogs`
log_file_prefix	Boolean `false`	Log file prefix
log_start_date	Boolean `false`	Log start date
log_name_format	Boolean `false`	Distribution ID (Required for `log_type='cloudfront:accesslogs'`)
interval	Boolean `true`	Interval
sourcetype	Boolean `true`	Sourcetype API for `aws:config`
index	Boolean `true`	Index

Inspector input

`https://<host>:<mPort>splunk_ta_aws_aws_inspector`
API for the AWS Inspector input.

GET, POST, or DELETE

API for the AWS Inspector input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
regions	Boolean `true`	AWS Regions
polling_interval	Boolean `true`	Interval
sourcetype	Boolean `true`	Sourcetype API for `aws:description`
index	Boolean `true`	Index

Kinesis input

`https://<host>:<mPort>splunk_ta_aws_aws_kinesis`
API for the AWS Kinesis input.

GET, POST, or DELETE

API for the AWS Kinesis input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
region	Boolean `true`	AWS Region
stream_names	Boolean `true`	Kinesis stream name
init_stream_position	Boolean `true`	Initial Stream Position: `LATEST` or `TRIM_HORIZON`
encoding	Boolean `false`	Encoding with: `gzip` or `(none). (none)` means empty string.
format	Boolean `false`	Record Format: `CloudWatchLogs` or `(none). (none)` means empty string."
sourcetype	Boolean `true`	Sourcetype API for `aws:description`
index	Boolean `true`	Index

S3 input

`https://<host>:<mPort>splunk_ta_aws_aws_s3`
API for the AWS S3 input.

GET, POST, or DELETE

API for the AWS S3 input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
aws_account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
host_name	Boolean `true`	S3 host name
bucket_name	Boolean `true`	S3 bucket name

Name	Type	Description
key_name	Boolean `false`	S3 key prefix
initial_scan_datetime	Boolean `false`	Start date/time.
blacklist	Boolean `false`	Blacklist
whitelist	Boolean `false`	Whitelist
polling_interval	Boolean `true`	Interval.
sourcetype	Boolean `true`	Sourcetype API for `aws:cloudtrail`, `aws:s3:accesslogs`, `aws:cloudfront:accesslogs`, and `aws:elb:accesslogs`.
index	Boolean `true`	Index

SQS-based S3 input

`https://<host>:<mPort>splunk_ta_aws_aws_sqs_based_s3`
API for the AWS SQS-based S3 input.

GET, POST, or DELETE

API for the AWS SQS-based S3 input

Request parameters

Name	Type	Description
name	Boolean `true`	Name
aws_account	Boolean `true`	AWS Account
aws_iam_role	Boolean `false`	Assume role
sqs_queue_region	Boolean `true`	Name of the AWS SQS region
sqs_queue_url	Boolean `true`	URL of the AWS SQS queue
sqs_batch_size	Boolean `true`	Maximum number of messages
s3_file_decoder	Boolean `true`	Name of an S3 file decoder
interval	Boolean `true`	Interval
sourcetype	Boolean `true`	Sourcetype API for `aws:description`
index	Boolean `true`	Index

Lookups for the Splunk Add-on for AWS

Lookup files are located in `$SPLUNK_HOME/etc/apps/Splunk_TA_aws/lookups` on *nix systems and `%SPLUNK_HOME%\etc\apps\Splunk_TA_aws\lookups` on Windows systems. Lookup files map fields from Amazon Web Services (AWS) to CIM-compliant values in the Splunk platform. The Splunk Add-on for AWS has the following lookups:

File name	Purpose
aws_config_action_lookup.csv	Maps the status field to a CIM-compliant value for the `action` field.
aws_config_object_category_lookup.csv	Sorts the various AWS Config object categories into CIM-compliant values for the `object_category` field.
aws-cloudtrail-action-status.csv	Maps the `eventName` and `errorCode` fields to CIM-compliant values for `action` and `status`.
aws-cloudtrail-changetype.csv	Maps the `eventSource` to a CIM-compliant value for the `change_type` field.
aws-health-error-type.csv	Maps `ErrorCode` to `ErrorDetail`, `ErrorCode`, `ErrorDetail`.
aws-log-sourcetype-modinput.csv	Maps `sourcetype` to `modinput`.
cloudfront_edge_location_lookup	Maps the `x_edge_location` value to a human-readable `edge_location_name`.
vendor-product-aws-cloudtrail.csv	Defines CIM-compliant values for the `vendor`, `product`, and `appfields` based on the source type.
vpcflow_action_lookup.csv	Maps the numerical protocol code to a CIM-compliant `protocol` field and a human-readable field `protocol_full_name`.
vpcflow_protocol_code_lookup.csv	Maps the `vpcflow_action` field to a CIM-compliant `action` field.
VmSizeToResources.csv	Maps the `instance_type` field to CIM-compliant `cpu_cores`, mem_capacity fields.

Saved searches for the Splunk Add-on for AWS

To enable or disable a saved search, follow these steps:

1. From the **Settings** menu, choose **Searches, reports, and alerts**.
2. Locate the saved search by filtering the list or entering the name of the saved search in the **filter** field to search for it.
3. Under the **Actions** column of the saved search list, select **Edit** > **Enable**/**Disable** to enable or disable the saved search.

Saved searches cannot be scheduled using a free license.

The "Addon Metadata - Summarize AWS Inputs" saved search is disabled by default, but you must enable this saved search in order to aggregate inputs and accounts data in the summary index.

The Splunk Add-on for AWS includes the following saved searches:

Name	Search
AWS Bill - Monthly Latest Snapshot	`search = index="<your index>" eventtype=aws_billing_monthly_report [search index="<your index>"]` `search = eventtype=aws_billing_monthly_report [search eventtype=aws_billing_monthly_report | dedup report_month sortby -_time | return 1000`

Name	Search
	S3KeyLastModified]
AWS Bill - Detailed Cost Latest Snapshot	search = index=<"your index"> eventtype=aws_billing_detail_report [search index=<"your index">] search = eventtype=aws_billing_detail_report [search eventtype=aws_billing_detail_report RecordType=StatementTotal | dedup report_month sortby -_time | return 1000 S3KeyLastModified]
AWS Bill - Total Cost until Now	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=StatementTotal | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode display.general.type = statistics display.visualizations.show = 0 request.ui_dispatch_view = search
AWS Bill - Total Cost until Now by Service	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=LinkedLineItem | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode by ProductName
AWS Bill - Total Cost until Now by Linked Account	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=AccountTotal | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode by LinkedAccount
AWS Bill - Monthly Cost	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=StatementTotal | timechart span=1mon sum(TotalCost) as TotalCost
AWS Bill - Monthly Cost by Service	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=LinkedLineItem | timechart span=1mon sum(TotalCost) as TotalCost by ProductName limit=20
AWS Bill - Monthly Cost by Linked Account	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=AccountTotal | timechart span=1mon sum(TotalCost) by LinkedAccount limit=20
AWS Bill - Current Month Cost until Now	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=StatementTotal | eval date_month=strftime(_time, "%Y-%m") | eval current_month=strftime(now(), "%Y-%m") | where date_month=current_month | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode display.general.type = statistics display.visualizations.show = 0 request.ui_dispatch_view = search
AWS Bill - Current Month Cost until Now by Service	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=LinkedLineItem | eval date_month=strftime(_time, "%Y-%m") | eval current_month=strftime(now(), "%Y-%m") | where date_month=current_month | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode by ProductName
AWS Bill - Current Month Cost until Now by Linked Account	search = | savedsearch "AWS Bill - Monthly Latest Snapshot" | search RecordType=AccountTotal | eval date_month=strftime(_time, "%Y-%m") | eval current_month=strftime(now(), "%Y-%m") | where date_month=current_month | stats sum(TotalCost) as TotalCost, first(CurrencyCode) as CurrencyCode by LinkedAccount
AWS Bill - Daily Cost through Last Month - Blended	search = | savedsearch "AWS Bill - Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(BlendedCost) as TotalCost
AWS Bill - Daily Cost through Last Month by Service - Blended	search = | savedsearch "AWS Bill - Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(BlendedCost) as TotalCost by ProductName limit=20
AWS Bill - Daily Cost through Last Month by Linked Account - Blended	search = | savedsearch "AWS Bill - Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(BlendedCost) as TotalCost by LinkedAccount limit=20

Name	Search
AWS Bill - Total Cost through Last Month by Region - Blended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | stats sum(BlendedCost) as TotalCost by AvailabilityZone`
AWS Bill - Monthly Cost through Last Month by Region - Blended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1mon sum(BlendedCost) as TotalCost by AvailabilityZone limit=20`
AWS Bill - Daily Cost through Last Month by Region - Blended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(BlendedCost) as TotalCost by AvailabilityZone limit=20`

AWS Bill - Total Daytime Cost through Last Month - Blended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | eval date_hour=strftime(_time, "%H") | search (date_hour>=7 AND date_hour<=17) | stats sum(BlendedCost) as TotalCost`
	`display.general.type = statistics`
	`display.visualizations.show = 0`
	`request.ui_dispatch_view = search`

AWS Bill - Total Nighttime Cost through Last Month - Blended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | eval date_hour=strftime(_time, "%H") | search (date_hour < 7 OR date_hour > 17) | stats sum(BlendedCost) as TotalCost`
	`display.general.type = statistics`
	`display.visualizations.show = 0`
	`request.ui_dispatch_view = search`

AWS Bill - Daily Cost through Last Month - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(UnBlendedCost) as TotalCost`
AWS Bill - Total Cost through Last Month by Region - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | stats sum(UnBlendedCost) as TotalCost by AvailabilityZone`
AWS Bill - Daily Cost through Last Month by Service - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(UnBlendedCost) as TotalCost by ProductName limit=20`
AWS Bill - Daily Cost through Last Month by Linked Account - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(UnBlendedCost) as TotalCost by LinkedAccount limit=20`
AWS Bill - Monthly Cost through Last Month by Region - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1mon sum(UnBlendedCost) as TotalCost by AvailabilityZone limit=20`
AWS Bill - Daily Cost through Last Month by Region - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | timechart span=1day sum(UnBlendedCost) as TotalCost by AvailabilityZone limit=20`

AWS Bill - Total Daytime Cost through Last Month - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | eval date_hour=strftime(_time, "%H") | search (date_hour>=7 AND date_hour<=17) | stats sum(UnBlendedCost) as TotalCost`
	`display.general.type = statistics`
	`display.visualizations.show = 0`
	`request.ui_dispatch_view = search`

AWS Bill - Total Nighttime Cost through Last Month - Unblended	`search = | savedsearch "AWS Bill – Detailed Cost Latest Snapshot" | search RecordType=LineItem | eval date_hour=strftime(_time, "%H") | search (date_hour < 7 OR date_hour > 17) | stats sum(UnBlendedCost) as TotalCost` `display.general.type = statistics`

Name	Search
	`display.visualizations.show = 0` `request.ui_dispatch_view = search`
Addon Metadata - Migrate AWS Accounts	`search = | listawsaccounts | collect` `` `aws-account-index` ``

Addon Metadata - Summarize AWS Inputs	`disabled = 1`
	`enableSched = 1`
	`cron_schedule = 0 * * * *`
	`dispatch.earliest_time = 0`
	`dispatch.latest_time = now`
	`search = | listawsinputs | collect` `` `aws-input-index` ``

Configure permissions for all inputs for the Splunk Add-on for AWS at once

The best practice for configuring permissions is to configure permissions for each input that you want to configure. See the *Input configuration* chapter in this manual for more information on configuring individual input permissions.

Release Notes

Release notes for the Splunk Add-on for AWS

Version 5.2.0 of the Splunk Add-on for Amazon Web Services was released on October 4, 2021.

Compatibility

Version 5.2.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.20 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, Metadata, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 5.2.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- CIM 4.20 compatibility and enhanced CIM mapping
- UI component upgrades (jQuery) that are compatible with future versions of the Splunk software.
- The aws:cloudtrail sourcetype is updated for app field mapping.

See the following tables for information on field changes between 5.1.0 and 5.2.0:

Source-type	Fields added	Fields removed
`aws:cloudfront:accesslogs`	action, app, bytes, bytes_in, bytes_out, c_port, category, cs_protocol_version, dest, duration, fle_encrypted_fields, fle_status, http_content_type, http_method, http_referrer, http_referrer_domain, http_user_agent, http_user_agent_length, response_time, sc_content_len, sc_content_type, sc_range_end, sc_range_start, src,src_ip, src_port, status, time_to_first_byte, uri_path, url, url_domain, url_length, vendor_product, x_edge_detail_result_type	

Source-type	Fields added	Fields removed
aws:cloudtrail	action, authentication_method, change_type, dest, men_free, object, object_attrs, object_id, rule_action, src_user, src_user_name, src_user_type, status, user_name, vendor_account, vendor_product	user_agent, user_id, user_type
aws:cloudwatchlogs:guardduty	body, findingType	
aws:cloudwatchlogs:vpcflow	app, protocol_version, user_id, vendor_product,	
aws:config	object_id, object_path, result, vendor_account, vendor_product,	
aws:config:notification	object_attrs, object_path, result, user, vendor_product	
aws:description	enabled, user_id, family, status, description, time, type, snapshot	
aws:elb:accesslogs	ActionExecuted, ChosenCertArn, ClientPort, DomainName, ELB, ELBStatusCode, ErrorReason, MatchedRulePriority, ReceivedBytes, RedirectUrl, Request, RequestCreationTime, RequestProcessingTime, RequestTargetIP, RequestTargetPort, RequestType, ResponseProcessingTime, ResponseTime, SSLCipher, SSLProtocol, SentBytes, TargetGroupArn, TargetPort, TargetProcessingTime, TargetStatusCode, TraceId, UserAgent, action, app, bytes, bytes_in, bytes_out, category, dest, dest_port, http_method, http_user_agent, http_user_agent_length, response_time, src, src_ip, src_port, status, url, url_length, vendor_product	
aws:metadata	enabled, region, snapshot, status, time, user_id, vendor_region	
aws:s3	AuthType, BucketCreationTime, BucketName, BucketOwner, BytesSent, CipherSuite, ErrorCode, HTTPMethod, HTTPStatus, HostHeader, HostId, ObjectSize, OperationKey, Referer, RemoteIp, RequestID, RequestKey, RequestURI, RequestURIPath, Requester, SignatureVersion, TLSVersion, TotalTime, TurnAroundTime, UserAgent, VersionId, action, bytes, bytes_out, category, dest, error_code, http_method, http_user_agent, http_user_agent_length, operation,response_time, src, src_ip, status, storage_name, url, url_domain, url_length, user, vendor_product	
aws:s3:accesslogs	action, category, http_referrer, http_referrer_domain, http_user_agent_length, src_ip,status, storage_name, url, url_length, vendor_product	

See the following table for a list of fields **modified** between 5.1.0 and 5.2.0:

Sourcetype	CIM Field	eventName, resourceID, resourceType, or source	
aws:cloudtrail	app	eventName: All	eventSource, example: sts.amazonaws.com
	user	eventName: AssumeRole	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: AssumeRoleWithSAML, AssumeRoleWithWebIdentity	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: AttachVolume, AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, CheckMfa, ConsoleLogin, CreateAccessKey, CreateBucket, CreateChangeSet, CreateDeliveryStream, CreateFunction20150331, CreateKeyspace, CreateLoadBalancerListeners, CreateLoadBalancerPolicy, CreateLogGroup, CreateLogStream, CreateLoginProfile,	userIdentity.principalId, example: AIDA3HRA7T6MUVTY

Sourcetype	CIM Field	eventName, resourceID, resourceType, or source	
		CreateNetworkAcl, CreateNetworkAclEntry, CreateNetworkInterface, CreateQueue, CreateSecurityGroup, CreateTable, CreateUser, CreateVirtualMFADevice, CreateVolume, DeleteNetworkAcl, DeleteNetworkAclEntry, DeleteSecurityGroup, DeleteVolume, DetachVolume, GetFederationToken, GetSessionToken, PutBucketAcl, PutBucketPublicAccessBlock, PutObject, RebootInstances, RevokeSecurityGroupEgress, ReplaceNetworkAclAssociation, ReplaceNetworkAclEntry, RevokeSecurityGroupIngress	
		eventNames: GetAccountSummary, GetUser, ListAccessKeys, ListAccountAliases, ListSigningCertificates - Failure Event	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: GetBucketEncryption, ListAliases, ListRoles	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventName: PutBucketAcl	requestParameters.AccessContr requestParameters.AccessContr example: splunk_aws_dsg_sa
		eventNames: RunInstances, StartInstances, StopInstances, TerminateInstances	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
	user_type	eventName: UpdateUser	requestParameters.userName, example: OldUserName
		eventNames: AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity	userIdentity.type, example: AWS::IAM::Role
		eventNames: ListAliases, ListRoles	userIdentity.type, example: AWS::IAM::Role
		eventName: PutBucketAcl	requestParameters.AccessContr example: CanonicalUser
	src_user	eventNames: AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventName: CreateUser	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: DeleteUser, GetUser, PutBucketAcl, UpdateUser	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: AssumeRole, AssumeRoleWithSAML	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
	user_id	AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity, example: responseElements.assumedRoleUser.assumedRoleId	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
	src_user_id		

Sourcetype	CIM Field	eventName, resourceID, resourceType, or source	
		eventNames: AttachVolume, AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, CreateAccessKey, CreateBucket, CreateChangeSet, CreateDeliveryStream, CreateFunction20150331, CreateNetworkAcl, CreateNetworkAclEntry, CreateSecurityGroup, CreateTable, CreateVirtualMFADevice, DeleteBucket, DeleteNetworkAcl, DeleteSecurityGroup, DeleteVolume, GetAccountSummary, ListSigningCertificates, PutBucketPublicAccessBlock, RebootInstances, ReplaceNetworkAclEntry, RevokeSecurityGroupEgress, RevokeSecurityGroupIngress, RunInstances, StartInstances, StopInstances, TerminateInstances	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventName: ConsoleLogin	userIdentity.principalId, example: AIDA3HRA7T6MUVTY
		eventNames: ListAliases, ListRoles	userIdentity.principalId, example: AROACKCEVSQ6C2E
	object_category	eventNames: AttachVolume, DeleteVolume, DetachVolume	Static Value: disk
		eventNames: AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, CreateSecurityGroup, DeleteSecurityGroup, RevokeSecurityGroupEgress, RevokeSecurityGroupIngress	Static Value: firewall
		eventNames: CreateAccessKey, CreateLoginProfile, CreateVirtualMFADevice, GetAccountSummary, GetUser, ListAccessKeys, ListAccountAliases, ListRoles, ListSigningCertificates	Static Value: unknown
		eventNames: CreateBucket, DeleteBucket, PutBucket, PublicAccessBlock, PutObject	Static Value: storage
		eventName: CreateChangeSet	Static Value: unknown
		eventName: CreateDeliveryStream	Static Value: unknown
		eventName: CreateFunction20150331	Static Value: unknown
		eventName: CreateKeyspace	Static Value: unknown
		eventNames: CreateLoadBalancerListeners, CreateLoadBalancerPolicy	Static Value: unknown
		eventName: CreateLogGroup	Static Value: unknown
		eventName: CreateLogStream	Static Value: unknown
		eventNames: CreateNetworkAcl, CreateNetworkAclEntry, DeleteNetworkAcl, DeleteNetworkAclEntry, ReplaceNetworkAclAssociation, ReplaceNetworkAclEntry	Static Value: unknown
		eventName: CreateNetworkInterface	Static Value: unknown

Sourcetype	CIM Field	eventName, resourceID, resourceType, or source	
		eventName: CreateQueue	Static Value: unknown
		eventName: CreateTable	Static Value: unknown
		eventNames: GetBucketEncryption, PutBucketAcl	Static Value: unknown
		eventName: ListAliases	Static Value: unknown
		eventNames: AttachVolume, CreateVolume, DeleteVolume, DetachVolume	Static Value: EC2
		eventNames: AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, CreateNetworkAcl, CreateNetworkAclEntry, CreateNetworkInterface, CreateSecurityGroup, DeleteNetworkAcl, DeleteNetworkAclEntry, DeleteSecurityGroup, ReplaceNetworkAclAssociation, ReplaceNetworkAclEntry, RevokeSecurityGroupEgress, RevokeSecurityGroupIngress	Static Value: EC2
	user_idchange_type	eventNames: CreateAccessKey, CreateLoginProfile, CreateUser, CreateVirtualMFADevice, DeleteUser, GetAccountSummary, GetUser, ListAccessKeys, ListAccountAliases, ListRoles, ListSigningCertificates, ListSigningCertificates, UpdateUser	Static Value: IAM
		eventNames: GetFederationToken, GetSessionToken	Static Value: STS
		eventNames: RunInstances, RebootInstances, StartInstances, StopInstances, TerminateInstances	Static Value: EC2
		eventName: AttachVolume	requestParameters.volumeId, example: vol-3ox0otf8xaqxrptxi
		eventNames: AuthorizeSecurityGroupEgress, AuthorizeSecurityGroupIngress, CreateSecurityGroup, RevokeSecurityGroupEgress, RevokeSecurityGroupIngress	requestParameters.groupId, example: sg-gnzeup7yzumo3f40
	dest	eventName: ConsoleLogin	eventSource, example: ec2.amazonaws.com
		eventNames: CreateBucket, DeleteBucket, GetBucketEncryption, PutBucketAcl, PutBucketPublicAccessBlock, PutObject	requestParameters.bucketName example: bucket1
		eventNames: CreateNetworkAcl, CreateNetworkAclEntry	requestParameters.networkAclId example: acl-328f8f90a8e21dc7
		eventName: CreateUser	responseElements.user.userId, example: UB9BNXNERJHO8AP
		eventNames: CreateVolume, DeleteVolume	responseElements.volumeId, example: vol-pjk4yh53x5xy3kldx
		eventNames: DeleteUser, UpdateUser	requestParameters.userName, example: test_user
		eventName: DetachVolume	responseElements.volumeId, example: vol-pjk4yh53x5xy3kldx

	CIM Field	eventName, resourceID, resourceType, or source	
		eventNames: RunInstances, StartInstances	responseElements.instancesSet example: i-pjk4yh53x5xy3kldx
		eventNames: CreateAccessKey, CreateLoginProfile, CreateNetworkAclEntry, CreateVirtualMFADevice, DeleteNetworkAclEntry	Static Value: created
		eventNames: GetAccountSummary, GetUser, ListAccessKeys, ListAccountAliases, ListSigningCertificates	Static Value: unknown
		eventName: CreateNetworkAclEntry	Static Value: TCP
	protocol object_attrs action	eventName: PutBucketAcl	requestParameters.AccessContr example: "READ READ_ACP WRITE FULL_
	object	eventName: RunInstances	responseElements.instancesSet example: i-pjk4yh53x5xy3kldx
		eventName: StartInstances	requestParameters.instancesSe example: i-pjk4yh53x5xy3kldx
		eventName: UpdateUser	requestParameters.userName, example: test_user
	object_id	eventName: StartInstances	requestParameters.instancesSe
		eventName: UpdateUser	requestParameters.userName, example: test_user
aws:config	object_category	resourceIDs: AWS::Redshift::ClusterSnapshot, AWS::Config::ResourceCompliance	Static Value: unknown
	object_id	resourceIDs: AWS::Redshift::ClusterSnapshot, AWS::EC2::NetworkInterface	ARN, example: arn:aws:redshift:eu-central-2:000
aws:config:notification	object_category	resourceTypes: AWS::Config::ResourceCompliance, AWS::Redshift::ClusterSnapshot	Static Value: unknown
	object_id	resourceTypes: All	N/A
aws:description	user_id	source: All	UserId, example: ZWV5FIRT1Q4ZOFCC
	status	source: *ec2_instances	status, example: completed
aws:cloudwatchlogs:guardduty	dest_type	N/A	Static value from lookup, example: user
	user	N/A	detail.resource.accessKeyDetail example: GeneratedFindingPrinc
	severity	N/A	Static Value: LOW, MEDIUM, HI

Sourcetype	CIM Field	eventName, resourceID, resourceType, or source	
	bytes	N/A	bytes, example: 0
	response_time	N/A	turn_around_time, example: 0

CIM model changes

See the following CIM model changes between 5.1.0 and 5.2.0:

Sourcetype	metric_name	Previous CIM model	New CIM model
aws:cloudwatch	FreeableMemory	Database:Stats, All_Performance:Memory	All_Performance:Memory

Sourcetype	eventName	Previous CIM model	New CIM model
aws:s3:accesslogs aws:cloudtrail	AssumeRole, AssumeRoleWithSAML, AssumeRoleWithWebIdentity, GetFederationToken, GetSessionToken	Authentication:Default_Authentication	
aws:cloudtrail	GetBucketEncryption, PutBucketAcl	Change:Account_Management	Change:All_Changes
aws:cloudtrail	GetBucketEncryption, PutBucketAcl	Change:Account_Management	Change:All_Changes
aws:cloudtrail	ListRoles, ListAliases		Change:All_Changes
aws:cloudtrail	RunInstances	Change:Endpoint_Changes, Change:Instance_Changes	Change:Instance_Changes

Sourcetype	source	Previous CIM model	New CIM model
aws:description	*:ec2_instances, *:ec2_images	All_Inventory	All_Inventory:Virtual_OS:Snapshot
aws:description	*:ec2_instances	All_Inventory	All_Inventory:Virtual_OS:Snapshot
aws:inspector	*:inspector:assessmentRun	All_Inventory:Newtwok, All_Inventory:User, All_Inventory:Virtual_OS:Snapshot	

Sourcetype	Previous CIM model	New CIM model
aws:cloudfront:accesslogs, aws:elb:accesslogs		Web
aws:cloudwatchlogs:guardduty	Alerts, Malware_Attacks	Alerts
aws:config:rule	All_Inventory:Network, All_Inventory:Virtual_OS:Snapshot	Alerts
aws:s3		Web:Storage

Fixed issues

Version 5.2.0 of the Splunk Add-on for Amazon Web Services fixes the following, if any, issues.

Date resolved	Issue number	Description
2021-09-21	ADDON-41646	aws:metadata input is populating S3 buckets for AWS accounts where the bucket does not exist.
2021-09-13	ADDON-35220	

Date resolved	Issue number	Description
		In Splunk_TA_aws KeyError: 'LaunchConfigurationName' appearing when attempting to ingest cloudwatch data
2021-09-10	ADDON-41009	cloudwatch input timeout issue
2021-09-07	ADDON-39428	On upgrade to 5.1.0 - Cloudwatch Inputs need manual line added in conf - private_endpoint_enabled

Known issues

Version 5.2.0 of the Splunk Add-on for Amazon Web Services has the following, if any, known issues.

Date filed	Issue number	Description
2021-11-23	ADDON-45091, ADDON-44250	Splunk Add-on for AWS v5.2.0 does not verify SNS Message signature sent to Splunk via SQS
2021-09-14	ADDON-42117	If Inputs Page page size is more than 25, then the alignment of input details is not consistent

Third-party software attributions

Version 5.2.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Boto
- boto3
- Httplib2
- remotepdb
- requests
- six.py
- SortedContainers
- u-msgpack-python
- urllib3

Release history for the Splunk Add-on for AWS

Latest release

The latest version of the Splunk Add-on for Amazon Web Services is version 5.2.0. See Release notes for the Splunk Add-on for AWS for the release notes of this latest version.

Version 5.1.0

Version 5.1.0 of the Splunk Add-on for Amazon Web Services was released on July 2, 2021.

Compatibility

Version 5.1.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.18 and later

Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, Metadata, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 5.1.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- A new data input called **Metadata**. The Metadata input , which can be accessed in Splunk Web by clicking **Create New Input > Description > Metadata**, uses the boto3 package to collect Description data. See the Metadata input topic in this manual for more information.
- Migrated the following data inputs from the boto2 package to the boto3 package:
    - Cloudtrail
    - Config
    - Cloudwatch logs.
    - Generic S3
- Support for Regional endpoints for all data inputs. Each API call can be made to a region-specific endpoint, instead than a public endpoint.
- Support for private endpoints for the following data inputs:
    - Billing Cost and Usage Reports (CUR)
    - Cloudtrail
    - Cloudwatch
    - Cloudwatch Logs
    - Generic S3
    - Incremental S3
    - Kinesis
    - SQS-based S3

  Private endpoints can perform account authentication and data collection for each supported input. For example, a Splunk instance within a Virtual Private Cloud (VPC) infrastructure.
- Support for disabling the DLQ (Dead Letter Queue) check for SQS-based S3 Crowdstrike event inputs.

The Description input will be deprecated in a future release. The Metadata input has been added as a replacement. The best practice is to begin moving your workloads to the Metadata input.

Fixed issues

Version 5.1.0 of the Splunk Add-on for Amazon Web Services fixes the following, if any, issues.

Date resolved	Issue number	Description
2021-07-30	ADDON-38682	Generic S3 - AttributeError: 'S3KeyReader' object has no attribute 'seekable'
2021-07-05	ADDON-37996	AWS add-on | To confirm if Osaka region on AWS is supported by AWS add-on
2021-06-10	ADDON-37528	modular input does not skip over old "GLACIER" folders and keep trying
2021-05-04	ADDON-34844	AWS sns Alert fails to be sent, only during first occurrence, it works from second trigger onwards
2021-03-15	ADDON-32067	AWS 4.6.1 will not load input/config page
2021-03-08	ADDON-33998	Splunk Add-on for Amazon Web Services 5.0.3 - issues with non default management port
2021-02-11	ADDON-30834	AWS-TA Kinesis Stream Inputs time is wrong
2021-02-11	ADDON-33377	Description Mod input not appending results correctly
2021-02-07	ADDON-29812	AWS security-group-rule description is missing in AWS TA
2021-01-12	ADDON-29815	Wrong start time to S3 input is mistakenly accepted by TA-AWS
2020-12-29	ADDON-22096	AWS Add-on is reporting NULL for NACL data

Known issues

Version 5.1.0 of the Splunk Add-on for Amazon Web Services has the following, if any, known issues.

Date filed	Issue number	Description
2021-11-23	ADDON-45091, ADDON-44250	Splunk Add-on for AWS v5.2.0 does not verify SNS Message signature sent to Splunk via SQS
2021-09-14	ADDON-42117	If Inputs Page page size is more than 25, then the alignment of input details is not consistent
2021-09-07	ADDON-41646	aws:metadata input is populating S3 buckets for AWS accounts where the bucket does not exist.
2021-08-24	ADDON-41009	cloudwatch input timeout issue
2021-07-01	ADDON-38997	<revenue-nsw> custom sourcetype/props is not getting honored and causing the line breaking issue
2021-06-13	ADDON-38108	v5.0.3 - The provided token has expired
2021-06-09	ADDON-37958	The impact of the format change of unstractured field in data events
2021-06-09	ADDON-37970	inputs.conf config generate from code for cloudwatch is not grouped together
2021-05-20	ADDON-37297	Splunk Add-on for AWS fails with TypeError: cannot unpack non-iterable NoneType object
2021-05-19	ADDON-37230	Not ingesting logs on Cloudwatch using AWS add-on:5.0.3
2021-04-22	ADDON-36123	When a role is assumed and a user performs any activity, Splunk extracts the role name as the "username" Workaround: We can easily fix this by using a regex based extraction for userName and user - field=userIdentity.arn ".*\:(?<user_action_type>.*)\/(?<user_role>.*)\/(?<user>.*)"
2021-03-23	ADDON-35020	v5.0.3 fields not extracting correctly

Date filed	Issue number	Description

Third-party software attributions

Version 5.1.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill
- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- requests
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python
- urllib3

Version 5.0.4

Version 5.0.4 of the Splunk Add-on for Amazon Web Services was released on June 2, 2021.

Compatibility

Version 5.0.4 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.18 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 5.0.4 of the Splunk Add-on for AWS version contains the following new and changed features:

- Simple Queue Service (SQS) modular input support for Crowdstrike Falcon Data Replicator (FDR)
- Bug fixes.

Fixed issues

Version 5.0.4 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2021-06-28	ADDON-36953	AWS TA is not loading kinesis data post upgrade from 4.5.0 to 5.0.3
2021-05-18	ADDON-36305	Getting error in splunkd.log when user tries to fresh install the addon and inputs page is not loading for the TA

Known issues

Version 5.0.4 of the Splunk Add-on for Amazon Web Services has the following, if any, known issues.

The Splunk Add-on for AWS version 5.x.x is incompatible with Splunk Enterprise versions 7.x.x and earlier.

Date filed	Issue number	Description
2021-09-14	ADDON-42117	If Inputs Page page size is more than 25, then the alignment of input details is not consistent
2021-06-25	ADDON-38682	Generic S3 - AttributeError: 'S3KeyReader' object has no attribute 'seekable'

Third-party software attributions

Version 5.0.4 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill
- Bootstrap
- boto
- boto3
- botocore
- dateutils

- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- requests
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python
- urllib3

Version 5.0.3

Version 5.0.3 of the Splunk Add-on for Amazon Web Services was released on October 8, 2020.

Compatibility

Version 5.0.3 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

The field alias functionality is compatible with the current version of this add-on. The current version of this add-on does not support older field alias configurations.

For more information about the field alias configuration change, refer to the Splunk Enterprise Release Notes.

New features

Version 5.0.3 of the Splunk Add-on for AWS version contains the following new and changed features:

- Bug fix with proxy behavior not working as expected.
- Bug fix with `no_proxy` taking effect with https.
- SQS modular input for proxy configuration code fix (Microsoft Windows only)

Fixed issues

Version 5.0.3 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Known issues

Version 5.0.3 of the Splunk Add-on for Amazon Web Services has the following known issues.

The Splunk Add-on for AWS version 5.x.x is incompatible with Splunk Enterprise versions 7.x.x and earlier.

Date filed	Issue number	Description
2021-09-14	ADDON-42117	If Inputs Page page size is more than 25, then the alignment of input details is not consistent
2021-08-24	ADDON-41009	cloudwatch input timeout issue
2021-07-01	ADDON-38997	<revenue-nsw> custom sourcetype/props is not getting honored and causing the line breaking issue
2021-06-13	ADDON-38108	v5.0.3 - The provided token has expired
2021-06-11	ADDON-37996	AWS add-on | To confirm if Osaka region on AWS is supported by AWS add-on
2021-06-09	ADDON-37958	The impact of the format change of unstractured field in data events
2021-06-01	ADDON-37528	modular input does not skip over old "GLACIER" folders and keep trying
2021-05-20	ADDON-37297	Splunk Add-on for AWS fails with TypeError: cannot unpack non-iterable NoneType object
2021-05-12	ADDON-36953	AWS TA is not loading kinesis data post upgrade from 4.5.0 to 5.0.3
2021-04-29	ADDON-36305	Getting error in splunkd.log when user tries to fresh install the addon and inputs page is not loading for the TA
2021-04-22	ADDON-36123	When a role is assumed and a user performs any activity, Splunk extracts the role name as the "username" Workaround: We can easily fix this by using a regex based extraction for userName and user - field=userIdentity.arn ".*\:(?<user_action_type>.*)\/(?<user_role>.*)\/(?<user>.*)"
2021-03-26	ADDON-35220	In Splunk_TA_aws KeyError: 'LaunchConfigurationName' appearing when attempting to ingest cloudwatch data
2021-03-23	ADDON-35020	v5.0.3 fields not extracting correctly
2021-02-19	ADDON-33998	Splunk Add-on for Amazon Web Services 5.0.3 - issues with non default management port
2021-01-28	ADDON-33377	Description Mod input not appending results correctly
2020-12-22	ADDON-32067	AWS 4.6.1 will not load input/config page

Third-party software attributions

Version 5.0.3 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill
- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python210
- urllib3

Version 5.0.2

Version 5.0.2 of the Splunk Add-on for Amazon Web Services was released on August 22, 2020.

Compatibility

Version 5.0.2 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

New features

Version 5.0.2 of the Splunk Add-on for AWS version contains the following new and changed features:

- Increased Network Traffic CIM data model compatibility.
- Increased Change CIM data model compatibility.
- Improved support for the Splunk Enterprise Security **Assets and Identities Framework** Interface

Fixed issues

Version 5.0.2 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2020-08-24	ADDON-26632	Update cloudfront_web and cloudfront_rtmp regex to account for ipv6 addresses
2020-08-24	ADDON-26878	Installing AWS TA on Enterprise Security SH breaks Suppression Auditing: stanzas For aws:resthandler:log and aws:util:log are too generic
2020-07-13	ADDON-22785	AWS calls increase when using aws:description
2020-07-13	ADDON-26599	Support for newer formatted cloudwatch ELB metrics, exception handling for logs which don't have all log field populated

Known issues

Version 5.0.2 of the Splunk Add-on for Amazon Web Services has the following known issues.

The Splunk Add-on for AWS version 5.x.x is incompatible with Splunk Enterprise versions 7.x.x and earlier.

Date filed	Issue number	Description
2021-09-14	ADDON-42117	If Inputs Page page size is more than 25, then the alignment of input details is not consistent
2021-06-01	ADDON-37528	modular input does not skip over old "GLACIER" folders and keep trying
2020-10-03	ADDON-29815	Wrong start time to S3 input is mistakenly accepted by TA-AWS

Third-party software attributions

Version 5.0.2 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill
- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath

- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python210
- urllib3

Version 5.0.1

Version 5.0.1 of the Splunk Add-on for Amazon Web Services was released on May 13, 2020.

Compatibility

Version 5.0.1 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

Versions 5.0.0 and above of the Splunk Add-on for AWS are Python 3 releases, and only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 or above on these versions of the Splunk platform.

New features

Version 5.0.1 of the Splunk Add-on for AWS version contains the following new and changed features:

- FIPS compliance release for Python 3
- Improved Support for the Authentication CIM Model.

Fixed issues

Version 5.0.1 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date	Issue number	Description

resolved		
2020-06-16	ADDON-25762	Generic AWS S3 inputs duplicating events after Splunk forwarder restart
2020-04-29	ADDON-24651	Improved ALB Access Logs parsing
2020-04-29	ADDON-21349, CMON-2382	Fix for S3 field extraction
2020-04-23	ADDON-21900	Input validation needed for AWS inputs to check for / (forward slash)
2020-04-23	ADDON-25454, ADDON-26096	Splunk Add-on for AWS repeatedly processing the same gzip file
2020-04-23	ADDON-25279	FIPS compliance release for Python 3
2020-04-23	ADDON-23358	Improvement to timestamp extraction for sourcetype aws:cloudwatchlogs:vpcflow
2020-04-23	ADDON-24325	AWS TA only ingesting up to 100 RDS instances.
2020-03-23	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2020-03-11	ADDON-25546, ADDON-25289	Region support improved for AWS Description: adding ap-east-1, eu-north-1, eu-west-3 and me-south-1

Known issues

Version 5.0.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

The Splunk Add-on for AWS version 5.x.x is incompatible with Splunk Enterprise versions 7.x.x and earlier.

Date filed	Issue number	
2020-05-26	ADDON-26878	Installing AWS TA on Enterprise Security SH breaks Suppression Auditing: stanzas For aws:resthandler:log and aws:util:log Workaround: Edit default/props.conf and change the lines [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)spl to [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splu
2020-05-14	ADDON-26632	Update cloudfront_web and cloudfront_rtmp regex to account for ipv6 addresses Workaround: Update local/props.conf with the following changes {code:java} [aws:cloudfront:accesslogs] EXTRACT-cloudfront_web = ^\s*(?P<date>[0-9-]+)\s+(?P[0-9:]+)\s+(?P<x_edge_location>[^\s]+)\s+(?P<sc_bytes>\d+)\s+(?P<c_ip>[EXTRACT-cloudfront_rtmp = ^\s*(?P<date>[0-9-]+)\s+(?P[0-9:]+)\s+(?P<x_edge_location>[^\s]+)\s+(?P
2020-05-13	ADDON-26599	Support for newer formatted cloudwatch ELB metrics, exception handling for logs which don't have all log field populated
2019-08-02	ADDON-22785	AWS calls increase when using aws:description

Date filed	Issue number	

Third-party software attributions

Version 5.0.1 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill
- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python210
- urllib3

Version 5.0.0

Version 5.0.0 of the Splunk Add-on for Amazon Web Services was released on December 19, 2019.

Compatibility

Version 5.0.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	8.0 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

Version 5.0.0 of the Splunk Add-on for AWS is a Python 3 release and is only compatible with Splunk platform versions 8.0.0 and later. To use version 5.0.0 or later of this add-on, upgrade your Splunk platform deployment to version 8.0.0 or later. For users of Splunk platforms 6.x.x and Splunk 7.x.x, the Splunk Add-on for Amazon Web Services version 4.6.1 is supported. Do not upgrade to Splunk Add-on for AWS 5.0.0 on these versions of the Splunk platform.

New features

Version 5.0.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- Support for Python3
- Python2 is no longer supported, starting in version 5.0.0 of the Splunk Add-on for AWS.

Fixed issues

Version 5.0.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2020-09-02	ADDON-29101, ADDON-21459	Make the naming convention of CloudWatch metric events compatible with SAI

Known issues

Version 5.0.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

- The Splunk Add-on for AWS version 5.x.x is incompatible with Splunk Enterprise versions 7.x.x and earlier.

Date filed	Issue number	
2020-10-02	ADDON-29812	AWS security-group-rule description is missing in AWS TA
2020-05-14	ADDON-26632	Update cloudfront_web and cloudfront_rtmp regex to account for ipv6 addresses Workaround: Update local/props.conf with the following changes {code:java} [aws:cloudfront:accesslogs] EXTRACT-cloudfront_web = ^\s*(?P<date>[0-9-]+)\s+(?P[0-9:]+)\s+(?P<x_edge_location>[^\s]+)\s+(?P<sc_bytes>\d+)\s+(?P<c_ip> EXTRACT-cloudfront_rtmp = ^\s*(?P<date>[0-9-]+)\s+(?P[0-9:]+)\s+(?P<x_edge_location>[^\s]+)\s+(?P
2020-05-13	ADDON-26599	Support for newer formatted cloudwatch ELB metrics, exception handling for logs which don't have all log field populated

2020-03-23	ADDON-25762	Generic AWS S3 inputs duplicating events after Splunk forwarder restart
		
		Workaround:
		Lookup following code block in file bin/splunk_ta_aws/modinputs/generic_s3/s3_key_reader.py.
		
		should be line 109 - 112
		
		if size == 0:
		
		`size = self.bufsize`

Date filed	Issue number	

		data = self._config[asc.key_object].read(size) Insert two lines like this:
		
		if size == 0:
		`size = self.bufsize`
		if self._reached_eof:
		`return b`
		data = self._config[asc.key_object].read(size)

2020-03-09	ADDON-25546, ADDON-25289	Region support improved for AWS Description: adding ap-east-1, eu-north-1, eu-west-3 and me-south-1
2020-03-04	ADDON-25454, ADDON-26096	Splunk Add-on for AWS repeatedly processing the same gzip file
2020-02-12	ADDON-25279	FIPS compliance release for Python 3
2019-12-12	ADDON-24651	Improved ALB Access Logs parsing
2019-11-14	ADDON-24325	AWS TA only ingesting up to 100 RDS instances.

2019-09-22	ADDON-23358	Improvement to timestamp extraction for sourcetype aws:cloudwatchlogs:vpcflow
		
		Workaround:
		Manually update sourcetype aws:cloudwatchlogs:vpcflow with TIME_FORMAT and TIME_PREFIX settings.
		For example:
		`TIME_FORMAT = %s`
		`TIME_PREFIX = ^(?>\S+\s){10}`
		`MAX_TIMESTAMP_LOOKAHEAD = 10`

2019-08-02	ADDON-22785	AWS calls increase when using aws:description
2019-04-29	ADDON-21900	Input validation needed for AWS inputs to check for / (forward slash)
2019-02-15	ADDON-21349, CMON-2382	Fix for S3 field extraction
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name

Third-party software attributions

Version 5.0.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- atomicwrites
- babel-polyfill

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- jquery.ui.autocomplete
- Httplib2
- Python SortedContainer
- remote-pdb
- s3transfer
- select2
- six.py
- SortedContainers
- u-msgpack-python210
- urllib3

Version 4.6.1

Version 4.6.1 of the Splunk Add-on for Amazon Web Services was released on December 10, 2019.

Compatibility

Version 4.6.1 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	6.5 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

New features

Version 4.6.1 of the Splunk Add-on for AWS version contains the following new and changed features:

- FIPS compliance
- Updated third party components

Fixed issues

Version 4.6.1 of the Splunk Add-on for Amazon Web Services fixes the following issues. If no issues appear below, no issues have yet been fixed.

Known issues

Version 4.6.1 of the Splunk Add-on for Amazon Web Services has the following known issues. If no issues appear below, no issues have yet been reported.

Date filed	Issue number	Description
2021-01-12	ADDON-32838	When using generic S3 to get S3 bucket, TA should start reading file from initial_scan_datetime
2020-12-22	ADDON-32067	AWS 4.6.1 will not load input/config page
2020-05-26	ADDON-26878	Installing AWS TA on Enterprise Security SH breaks Suppression Auditing: stanzas For aws:resthandler:log and aws:util:log are too generic Workaround: Edit default/props.conf and change the lines [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*util.log*] to [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*util.log*]
2020-03-09	ADDON-25546, ADDON-25289	Region support improved for AWS Description: adding ap-east-1, eu-north-1, eu-west-3 and me-south-1
2019-12-12	ADDON-24651	Improved ALB Access Logs parsing
2019-02-15	ADDON-21349, CMON-2382	Fix for S3 field extraction

Third-party software attributions

Version 4.6.1 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- requests
- SortedContainers
- select2
- splunksdk
- u-msgpack-python
- urllib3

Version 4.6.0

Version 4.6.0 of the Splunk Add-on for Amazon Web Services was released on October 3, 2018.

Compatibility

Version 4.6.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms:

Splunk platform versions	6.5 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

New features

Version 4.6.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- CloudWatch Metrics input to enable discovery of new entities without Splunk restart
- Metrics store support (requires a Splunk forwarder version 7.2.0 or above.)
- Ability to detect configuration of SSL on management port
- Line/event breaking enforcement for ELB/S3 Access Logs
- Support for Splunk Enterprise 7.2.0

Fixed issues

Version 4.6.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2018-08-27	ADDON-18031	Small page size causing LimitExceededException error during Kinesis ListStreams operations
2018-07-17	ADDON-18087, SII-1746	Invalid AWS credentials can be added and interacted with as valid AWS credentials
2018-06-27	ADDON-17277	Line/event breaking enforcement for ELB/S3 Access Logs

Known issues

Version 4.6.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2021-06-01	ADDON-37528	modular input does not skip over old "GLACIER" folders and keep trying
2020-11-08	ADDON-30834	AWS-TA Kinesis Stream Inputs time is wrong
2020-09-02		Make the naming convention of CloudWatch metric events compatible with SAI

Date filed	Issue number	Description
	ADDON-29101, ADDON-21459	
2020-05-26	ADDON-26878	Installing AWS TA on Enterprise Security SH breaks Suppression Auditing: stanzas For aws:resthandler:log and aws:util:log are too generic Workaround: Edit default/props.conf and change the lines [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*util.log*] to [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*util.log*]
2019-11-14	ADDON-24325	AWS TA only ingesting up to 100 RDS instances.

2019-09-22	ADDON-23358	Improvement to timestamp extraction for sourcetype aws:cloudwatchlogs:vpcflow
		
		Workaround:
		Manually update sourcetype aws:cloudwatchlogs:vpcflow with TIME_FORMAT and TIME_PREFIX settings.
		
		For example:
		
		`TIME_FORMAT = %s`
		`TIME_PREFIX = ^(?>\S+\s){10}`
		`MAX_TIMESTAMP_LOOKAHEAD = 10`

2019-08-02	ADDON-22785	AWS calls increase when using aws:description
2019-04-29	ADDON-21900	Input validation needed for AWS inputs to check for / (forward slash)
2019-02-15	ADDON-21349, CMON-2382	Fix for S3 field extraction
2018-08-23	ADDON-19179	UI shows error message when a CloudWatch mod input has dimensions with different query_window_size
2018-08-16	ADDON-19138	Splunk 7.1 and below outputs 'Invalid key in stanza' warning on startup about INGEST_EVAL, METRIC-SCHEMA-MEASURES, and METRIC-SCHEMA-TRANSFORMS
2018-03-28	ADDON-17571	AWS TA and *nix TA lack spec files for eventgen.conf, which causes cluster bundle validation errors, and breaks Manage Indexes page in clustered Splunk Cloud Workaround: Splunk Cloud customers who cannot create indexes on their own due to this bug should file a support case when they need new indexes created.
2018-02-19	ADDON-17158	The style of multi-input text box is not correct
2018-02-19	ADDON-17157	The header view of customized page is inconsistent with the default NightLight style
2018-02-13	ADDON-17132	Create/edit input page layout is broken
2018-02-13	ADDON-17135	Placeholder tooltip is missing for dropdown
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround:

Date filed	Issue number	Description
		Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-09-03	ADDON-15718	Duplicate cloudfront data in description when there are more than 1 regions
2017-08-22	ADDON-15603	Users can delete an account in use.
2017-03-29	ADDON-14287	After you replace an IAM role attached to an EC2 instance, the inputs that use the old IAM role stop collecting data.
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.

Third-party software attributions

Version 4.6.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.5.0

Version 4.5.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.5 and later
CIM	4.3 and later
Supported OS for data collection	Platform independent
Vendor products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

New features

Version 4.5.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- Support for the configuration of billing inputs to collect Cost and Usage Report data (sourcetype: `aws:billing:cur`).

Fixed issues

Version 4.5.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2018-01-22	ADDON-15918	AWS TA is unable to validate role ARNs with "/" in path
2018-01-22	ADDON-16435	AWS - Getting error trying to connect to CloudTrail using SQS Based S3 - EU-WEST-1

Known issues

Version 4.5.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2020-05-26	ADDON-26878	Installing AWS TA on Enterprise Security SH breaks Suppression Auditing: stanzas For aws:resthandler:log and aws:util:log are too generic Workaround: Edit default/props.conf and change the lines [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*util.log*] to [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*rest*.log*] [source::...(/|\\)var(/|\\)log(/|\\)splunk(/|\\)*Splunk_TA_aws*util.log*]
2019-06-03	ADDON-22096	AWS Add-on is reporting NULL for NACL data
2019-02-15	ADDON-21349, CMON-2382	Fix for S3 field extraction
2018-08-22	ADDON-19171	Cannot add regions when configuring Inspector inputs for the TA for AWS
2018-05-17	ADDON-18087, SII-1746	Invalid AWS credentials can be added and interacted with as valid AWS credentials
2018-05-09	ADDON-18031	Small page size causing LimitExceededException error during Kinesis ListStreams operations
2018-03-28	ADDON-17571	AWS TA and *nix TA lack spec files for eventgen.conf, which causes cluster bundle validation errors, and breaks Manage Indexes page in clustered Splunk Cloud Workaround: Splunk Cloud customers who cannot create indexes on their own due to this bug should file a support case when they need new indexes created.

Date filed	Issue number	Description
2018-02-27	ADDON-17277	Line/event breaking enforcement for ELB/S3 Access Logs
2018-02-19	ADDON-17158	The style of multi-input text box is not correct
2018-02-19	ADDON-17157	The header view of customized page is inconsistent with the default NightLight style
2018-02-13	ADDON-17135	Placeholder tooltip is missing for dropdown
2018-02-13	ADDON-17132	Create/edit input page layout is broken
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround: Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-09-03	ADDON-15718	Duplicate cloudfront data in description when there are more than 1 regions
2017-09-01	ADDON-15712	It stops pulling Kinesis stream data when the Kinesis stream is resharded
2017-08-22	ADDON-15603	Users can delete an account in use.
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.

Third-party software attributions

Version 4.5.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.4.0

Version 4.4.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.5 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

New features

Version 4.4.0 of the Splunk Add-on for AWS version contains the following new and changed features:

- Splunk Add-on for AWS 4.4.0 is only compatible with Splunk App for AWS 5.1.0. Previous versions of Splunk App for AWS are not supported.
- Optimized Web UI for better usability and more streamlined configuration workflow
  - The **Create New Input** menu has been redesigned with all the menu options organized by the type of data to collect.
  - Two separate configuration pages are now available for Generic S3 and Incremental S3 input types respectively. Previously, the two different input types were configured in one configuration page.
  - Input configuration fields are now grouped into **AWS Input Configuration**, **Splunk-related Configuration**, and **Advanced Settings** sections on the Web UI.
  - Redesigned input configuration UIs for CloudWatch and Config input types let you create multiple inputs all at once.
- Added a new **Temp Folder** setting to the Billing input type configuration, which lets you specify a non-default folder for temporarily storing downloaded detailed billing report .zip files when the system default temp folder does not provide sufficient space.
- You can now configure SQS-based S3 inputs to index non-AWS custom logs in plain text in addition to its supported AWS log types.
- SQS-based S3 input type now supports CloudTrail and Config SQS notifications.
- Assume Role is now supported in SQS, Config Rule, and Inspector input types.
- The Description input type now supports the iam_users service.

Upgrade

To upgrade from versions 4.3 and below, AWS users must be given permission to use the `ec2:RunInstances` API action, and depending on deployment, the following API actions:

API Action	Description
`ec2:DescribeImages`	Allows users to view and select an AMI.
`ec2:DescribeVpcs`	Allows users to view the available EC2-Classic and virtual private clouds (VPCs) network options. This API action is required even if you are not launching into a VPC.
`ec2:DescribeSubnets`	Allows users to view all available subnets for the chosen VPC, when launching into a VPC.
`ec2:DescribeSecurityGroups`	Allows users to view the security groups page in the wizard. Users can select an existing security group.
`ec2:DescribeKeyPairs` or `ec2:CreateKeyPair`	Allows users to select an existing key pair, or create a new key pair.

See Configure Description permissions for more information on how to configure AWS permissions.

See the AWS documentation for more information on the **DescribeImages** function.
https://docs.aws.amazon.com/AWSEC2/latest/APIReference/API_DescribeImages.html.

Fixed issues

Version 4.4.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2017-08-03	ADDON-14890	Add-on truncates Kinesis stream dropdown to 20 items.
2017-07-27	ADDON-12700	Pagination issue in Account page.
2017-07-11	ADDON-11974	Cannot get CloudWatch data using some default configuration in Add-on
2017-05-25	ADDON-13282	Cannot change Description interval in UI more than once

Known issues

Version 4.4.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2021-08-05	ADDON-40189	addon 2648 shows inputs page from app 3670 CISCO AMP for Endpoints Events Input
2021-08-05	ADDON-40188	addon 3185 shows inputs page from app 3670 CISCO AMP for Endpoints Events Input
2018-08-22	ADDON-19171	Cannot add regions when configuring Inspector inputs for the TA for AWS
2018-05-17	ADDON-18087, SII-1746	Invalid AWS credentials can be added and interacted with as valid AWS credentials
2018-03-28	ADDON-17571	AWS TA and *nix TA lack spec files for eventgen.conf, which causes cluster bundle validation errors, and breaks Manage Indexes page in clustered Splunk Cloud Workaround: Splunk Cloud customers who cannot create indexes on their own due to this bug should file a support case when they need new indexes created.
2018-02-27	ADDON-17277	Line/event breaking enforcement for ELB/S3 Access Logs
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround: Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-12-20	ADDON-16435	AWS - Getting error trying to connect to CloudTrail using SQS Based S3 - EU-WEST-1
2017-09-21	ADDON-15918	AWS TA is unable to validate role ARNs with "/" in path
2017-09-03	ADDON-15718	Duplicate cloudfront data in description when there are more than 1 regions
2017-09-01	ADDON-15712	It stops pulling Kinesis stream data when the Kinesis stream is resharded
2017-08-22	ADDON-15603	Users can delete an account in use.
2017-08-19	ADDON-15578	On Windows, fails to rotate CloudWatch and Incremental S3 logs when indexing speed cannot catch up with data collection
2017-07-25	ADDON-15371	Add-on should support non-UTF fields in access logs.
2017-03-29	ADDON-14287	

Date filed	Issue number	Description
		After you replace an IAM role attached to an EC2 instance, the inputs that use the old IAM role stop collecting data.
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.

Third-party software attributions

Version 4.4.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.3.0

Version 4.3.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.4 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Logs, Billing services, SQS, and SNS.

New features

Version 4.3.0 of the Splunk Add-on for AWS contains the following new and changed features:

- SQS-based S3 input type
  A multi-purpose input type that collects several types of logs in response to messages polled from SQS queues. A

scalable and higher-performing alternative to the generic S3 and incremental S3 input types. See Multi-purpose input types.
- Heath Check dashboards
  Health Overview and S3 Health dashboards to help you troubleshoot data collection errors and performance issues. See Health Check dashboards.
- Optimized logging. See Internal logs.

Fixed issues

Version 4.3.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2017-06-09	ADDON-13860	Configuring more AWS accounts increases CPU usage and lowers throughput performance due to increased API calls
2017-06-07	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud
2017-05-10	ADDON-14039	Incremental S3 input fails to decode non-utf8 encoded files
2017-05-10	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-03-23	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-03-06	ADDON-11846, SPL-138046	Logging breaks on rotation when multiple inputs write to the same log. If > 6 inputs, some inputs cannot log
2017-02-28	ADDON-13867	Major performance issue for incremental S3 data inputs when ingesting large plain text files (max throughput only around 4MB/s for files of size 20MB)

Known issues

Version 4.3.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround: Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-09-21	ADDON-15918	AWS TA is unable to validate role ARNs with "/" in path
2017-09-03	ADDON-15718	Duplicate cloudfront data in description when there are more than 1 regions
2017-09-01	ADDON-15712	It stops pulling Kinesis stream data when the Kinesis stream is resharded
2017-07-25	ADDON-15371	Add-on should support non-UTF fields in access logs.
2017-06-29	ADDON-15188	Too long input name lead to modular input failure
2017-03-29	ADDON-14287	After you replace an IAM role attached to an EC2 instance, the inputs that use the old IAM role stop collecting data.

Date filed	Issue number	Description
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.
2016-12-14	ADDON-12700	Pagination issue in Account page.

Third-party software attributions

Version 4.3.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.2.3

Version 4.2.3 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.4 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.2.3 of the Splunk Add-on for AWS does not contain any new features.

Fixed issues

Version 4.2.3 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2017-04-26	ADDON-13891	The S3 incremental input fails to skip the Glacier storage type keys
2017-04-16	ADDON-11326	Unexpected timestamp format blocks data ingestion
2017-04-06	ADDON-13768	Upgrading the add-on causes the EC2 configuration in the Splunk App for AWS to fail with IAM Role

Known issues

Version 4.2.3 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2017-09-03	ADDON-15718	Duplicate cloudfront data in description when there are more than 1 regions
2017-09-01	ADDON-15712	It stops pulling Kinesis stream data when the Kinesis stream is resharded
2017-06-22	ADDON-15124	Logging breaks on rotation for Billing & AWS Config when multiple inputs write to the same log.
2017-05-24	ADDON-14890	Add-on truncates Kinesis stream dropdown to 20 items.
2017-03-29	ADDON-14287	After you replace an IAM role attached to an EC2 instance, the inputs that use the old IAM role stop collecting data.
2017-03-09	ADDON-14038	Orphan process issue after master process been force killed
2017-03-09	ADDON-14039	Incremental S3 input fails to decode non-utf8 encoded files
2017-02-27	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud
2017-02-27	ADDON-13867	Major performance issue for incremental S3 data inputs when ingesting large plain text files (max throughput only around 4MB/s for files of size 20MB)
2017-02-27	ADDON-13879	Regional Reserve Instance is missing in description data
2017-02-26	ADDON-13860	Configuring more AWS accounts increases CPU usage and lowers throughput performance due to increased API calls Workaround: Consolidate AWS accounts when configuring the Splunk Add-on for AWS.
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2017-02-19	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-02-06	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-01-13	ADDON-13282	Cannot change Description interval in UI more than once
2016-12-28	ADDON-12983	S3 dead loop when processing extremely large S3 files
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround:

Date filed	Issue number	Description
		To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.
2016-12-14	ADDON-12700	Pagination issue in Account page.
2016-11-21	ADDON-12267	Disabling an active incremental s3 data input may cause duplicate data

Third-party software attributions

Version 4.2.3 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.2.2

Version 4.2.2 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.2.2 of the Splunk Add-on for AWS does not contain any new features.

Fixed issues

Version 4.2.2 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2017-01-21	ADDON-13369	Failed to list S3 buckets and Kinesis streams in GUI in proxy mode

Known issues

Version 4.2.2 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2017-03-29	ADDON-14287	After you replace an IAM role attached to an EC2 instance, the inputs that use the old IAM role stop collecting data.
2017-03-09	ADDON-14038	Orphan process issue after master process been force killed
2017-03-09	ADDON-14039	Incremental S3 input fails to decode non-utf8 encoded files
2017-02-28	ADDON-13891	The S3 incremental input fails to skip the Glacier storage type keys
2017-02-27	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud
2017-02-27	ADDON-13867	Major performance issue for incremental S3 data inputs when ingesting large plain text files (max throughput only around 4MB/s for files of size 20MB)
2017-02-26	ADDON-13860	Configuring more AWS accounts increases CPU usage and lowers throughput performance due to increased API calls Workaround: Consolidate AWS accounts when configuring the Splunk Add-on for AWS.
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2017-02-19	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-02-06	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-01-13	ADDON-13282	Cannot change Description interval in UI more than once
2016-12-28	ADDON-12983	S3 dead loop when processing extremely large S3 files
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.
2016-11-21	ADDON-12267	Disabling an active incremental s3 data input may cause duplicate data

Third-party software attributions

Version 4.2.2 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils

- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.2.1

Version 4.2.1 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Added support for two new AWS regions: EU (London) and Canada (Central).

Fixed issues

Version 4.2.1 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2017-01-12	ADDON-13260	Error message during restart Splunk on EC2 instance
2017-01-11	ADDON-13209	Unexpected SQS message increases the size of the checkpoint file in SQS-based CloudTrail input and causes performance drop
2017-01-09	ADDON-11838	Cloudtrail event username mismatch between AWS console and app
2017-01-06	ADDON-12874	ExpiredToken error when calling the ListObjects operation may terminate the process

Known issues

Version 4.2.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2017-02-27	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud

Date filed	Issue number	Description
2017-02-27	ADDON-13867	Major performance issue for incremental S3 data inputs when ingesting large plain text files (max throughput only around 4MB/s for files of size 20MB)
2017-02-26	ADDON-13860	Configuring more AWS accounts increases CPU usage and lowers throughput performance due to increased API calls Workaround: Consolidate AWS accounts when configuring the Splunk Add-on for AWS.
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2017-02-19	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-02-09	ADDON-13768	Upgrading the add-on causes the EC2 configuration in the Splunk App for AWS to fail with IAM Role
2017-02-06	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-01-19	ADDON-13369	Failed to list S3 buckets and Kinesis streams in GUI in proxy mode
2017-01-13	ADDON-13282	Cannot change Description interval in UI more than once
2016-12-28	ADDON-12983	S3 dead loop when processing extremely large S3 files
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.
2016-11-21	ADDON-12267	Disabling an active incremental s3 data input may cause duplicate data

Third-party software attributions

Version 4.2.1 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.2.0

Version 4.2.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3 and later
CIM	4.3 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.2.0 of the Splunk Add-on for Amazon Web Services supports the AWS Security Token Service (AWS STS) AssumeRole API action that lets you use IAM roles to delegate permissions to IAM users to access these AWS resources. You can configure accounts to use AssumeRole in these data inputs: S3 (general and incremental), Billing, Description, CloudWatch, Kinesis.

Fixed issues

Version 4.2.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2016-12-27	ADDON-12918	API throttling error occurs during ingestion of ELB description input data and blocks ELB data collection
2016-12-12	ADDON-12600	Incorrect file name format blocks data ingestion
2016-12-12	ADDON-12660	Failed to retrieve cloudfront_distributions through proxy
2016-12-07	ADDON-12342	Poor list bucket performance in collecting S3 data
2016-12-07	ADDON-12344	Unwarranted config changed message in the S3 incremental input log
2016-12-06	ADDON-12236	Force killing splunkd leaves input orphan processes, which will be killed after splunkd restarts
2016-12-06	ADDON-12123, ADDON-12485	Race condition after checkpoint files are replaced
2016-12-06	ADDON-12397	One invalid Kinesis input blocks all other Kinesis inputs
2016-12-06	ADDON-12340	ReadTimeoutError - S3 data collection failed
2016-11-28	ADDON-11855, ADDON-11852	Performance degradation of AWS add-on modular input data collection in Splunk Platform 6.5.0
2016-11-27	ADDON-11894, ADDON-12867	S3-generic input ckpt file is too large

Known issues

Version 4.2.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround: Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-02-27	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud
2017-02-26	ADDON-13860	Configuring more AWS accounts increases CPU usage and lowers throughput performance due to increased API calls Workaround: Consolidate AWS accounts when configuring the Splunk Add-on for AWS.
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2017-02-19	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-02-06	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-01-19	ADDON-13369	Failed to list S3 buckets and Kinesis streams in GUI in proxy mode
2017-01-13	ADDON-13282	Cannot change Description interval in UI more than once
2017-01-11	ADDON-13260	Error message during restart Splunk on EC2 instance
2017-01-05	ADDON-13209	Unexpected SQS message increases the size of the checkpoint file in SQS-based CloudTrail input and causes performance drop
2017-01-02	ADDON-13041	s3 indexing latency introduced by assumerole feature (even account do not have assumerole)
2016-12-28	ADDON-12983	S3 dead loop when processing extremely large S3 files
2016-12-27	ADDON-12931	Upgrading from version 4.0.0 to 4.2.0 causes the Start Date/Time field value to be displayed incorrectly on the UI
2016-12-24	ADDON-12874	ExpiredToken error when calling the ListObjects operation may terminate the process
2016-12-22	ADDON-12867, ADDON-11894	S3 input: large key numbers lead to excessively large checkpoint files Workaround: To migrate to SQS based S3 or Incremental S3. Large number of files always leads to large size of checkpoint by the nature of Generic S3. This will improve the checkpoint file size, however, as long as the Jira is not fixed, the checkpoint file size might still be not as little as expected.
2016-12-14	ADDON-12700	Pagination issue in Account page.
2016-11-21	ADDON-12267	Disabling an active incremental s3 data input may cause duplicate data
2016-10-27	ADDON-11838	Cloudtrail event username mismatch between AWS console and app
2016-09-08	ADDON-11225	Fails to download Billing files due to "Operation timed out" error

Date filed	Issue number	Description
2015-09-09	ADDON-12762	Selecting all regions and all services in CloudWatch input results in some invalid tasks.

Third-party software attributions

Version 4.2.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.1.2

Version 4.1.2 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3, 6.4, 6.5
CIM	4.3 or later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.1.2 of the Splunk Add-on for Amazon Web Services contains no new features.

Fixed issues

Version 4.1.2 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Date resolved	Issue number	Description
2016-11-16	ADDON-12078	S3 incremental orphan process issue
2016-11-08	ADDON-11960	App menu display issue in Splunk Light

Known issues

Version 4.1.2 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2018-01-05	ADDON-16518	When kinesis and cloudwatch inputs send large volumes of data over HEC, HEC can block the ingest pipeline, which breaks non-HEC inputs. Workaround: Set use_hec=false in [global_settings] stanza of aws_kinesis.conf and/or aws_cloudwatch.conf
2017-02-27	ADDON-13865	Cannot disable/enable inputs under sc_admin role in Splunk Cloud
2017-02-24	ADDON-13856, ADDON-13200	Add input name as part of Kinesis checkpoint file name
2017-02-19	ADDON-13651	Describe EC2 is blocked by API throttling of get EBS snapshot data
2017-02-06	ADDON-13492, ADDON-13015, ADDON-13855	Ingesting a continuous stream of large files (e.g., 20MB) from a single incremental S3 data input may cause out-of-memory error
2017-01-13	ADDON-13282	Cannot change Description interval in UI more than once
2017-01-05	ADDON-13209	Unexpected SQS message increases the size of the checkpoint file in SQS-based CloudTrail input and causes performance drop
2016-12-26	ADDON-12918	API throttling error occurs during ingestion of ELB description input data and blocks ELB data collection
2016-12-12	ADDON-12660	Failed to retrieve cloudfront_distributions through proxy
2016-11-25	ADDON-12395	File descriptor leaking in generic S3 due to boto2 defects
2016-11-23	ADDON-12342	Poor list bucket performance in collecting S3 data
2016-11-23	ADDON-12340	ReadTimeoutError - S3 data collection failed
2016-11-21	ADDON-12267	Disabling an active incremental s3 data input may cause duplicate data
2016-11-18	ADDON-12236	Force killing splunkd leaves input orphan processes, which will be killed after splunkd restarts
2016-11-08	ADDON-11974	Cannot get CloudWatch data using some default configuration in Add-on
2016-10-28	ADDON-11846, SPL-138046	Logging breaks on rotation when multiple inputs write to the same log. If > 6 inputs, some inputs cannot log
2016-09-08	ADDON-11225	Fails to download Billing files due to "Operation timed out" error

Third-party software attributions

Version 4.1.2 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation

- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.1.1

Version 4.1.1 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3, 6.4 and 6.5
CIM	4.3 or later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.1.1 of the Splunk Add-on for Amazon Web Services contains no new features.

Fixed issues

Version 4.1.1 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Issue number	Description
2016-10-12	ADDON-11604	Incremental S3 fails to collect data using the IAM role.
2016-09-30	ADDON-11470	The inputs page cannot display more than 30 inputs (S3 as input).
2016-10-11	ADDON-11498, ADDON-11488	Ingesting data from aws:cloudwatchlogs results in invalid JSON format with extraneous trailing angle brackets.
2016-10-04	ADDON-11482	Cloudtrail/SQSâ fails to collect data using the IAM role.

Known issues

Version 4.1.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2016-12-26	ADDON-12918	API throttling error occurs during ingestion of ELB description input data and blocks ELB data collection
2016-11-23	ADDON-12342	Poor list bucket performance in collecting S3 data
2016-11-17	ADDON-12232	Get S3 error during upgrade from 4.0.0
2016-11-14	ADDON-12123, ADDON-12485	Race condition after checkpoint files are replaced

Date filed	Issue number	Description
2016-11-10	ADDON-12072	Do not support Splunk global proxy. Update it in add-on configuration if needed.
2016-11-10	ADDON-12078	S3 incremental orphan process issue
2016-11-08	ADDON-11974	Cannot get CloudWatch data using some default configuration in Add-on
2016-11-07	ADDON-11960	App menu display issue in Splunk Light
2016-11-02	ADDON-11893	IO exception in S3 input
2016-11-02	ADDON-11894, ADDON-12867	S3-generic input ckpt file is too large
2016-10-30	ADDON-11855, ADDON-11852	Performance degradation of AWS add-on modular input data collection in Splunk Platform 6.5.0
2016-10-28	ADDON-11847	s3 input zombie processes Workaround: Update the symbolic link so that /bin/sh targets /bin/bash. $ debconf-set-selections <<< "dash dash/sh string false" $ dpkg-reconfigure -f noninteractive dash
2016-10-28	ADDON-11846, SPL-138046	Logging breaks on rotation when multiple inputs write to the same log. If > 6 inputs, some inputs cannot log
2016-09-22	ADDON-11415	The input name is case sensitive lead to failure on Windows platform
2016-09-13	ADDON-11295	Cloudtrail still delete SQS message even if failed to get S3 file
2016-09-08	ADDON-11225	Fails to download Billing files due to "Operation timed out" error
2016-08-18	ADDON-10957	Log level set to ERROR but still found INFO logs
2016-06-20	ADDON-10286	CloudWatch modular input generates duplicate events when the Splunk platform is restarted Workaround: dedup based on the _time field
2016-05-30	ADDON-9753	Proxy password does not support the special characters '|', ':' or '@'
2016-05-12	ADDON-9435	Wrong number of inputs listed on Account page.
2016-05-12	ADDON-9422	CloudWatch input can have data loss when empty results are returned twice in succession and then Splunk platform restarts before the input next collects data.
2016-05-11	ADDON-9408	Detailed Billing is not indexed using UTC timezone
2016-05-11	ADDON-9409	Checkpoints file will not be removed when deleting Config Rules
2016-05-07	ADDON-9332	fails to get latest cloudwatch data sometimes
2016-04-29	ADDON-9148	Updating directly from v2.0.0 to v4.0.0 makes existing accounts unavailable
2016-04-28	ADDON-9133	CloudWatch default configuration may not work in cases where there are millions of dimensions
2016-04-28	ADDON-9145	Error message shown on input creation screen has logic issues and is not as specific as we could be
2016-01-13	ADDON-7448	In the Description data input, the port range defaults to null in vpc_network_acls if no range is specified, which is confusing, because it actually has a range of "all".
2015-12-29	ADDON-7239	Using "/" in data input name causes exceptions. UI does not accept this character in the input names, but if you configure your input using conf files, you will find exceptions in logs.

Date filed	Issue number	Description
2015-12-22	ADDON-7159	After removing all search peers, add-on still shows performance warnings. Workaround: Restart a Splunk platform instance after changing its role.
2015-12-16	ADDON-7035	Add-on ingests the header line of the CloudFront access log, but it should be skipped.
2015-11-26	ADDON-6701	EC2, RDS, ELB, and EC2 APIs do not consider pagination.
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.
2015-04-02	ADDON-3578	S3: uppercase bucket names cause an error
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart the Splunk platform after deleting or modifying an AWS account.
2014-09-25	ADDON-2113	The app.conf file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. Workaround: This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in app.conf.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.

Third-party software attributions

Version 4.1.1 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath

- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.1.0

Version 4.1.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3, 6.4
CIM	4.3 or later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, Billing services, SQS, and SNS.

New features

Version 4.1.0 of the Splunk Add-on for Amazon Web Services has the following new features.

Date	Issue number	Description
2016-09-22	ADDON-6145	Add AWS SQS modular input for Splunk add-on for AWS.
2016-09-22	ADDON-6146	Add custom alert to AWS SNS for Splunk add-on for AWS.
2016-09-22	ADDON-10952	Performance enhancement for AWS Cloudtrail modular input.
2016-09-22	ADDON-11149	Add **Record Format** field for AWS Kinesis modular input.
2016-09-22	ADDON-10917	Mapping to ITSI IaaS data module.
2016-09-22	ADDON-10941	Add new incremental data collection for S3 modular input.
2016-09-22	ADDON-10414	Checkpoint and performance enhancement for S3 modular input.
2016-09-22	ADDON-10906	Performance and API call enhancement for Cloudwatch modular input.

Fixed issues

Version 4.1.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Issue number	Description
2016-09-20	ADDON-11251	There will be data loss of ASW S3 input if the network connection is bad.
2016-09-20	ADDON-11196	If there is a blank space at the beginning or the end of the input name (or both). The input name displays on the UI is not the consistent with the one saved in the configuration file.
2016-09-20	ADDON-11056	In the AWS Region list, it displays **ap-northeast-2** instead of Seoul.

Resolved date	Issue number	Description
2016-09-20	ADDON-10980	Line breaker error for AWS S3 input.
2016-09-14	ADDON-10186	AWS Config fails to fetch S3 object in AWS GovCloud (US) region.
2016-09-09	ADDON-11009	Vanguard: Not getting data from 1 of 3 S3 inputs. This is considered critical for the customer as they have PS on site.
2016-08-18	ADDON-10137	If the number of the AWS input exceeds 30, some of the inputs cannot run successfully.
2016-09-14	ADDON-9778	There are some errors of AWS Kinesis modular input if the request from HEC exceeds its max limit.
2016-09-05	ADDON-9732	Failed to get proxy credentials when password includes **#** character.
2016-08-28	ADDON-9533	The default Dimension Name is empty square brackets for Autoscaling and EBS namespaces.
2016-08-08	ADDON-9328	CloudWatch data input encounters API rate limit for large metrics.
2016-09-09	ADDON-8758	Mixing log types or gzip with plain text in the same stream causes knowledge extraction to fail for CloudWatch Logs data collected through Kinesis

Known issues

Version 4.1.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2016-10-30	ADDON-11855, ADDON-11852	Performance degradation of AWS add-on modular input data collection in Splunk Platform 6.5.0
2016-10-28	ADDON-11846, SPL-138046	Logging breaks on rotation when multiple inputs write to the same log. If > 6 inputs, some inputs cannot log
2016-10-12	ADDON-11611	Fails to publish search result to SNS using the IAM role.
2016-10-11	ADDON-11604	S3 incremental failed to fetch data using IAM role
2016-10-05	ADDON-11498	Trailing angle bracket and invalid JSON in aws:cloudwatchlogs
2016-10-04	ADDON-11488	aws_cloudwatch_logs_data_loader.py#L88
2016-10-03	ADDON-11482	Cloudtrail input error after upgrade to 4.1
2016-09-28	ADDON-11470	Inputs page doesn't show more than 30 inputs (S3 as input)
2016-09-22	ADDON-11415	The input name is case sensitive lead to failure on Windows platform
2016-09-19	ADDON-11326	Unexpected timestamp format blocks data ingestion
2016-09-13	ADDON-11295	Cloudtrail still delete SQS message even if failed to get S3 file
2016-09-08	ADDON-11225	Fails to download Billing files due to "Operation timed out" error
2016-08-18	ADDON-10957	Log level set to ERROR but still found INFO logs
2016-06-20	ADDON-10286	CloudWatch modular input generates duplicate events when the Splunk platform is restarted Workaround: dedup based on the _time field
2016-05-30	ADDON-9753	Proxy password does not support the special characters '|', ':' or '@'

Date filed	Issue number	Description
2016-05-30	ADDON-9745	Add-on does not support proxy accounts that do not require passwords
2016-05-12	ADDON-9435	Wrong number of inputs listed on Account page.
2016-05-12	ADDON-9422	CloudWatch input can have data loss when empty results are returned twice in succession and then Splunk platform restarts before the input next collects data.
2016-05-11	ADDON-9408	Detailed Billing is not indexed using UTC timezone
2016-05-11	ADDON-9409	Checkpoints file will not be removed when deleting Config Rules
2016-05-07	ADDON-9332	fails to get latest cloudwatch data sometimes
2016-04-29	ADDON-9148	Updating directly from v2.0.0 to v4.0.0 makes existing accounts unavailable
2016-04-28	ADDON-9133	CloudWatch default configuration may not work in cases where there are millions of dimensions
2016-04-28	ADDON-9145	Error message shown on input creation screen has logic issues and is not as specific as we could be
2016-01-13	ADDON-7448	In the Description data input, the port range defaults to null in vpc_network_acls if no range is specified, which is confusing, because it actually has a range of "all".
2015-12-29	ADDON-7239	Using "/" in data input name causes exceptions. UI does not accept this character in the input names, but if you configure your input using conf files, you will find exceptions in logs.
2015-12-22	ADDON-7159	After removing all search peers, add-on still shows performance warnings. Workaround: Restart a Splunk platform instance after changing its role.
2015-12-16	ADDON-7035	Add-on ingests the header line of the CloudFront access log, but it should be skipped.
2015-11-26	ADDON-6701	EC2, RDS, ELB, and EC2 APIs do not consider pagination.
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.
2015-04-02	ADDON-3578	S3: uppercase bucket names cause an error
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input.

Date filed	Issue number	Description
		Workaround: Restart the Splunk platform after deleting or modifying an AWS account.
2014-09-25	ADDON-2113	The app.conf file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. Workaround: This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in app.conf.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.

Third-party software attributions

Version 4.1.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 4.0.0

Version 4.0.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.2.X and later
CIM	4.0 and later
Platforms	Platform independent
Vendor Products	Amazon Web Services CloudTrail, CloudWatch, CloudWatch Logs, Config, Config Rules, Inspector, Kinesis, S3, VPC Flow Log, and Billing services

Upgrade

If you are upgrading from a previous version of the Splunk Add-on for AWS, be aware of the following changes which may require some actions to preserve the functionality of your existing accounts and inputs:

- This release includes three new inputs that each require new IAM permissions. Be sure to adjust the IAM permissions of your existing accounts if you want to use them to collect these new data sources. See Configure AWS permissions for the Splunk Add-on for AWS for details.

- If you are upgrading directly from version 2.0.0 or earlier of this add-on to the 4.0.0 version, you need to open and resave the AWS accounts using the Splunk Add-on for AWS account UI.
- In this version, the CloudWatch input is rearchitected for better performance and improved stability. One result of this new architecture is that the input has a built in four minute delay after a polling period has ended for any given metric before the actual data collection occurs. This change ensures that there is no data loss due to latency on the AWS side.
- This version requires a single selection for the Region Category for each AWS account. If you added accounts before region category selection was required, or if you added accounts and selected more than one region category for a single account, the upgrade to version 4.0.0 will put these accounts into an error state until you edit them to select a single region category. On your data collection node, open the add-on and check your Configuration tab to see if any of your existing accounts are missing a region category. If they are, edit the account to add the region category. Any inputs using accounts that were determined to be in error stop collecting data until the account has a region category assigned. Once the account error is resolved, the affected inputs start collecting data again automatically starting from the point when data collection stopped.

New Features

Version 4.0.0 of the Splunk Add-on for Amazon Web Services has the following new features.

Resolved date	Issue number	Description
2016-04-29	ADDON-7042	CloudWatch input configuration UI now provides auto-filled correct default JSON for metrics and dimensions in each namespace.
2016-04-08	ADDON-7587	Support for AWS Signature V.4 managed keys for S3 related data collection.
2016-04-05	ADDON-7818	New input and CIM mapping for Amazon Inspector data.
2016-04-05	ADDON-7817	New input and CIM mapping for AWS Config rules data.
2016-04-05	ADDON-5391	New input for data from Kinesis streams, including high volume VPC flow log data.
2016-03-31	ADDON-6811	Support for using an EC2 IAM role instead of an AWS account when the add-on's collection node is on your own managed AWS instance.
2016-03-23	ADDON-7872	Support for the Seoul region.
2016-01-08	ADDON-7311	Support for setting an initial scan time in the Billing input if configuring using the conf files.

Fixed issues

Version 4.0.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
2016-05-04	ADDON-9169	Monthly Billing is not indexed using the UTC timezone
2016-04-19	ADDON-8801	Billing initial scan time should not use last modified time of S3 key
2016-04-15	ADDON-8721	Sourcetype="aws:cloudwatchlogs:vpcflow" handles src and dest incorrectly
2016-04-11	ADDON-8686	S3 input UI cannot display custom source types when user edits the input.
2016-04-03	ADDON-8547	S3 modular input loses data if new keys are generated during the key listing process
2016-04-02	ADDON-8546	S3 logging is unclear, should include indication of which input stanza is involved.
2016-03-31	ADDON-8548	CloudWatch collection failing with "Failed to get proxy information Empty"

Resolved date	Defect number	Description
2016-03-15	ADDON-8299	S3 input cannot progress if keys are deleted during the data collection.
2016-02-29	ADDON-8705	Add-on throws "is not JSON serializable" error when calling AWS API for ELB information
2016-02-25	ADDON-7969	CloudWatch has performance problems in large AWS accounts.
2016-02-24	ADDON-7957	Unnecessary tag expansion slows performance.
2016-02-24	ADDON-7926	Default value of max_file_size_csv_zip_in_bytes is too small to handle large detailed billing reports
2016-02-22	ADDON-7897	s3util.py list_cloudwatch_namespaces has performance issue
2016-02-19	ADDON-7877	Upon upgrade from version 2.0.X, S3 inputs experience two problems. Workaround: 1. Inputs with a S3 key prefix specified stop collecting data from AWS. Workaround: Stop splunkd and go to $SPLUNK_HOME/var/lib/modinputs/aws_s3/, find the checkpoint file for that data input (ls -lh to list and find the large files), open the file, and note the last_modified_time in the file. Remove the checkpoint file and update the data input in inputs.conf using the last_modified_time value that you observed in the checkpoint file for the initial_scan_time in the new input. Reboot splunkd. 2. The polling_interval does not persist automatically. Workaround: In Splunk Web, open the input configuration, go to Settings, set an interval value, then click Update. Or, in local/inputs.conf, set the polling_interval to a value that matches your needs, then save the file.
2016-02-14	ADDON-7777	Not all fields are parsed for CloudFront
2016-02-13	ADDON-7778	Cannot create new input when Splunk does not have a user named "admin"
2016-02-13	ADDON-7776	CloudFront logs should be urldecoded
2016-01-25	ADDON-7573	CloudWatch input requests too many data points in long time windows.
2016-01-18	ADDON-7701	CloudWatch fails to gather data when no metrics appear in a namespace for more than 12 hours.
2015-09-11	ADDON-5498	Unclear error: Unexpected error "<class 'socket.error'>" from python handler: " Connection refused" when user specifies all regions in CloudWatch for one namespace, saves the configuration, and reloads it.
2015-09-10	ADDON-5469	Missing or improper default value for un-required fields.

Known issues

Version 4.0.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Issue number	Description
2016-10-28	ADDON-11847	s3 input zombie processes Workaround: Update the symbolic link so that /bin/sh targets /bin/bash. $ debconf-set-selections <<< "dash dash/sh string false" $ dpkg-reconfigure -f noninteractive dash
2016-10-28	ADDON-11846, SPL-138046	Logging breaks on rotation when multiple inputs write to the same log. If > 6 inputs, some inputs cannot log

Date filed	Issue number	Description
2016-10-05	ADDON-11498	Trailing angle bracket and invalid JSON in aws:cloudwatchlogs
2016-09-22	ADDON-11415	The input name is case sensitive lead to failure on Windows platform
2016-09-19	ADDON-11326	Unexpected timestamp format blocks data ingestion
2016-09-12	ADDON-11266	Chrome failed to create account
2016-09-10	ADDON-11251	Data loss when creating multi inputs to ingesting data
2016-09-08	ADDON-11225	Fails to download Billing files due to "Operation timed out" error
2016-09-06	ADDON-11196	Strip blank space in input name
2016-08-29	ADDON-11056	Region shows "ap-northeast-2" but not Seoul
2016-08-24	ADDON-11009	Vanguard: Not getting data from 1 of 3 S3 inputs. This is considered critical for the customer as they have PS on site
2016-08-22	ADDON-10978	S3 data loss after disable/enable
2016-08-22	ADDON-10980	S3 line breaker error
2016-08-18	ADDON-10957	Log level set to ERROR but still found INFO logs
2016-07-20	ADDON-10643	Rest handler splunk_ta_aws_settings_account_region is missing
2016-07-17	ADDON-10574	Log level for can't find checkpoint should not be ERROR
2016-07-06	ADDON-10450	REST handler s3buckets still returns status 200 while connection failed
2016-06-20	ADDON-10286	CloudWatch modular input generates duplicate events when the Splunk platform is restarted Workaround: dedup based on the _time field
2016-06-13	ADDON-10186	AWS Config fails to fetch S3 object in AWS GovCloud (US) region
2016-05-31	ADDON-9778	HEC max limit needs to take padding into account to avoid 413 "Content-Length of <value> too large" errors
2016-05-30	ADDON-9745	Add-on does not support proxy accounts that do not require passwords
2016-05-30	ADDON-9753	Proxy password does not support the special characters '|', ':' or '@'
2016-05-27	ADDON-9732	failed to get proxy credentials when password includes # sign
2016-05-18	ADDON-9533	Dimensions default to empty square brackets for Autoscaling and EBS namespaces
2016-05-16	ADDON-9451	Monthly billing date is displayed as next month for some timezones
2016-05-12	ADDON-9435	Wrong number of inputs listed on Account page.
2016-05-12	ADDON-9431	further save the cost with more efficient API call
2016-05-12	ADDON-9422	CloudWatch input can have data loss when empty results are returned twice in succession and then Splunk platform restarts before the input next collects data.
2016-05-12	ADDON-9434, ADDON-10137	Rest Handler Of List Data Inputs Truncates Result. Workaround: 1) Navigate to /opt/splunk/etc/apps/Splunk_TA_aws/bin/splunktalib/rest.py 2) Change line 44 of this script from: resp, content = http.request(splunkd_uri, method=method, to resp, content = http.request(splunkd_uri + "?count=-1",

Date filed	Issue number	Description
		method=method, 3) Save and exit
2016-05-11	ADDON-9408	Detailed Billing is not indexed using UTC timezone
2016-05-11	ADDON-9409	Checkpoints file will not be removed when deleting Config Rules
2016-05-07	ADDON-9332	fails to get latest cloudwatch data sometimes
2016-05-06	ADDON-9328	CloudWatch data input encounters API rate limit for large metrics Workaround: Increase your granularity and polling interval in order to make fewer API calls, or contact AWS to increase your allowed number of API calls per month.
2016-04-29	ADDON-9148	Updating directly from v2.0.0 to v4.0.0 makes existing accounts unavailable
2016-04-28	ADDON-9145	Error message shown on input creation screen has logic issues and is not as specific as we could be
2016-04-28	ADDON-9133	CloudWatch default configuration may not work in cases where there are millions of dimensions
2016-04-27	ADDON-9117	Using EC2 IAM role for data collection does not work in China or GovCloud regions.
2016-04-20	ADDON-8905	Add-on throws "connection refused" error when Splunk platform restarts
2016-04-19	ADDON-8758	Mixing log types or gzip with plain text in the same stream causes knowledge extraction to fail for CloudWatch Logs data collected through Kinesis
2016-03-01	ADDON-8113	Excessive S3 API calls
2016-01-13	ADDON-7448	In the Description data input, the port range defaults to null in vpc_network_acls if no range is specified, which is confusing, because it actually has a range of "all".
2015-12-29	ADDON-7239	Using "/" in data input name causes exceptions. UI does not accept this character in the input names, but if you configure your input using conf files, you will find exceptions in logs.
2015-12-22	ADDON-7159	After removing all search peers, add-on still shows performance warnings. Workaround: Restart a Splunk platform instance after changing its role.
2015-12-16	ADDON-7035	Add-on ingests the header line of the CloudFront access log, but it should be skipped.
2015-11-26	ADDON-6701	EC2, RDS, ELB, and EC2 APIs do not consider pagination.
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.

Date filed	Issue number	Description
2015-07-06	ADDON-6177	When tmp file system runs out of space, aws_billing.py fails with IOError: No space left on device.
2015-04-02	ADDON-3578	S3: uppercase bucket names cause an error
2015-03-25	ADDON-3460	On OSs (like Debian and Ubuntu) that use dash for shell scripts, aws_cloudwatch.py spawns zombie processes. Workaround: Kill the processes and restart. Use bash to prevent re-occurrence.
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart the Splunk platform after deleting or modifying an AWS account.
2014-09-25	ADDON-2113	The app.conf file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. Workaround: This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in app.conf.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.

Third-party software attributions

Version 4.0.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- boto3
- botocore
- dateutils
- docutils
- jmespath
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2
- urllib3

Version 3.0.0

Version 3.0.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.2.X and later
CIM	4.0 and later

Platforms	Platform independent
Vendor Products	AWS CloudTrail, CloudWatch, CloudWatch Logs, Config, Billing, S3

Upgrade guide

This release includes some changes to the S3 input configuration that break backwards compatibility. If you are upgrading from a previous version and had previously used any of the following parameters, review the new behavior noted here and make any necessary changes in your existing S3 inputs:

- `interval` now refers to how long splunkd should wait before checking the health of the modular input and restarting it if it has crashed. The new argument `polling_interval`, still shown as Interval in the UI, handles the data collection interval. If you had a custom value configured, the 3.0.0 version of the add-on copies your custom setting to the `polling_interval` value so that your data collection behavior does not change. However, you may wish to tune the `interval` value to enable splunkd to check for input crashes more frequently.
- `is_secure` is deprecated and removed, but the parameter is retained in `default/inputs.conf` to avoid spec file violations. All traffic is over https. If you have this parameter in your `local/inputs.conf`, it will have no effect.
- `max_items` is deprecated and removed, but the parameter is retained in `default/inputs.conf` to avoid spec file violations. It is set to 100000 items. If you have this parameter in your `local/inputs.conf`, it will have no effect.
- `queueSize` is deprecated and removed. If you have this parameter in your `local/inputs.conf`, remove it to avoid potential data loss.
- `persistentQueueSize` is deprecated and removed. If you have this parameter in your `local/inputs.conf`, remove it to avoid potential data loss.
- `recursion_depth` is deprecated and removed, but the parameter is retained in `default/inputs.conf` to avoid spec file violations. The input recursively scans all subdirectories. If you have this parameter in your `local/inputs.conf`, it will have no effect.
- `ct_excluded_events_index` is deprecated and removed, but the parameter is retained in `default/inputs.conf` to avoid spec file violations. Excluded events will be discarded. If you have this parameter in your `local/inputs.conf`, it will have no effect.

New features

Version 3.0.0 of the Splunk Add-on for Amazon Web Services has the following new features.

Resolved date	Issue number	Description
2015-11-16	ADDON-6690	Add-on configuration screen serves a warning message when you access it on a Splunk search head to remind you to configure it on heavy forwarders as a best practice.
2015-12-23	ADDON-6870	Support for GovCloud and China regions in the configuration UI.
2015-12-22	ADDON-6862	Support in the configuration UI and backend for new source types: `aws:s3:accesslogs`, `aws:cloudfront:accesslogs`, `aws:elb:accesslogs`
2015-12-17	ADDON-6190	CloudWatch input refreshes the resource ID list every few hours so as to include additional resources to a wildcarded statement.
2015-12-17	ADDON-6187	CloudWatch collects S3 key count and total size of all keys in buckets.
2015-12-15	ADDON-6864	S3 modular input backend automatically detects the region, thus supporting bucket names with dots in them without user's needing to specify a region-specific endpoint.
2015-12-15	ADDON-6854	Deprecation of character_set parameter for S3 input. Input supports auto-detection among UTF-8 with/without BOM, UTF-16LE/BE with BOM, UTF-32BE/LE with BOM. Other character sets are not supported.

Resolved date	Issue number	Description
2015-12-15	ADDON-6189	Support for collecting ELB access logs using the `aws:elb:accesslogs`.
2015-12-14	ADDON-6869	Support for S3 buckets in the Frankfurt region with V4 signature only.
2016-12-14	ADDON-6866	Improved auditing information for log enrichment.
2015-12-14	ADDON-6859	S3 input blacklist has improved performance.
2015-12-14	ADDON-6857	S3 input whitelist has improved performance.
2015-12-14	ADDON-6860	Improved handling of process failures without duplication or loss of data.
2015-12-14	ADDON-6861	Support for checkpoint deletion behavior for the S3 input to avoid running into collection limits.
2015-12-14	ADDON-6865	Support for initial scan time in the S3 input, as well as in the new `aws:s3:accesslogs`, `aws:cloudfront:accesslogs`, and `aws:elb:accesslogs` source types.
2015-12-14	ADDON-6863	Improved collection behavior in the S3 input: if the key is updated without content changes, the add-on indexes the key again. If the key is changed during data collection, the add-on starts over with the data collection.
2015-12-14	ADDON-6868	The S3 input supports standard server-side KMS encrypted objects.
2015-12-14	ADDON-6855	The S3 input supports bin files.
2015-12-14	ADDON-6852	Improved performance for S3 input. Approximately 300% performance enhancement against 2.0.1 release. Over 8000% performance improvement for small files. See Performance reference for the S3 input in the Splunk Add-on for AWS for details.
2015-12-14	ADDON-6434	UI support for configuring alternate source types within the S3 input.
2015-12-14	ADDON-6196	Support for collecting CloudFront access logs with the `aws:cloudfront:accesslogs` source type.
2015-12-14	ADDON-6526	S3 input recognizes and skips S3 buckets with contents that have been moved to Glacier.
2015-12-14	ADDON-6188	New source type for S3 access logs: `aws:s3:accesslogs`.
2015-12-03	ADDON-6433	Improvements to the Description input's API and interval configuration UI.
2015-12-01	ADDON-6519	Improved timeout behavior in the configuration UI.
2015-11-26	ADDON-6194	Improvements to field aliasing for AWS regions.
2015-11-26	ADDON-6207	Gather metadata through the Description input for EBS, VPC, Security Group, Subnet, Network ACL, Key Pairs, ELB, CloudFront, RDS.

Fixed issues

Version 3.0.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
2016-01-14	ADDON-7291	S3 data input only shows 30 entries at maximum.
2016-01-03	ADDON-7258	Configuration screen needs to show better error message when user may be trying to use an invalid AWS account.
2015-12-31	ADDON-7253	Default initial_scan_datetime should be ISO8601 instead of the current default of current time minus 7 days.
2015-12-16	ADDON-7031	UI errors when using the base URL via reverse proxy.

Resolved date	Defect number	Description
2015-12-15	ADDON-6754	Typo in aws_cloudtrail.py script throws critical error in aws_cloudtrail.log with "NameError: global name 'taaw' is not defined".
2015-12-15	ADDON-7008	Add-on is not indexing ELB data through Description input.
2015-12-14	ADDON-6308	S3 input should validate key name does not include invalid characters such as leading or trailing whitespace.
2015-11-26	ADDON-6698	AWS Billing account ID should be payer's account ID instead of linked account ID.
2015-12-22	ADDON-5491	The add-on configuration UI displays all regions instead of those within the selected account's permission scope.
2015-12-20	ADDON-6958 / ADDON-5474	No detailed error shown while getting S3 buckets via REST endpoint with wrong proxy or account settings.
2015-01-22	ADDON-3050/ SPL-96729/ SPL-64904	S3 input is breaking lines incorrectly and inconsistently indexing only partial events due to use of `persistentQueueSize`.
2014-08-14	ADDON-1827	Checkpoints are not cleared after data inputs are removed or the add-on is uninstalled, thus if you create a new input with the same name as the deleted one, the add-on uses the checkpoint from the old input.

Known issues

Version 3.0.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Defect number	Description
2016-05-04	ADDON-9169	Monthly Billing is not indexed by using UTC timezone
2016-04-28	ADDON-9145	Error message shown on input creation screen has logic issues and is not as specific as we could be
2016-04-19	ADDON-8801	Billing initial scan time should not use last modified time of S3 key
2016-04-15	ADDON-8721	Sourcetype="aws:cloudwatchlogs:vpcflow" handles src and dest incorrectly
2016-04-11	ADDON-8686	S3 input UI cannot display custom source types when user edits the input.
2016-04-03	ADDON-8547	S3 modular input loses data if new keys are generated during the key listing process
2016-04-02	ADDON-8546	S3 logging is unclear, should include indication of which input stanza is involved.
2016-03-31	ADDON-8548	Cloudwatch Collection failing with Failed to get proxy information Empty
2016-03-15	ADDON-8299	S3 input cannot progress if keys are deleted during the data collection.
2016-02-29	ADDON-8705	Add-on throws "is not JSON serializable" error when calling AWS API for ELB information
2016-02-25	ADDON-7969	CloudWatch has performance problems in large AWS accounts.
2016-02-24	ADDON-7957	Unnecessary tag expansion slows performance.
2016-02-24	ADDON-7926	Default value of max_file_size_csv_zip_in_bytes is too small to handle large detailed billing reports
2016-02-22	ADDON-7897	s3util.py list_cloudwatch_namespaces has performance issue
2016-02-19	ADDON-7877	Upon upgrade from version 2.0.X, S3 inputs experience two problems. Workaround: 1. Inputs with a S3 key prefix specified stop collecting data from AWS.

Date filed	Defect number	Description
		Workaround: Stop splunkd and go to $SPLUNK_HOME/var/lib/modinputs/aws_s3/, find the checkpoint file for that data input (ls -lh to list and find the large files), open the file, and note the last_modified_time in the file. Remove the checkpoint file and update the data input in inputs.conf using the last_modified_time value that you observed in the checkpoint file for the initial_scan_time in the new input. Reboot splunkd. 2. The polling_interval does not persist automatically. Workaround: In Splunk Web, open the input configuration, go to Settings, set an interval value, then click Update. Or, in local/inputs.conf, set the polling_interval to a value that matches your needs, then save the file.
2016-02-14	ADDON-7777	Not all fields are parsed for CloudFront
2016-02-13	ADDON-7778	Cannot create new input when Splunk does not have a user named "admin"
2016-02-13	ADDON-7776	CloudFront logs should be urldecoded
2016-02-11	ADDON-7764	FIPS mode is not supported by this add-on.
2016-01-25	ADDON-7573	CloudWatch input requests too many data points in long time windows.
2016-01-18	ADDON-7701	CloudWatch fails to gather data when no metrics appear in a namespace for more than 12 hours.
2016-01-13	ADDON-7448	In the Description data input, the port range defaults to null in vpc_network_acls if no range is specified, which is confusing, because it actually has a range of "all".
2015-12-29	ADDON-7239	Using "/" in data input name causes exceptions. UI does not accept this character in the input names, but if you configure your input using conf files, you will find exceptions in logs.
2015-12-22	ADDON-7160	Add-on throws a timeout error in the UI when user attempts to create a new S3 input, but successfully creates the input in the backend, causing errors if the user tries to create the same input again.
2015-12-22	ADDON-7159	After removing all search peers, add-on still shows performance warnings. Workaround: Restart a Splunk platform instance after changing its role.
2015-12-21	ADDON-7077	Infrequent Access storage type not supported
2015-12-16	ADDON-7035	Add-on ingests the header line of the CloudFront access log, but it should be skipped.
2015-11-26	ADDON-6701	EC2, RDS, ELB, and EC2 APIs do not consider pagination.
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change
2015-09-11	ADDON-5498	Unclear error: Unexpected error "<class 'socket.error'>" from python handler: " Connection refused" when user specifies all regions in CloudWatch for one namespace, saves the configuration, and reloads it.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5469	Missing or improper default value for un-required fields.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file

Date filed	Defect number	Description
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.
2015-08-31	ADDON-5212	Chrome highlights "misspelling" of configuration text in the GUI.
2015-07-06	ADDON-6177	When tmp file system runs out of space, aws_billing.py fails with IOError: No space left on device.
2015-04-02	ADDON-3578	S3: uppercase bucket names cause an error
2015-03-25	ADDON-3460	On OSs (like Debian and Ubuntu) that use dash for shell scripts, aws_cloudwatch.py spawns zombie processes. Workaround: Kill the processes and restart. Use bash to prevent re-occurrence.
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart the Splunk platform after deleting or modifying an AWS account.
2014-09-25	ADDON-2113	The app.conf file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. Workaround: This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in app.conf.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.

Third-party software attributions

Version 3.0.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- jqBootstrapValidation
- jquery-cookie
- Httplib2
- remote-pdb
- SortedContainers
- select2

Version 2.0.1

Version 2.0.1 of the Splunk Add-on for Amazon Web Services has the same compatibility specifications as version 3.0.0.

Fixed issues

Version 2.0.1 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
2015-11-04	ADDON-5813	S3 input cannot handle bucket names with "." in them. See "Add an S3 input for the Splunk Add-on for AWS" for details of the solution.
2015-10-28	ADDON-6125	Add-on makes too many unnecessary get_log_event API calls, causing inefficiencies in environments with many spot instances.
2015-10-26	ADDON-5785	Corrupt VPC Flow checkpointer file in race condition.

Resolved date	Defect number	Description
2015-10-20	ADDON-5612	When CloudTrail userName is null, add-on coalesces the userName to "root" instead of "unknown".
2015-10-15	ADDON-6004	Add-on GUI does not allow user to select an index that is only defined on the indexers.
2015-10-11	ADDON-6003	Incorrect regions shown in region drop-down list.
2015-10-11	ADDON-6001	Config fails to fetch events from an S3 bucket in a different region.
2015-10-09	ADDON-5833	AWS CloudWatch log formatting exception.
2015-10-09	ADDON-4505	Cloudwatchlog deadlocks due to throttling exceptions when an input task includes a large number of log groups.
2015-10-09	ADDON-5782	A corrupted checkpointer file for VPC Flow blocks other logstreams.

Known issues

Version 2.0.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Defect number	Description
2015-12-15	ADDON-7930	Data collection for Cloudwatch S3 metrics does not support wildcard in BucketName or array length > 1.
2015-11-09	ADDON-6371	In some cases, Splunk Cloud does not save the AWS account credentials after they are correctly entered. Workaround: File a support request to redeploy the add-on and restart the instance.
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change.
2015-09-11	ADDON-5498	Unclear error message: Failed to load options for Metric namespace. Detailed Error: Unexpected error "<class 'socket.error'>" from python handler: "[Errno 111] Connection refused" when user specifies all regions in CloudWatch for one namespace, saves the configuration, and reloads it.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-10	ADDON-5474	No detailed error shown while getting S3 buckets via REST endpoint with wrong proxy or account settings.
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5469	Missing or improper default value for un-required fields.
2015-09-10	ADDON-5491	The add-on configuration UI displays all regions instead of those within the selected account's permission scope.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file.
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.
2015-08-31	ADDON-5212	Chrome highlights "misspelling" of configuration text in the GUI.
2015-07-09	ADDON-3460 / CO-4749 /	On OSs (like Debian and Ubuntu) that use dash for shell scripts, `aws_cloudwatch.py` spawns zombie processes. Workaround: Kill the processes and restart. Use bash to prevent re-occurrence.

Date filed	Defect number	Description
	SPL-55904	
2015-07-06	ADDON-6177	aws_billing.py fails with IOError: [Errno 28] No space left on device.
2015-04-03	ADDON-3578	Uppercase bucket name causes errors.
2015-01-22	ADDON-3050/ SPL-96729/ SPL-64904	S3 input is breaking lines incorrectly and inconsistently indexing only partial events. Workaround: Disable the persistent queue for the S3 input by changing `persistentQueueSize = 24MB` to `persistentQueueSize = 0` in `local/inputs.conf`.
2015-01-25	ADDON-3070	The add-on does not index the Configuration.State.Code change from SQS that is reported to users on the AWS Config UI. Splunk Enterprise only indexes configuration snapshots from S3 as new events, and only after a "ConfigurationHistoryDeliveryCompleted" notification is recieved by SQS.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart Splunk Enterprise after deleting or modifying an AWS account.
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2116/ SPL-91709	On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page.
2014-09-25	ADDON-2113	The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in `app.conf`.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.
2014-09-09	ADDON-1983 / ADDON-1938 / SPL-81771	Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination. Checkpoint and retry time do not log correctly when Splunkd stops.
2014-08-26	ADDON-1919	If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account.
2014-08/17	ADDON-1854	After initial configuration, adjusting Max trackable items might cause data loss.
2014-08-14	ADDON-1827	Checkpoints are not cleared after data inputs are removed or the add-on is uninstalled, thus if you create a new input with the same name as the deleted one, the add-on uses the checkpoint from the old input. Workaround: create unique input names to avoid picking up old checkpoint files.

Third-party software attributions

Version 2.0.1 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- jqBootstrapValidation
- Httplib2
- SortedContainers
- select2

Version 2.0.0

Version 2.0.0 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk platform versions	6.3, 6.2
CIM	4.0 and above
Platforms	Platform independent
Vendor Products	AWS CloudTrail, CloudWatch, CloudWatch Logs, Config, Billing, S3

New features

Version 2.0.0 of the Splunk Add-on for Amazon Web Services has the following new features.

Resolved date	Defect number	Description
2015-09-08	ADDON-1671	New configuration UI.
2015-09-08	ADDON-2126 / ADDON-5466	Ability to manually enter S3 bucket names, SQS queue names, and metric namespaces in Splunk Web fields, in case connection to AWS is poor or user account lacks permissions to list buckets.
2015-07-14	ADDON-4543	Added unified field for AWS account ID across all data inputs: `aws_account_id`.
2015-07-06	ADDON-3189	Currency field added to AWS billing report data, allowing users to more accurately judge financial impact.
2015-07-03	ADDON-4260 / ADDON-1665	Support for data ingestion from AWS CloudWatch Logs service, including VPC Flow Logs.
2015-07-03	ADDON-4259	CIM mapping for VPC Flow Logs data.
2015-06-30	ADDON-4158	Support for Config snapshot collection.
2015-06-29	ADDON-2364	Support for collecting archives of CloudTrail data via S3 buckets by configuring the sourcetype `aws:cloudtrail` in an S3 input.
2015-06-29	ADDON-4413	Support for multiple regions in a single CloudWatch input.
2015-06-29	ADDON-3235	Support for disabling SSL proxies using the `is_secure` parameter in `local/aws_global_settings.conf` to alter the behavior of connections to AWS.
2015-06-29	ADDON-4180	Support for inventory metadata collection from AWS.

Fixed issues

Version 2.0.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
2015-09-14	ADDON-5158	CloudTrail data missing some CIM tagging.
2015-08-31	ADDON-5200	CloudWatch input calls AWS API inefficiently, using separate API call for each instance-metric combination.
2015-08-31	ADDON-2006	Unfriendly error message when user specifies invalid account.
2015-08-31	ADDON-1932	Unfriendly error message when configuring proxy incorrectly.
2015-08-31	ADDON-1926	Splunk Web allows you to update and delete an AWS account for the add-on simultaneously.
2015-09-09	ADDON-4822 / CO-4912	Some instances of Splunk Cloud show blank screens for all data input pages. Workaround: Set up a heavy forwarder on-prem to handle data inputs and forward the data to Splunk Cloud.

Known issues

Version 2.0.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date filed	Defect number	Description
2015-10-14	ADDON-6056	S3 logging errors on Windows.
2015-10-13	ADDON-6043	SQS message mistakenly deleted when the add-on throws an error retrieving data from an S3 bucket.
2015-10-09	ADDON-6004	Add-on GUI does not allow user to select an index that is only defined on the indexers.
2015-10-09	ADDON-6003	Incorrect regions shown in region drop-down list.
2015-10-09	ADDON-6001	Confg fails to fetch events from an S3 bucket in a different region.
2015-10-03	ADDON-5833	AWS CloudWatch log formatting exception.
2015-09-28	ADDON-5813	S3 input cannot handle bucket names with "." in them.
2015-09-24	ADDON-5785	Corrupt VPC Flow checkpointer file in race condition.
2015-09-24	ADDON-5782	A corrupted checkpointer file for VPC Flow blocks other logstreams.
2015-09-17	ADDON-5612	When CloudTrail userName is null, add-on coalesces the userName to "root" instead of "unknown".
2015-09-11	ADDON-5500	Preconfigured reports for billing data cannot handle reports that have a mix of different currencies. The report will use the first currency found and apply that to all costs.
2015-09-11	ADDON-5499	CloudWatch: Previous selected Metric namespace always exists in the list regardless of the region change.
2015-09-11	ADDON-5498	Unclear error message: Failed to load options for Metric namespace. Detailed Error: Unexpected error "<class 'socket.error'>" from python handler: "[Errno 111] Connection refused" when user specifies all regions in CloudWatch for one namespace, saves the configuration, and reloads it.
2015-09-10	ADDON-5481	The add-on configuration UI does not handle insufficient Splunk user permissions gracefully.
2015-09-10	ADDON-5491	The add-on configuration UI displays all regions instead of those within the selected account's permission scope.
2015-09-10	ADDON-5474	No detailed error shown while getting S3 buckets via REST endpoint with wrong proxy or account settings.
2015-09-10	ADDON-5471	Deleting a CloudWatch data input takes too long.
2015-09-10	ADDON-5469	Missing or improper default value for un-required fields.
2015-09-07	ADDON-5355	Different error message for same error when creating duplicated data inputs.
2015-09-06	ADDON-5354	Using keyboard to delete selections from configuration dropdown multi-select field causes drop-down list to appear in corner of screen.
2015-09-01	ADDON-5309	UI default value is not read from default input config file.
2015-09-01	ADDON-5295	Description inconsistent in the GUI for CloudTrail service and CloudTrail from S3 service blacklist behavior.
2015-08-31	ADDON-5212	Chrome highlights "misspelling" of configuration text in the GUI.
2015-07-10	ADDON-4505	Cloudwatchlog deadlocks due to throttling exceptions when an input task includes a large number of log groups.
2015-07-09	ADDON-3460 / CO-4749 / SPL-55904	On OSs (like Debian and Ubuntu) that use dash for shell scripts, `aws_cloudwatch.py` spawns zombie processes. Workaround: Kill the processes and restart. Use bash to prevent re-occurrence.

Date filed	Defect number	Description
2015-07-06	ADDON-6177	aws_billing.py fails with IOError: [Errno 28] No space left on device.
2015-04-03	ADDON-3578	Uppercase bucket name causes errors.
2015-01-22	ADDON-3050/ SPL-96729/ SPL-64904	S3 input is breaking lines incorrectly and inconsistently indexing only partial events. Workaround: Disable the persistent queue for the S3 input by changing `persistentQueueSize = 24MB` to `persistentQueueSize = 0` in `local/inputs.conf`.
2015-01-25	ADDON-3070	The add-on does not index the Configuration.State.Code change from SQS that is reported to users on the AWS Config UI. Splunk Enterprise only indexes configuration snapshots from S3 as new events, and only after a "ConfigurationHistoryDeliveryCompleted" notification is recieved by SQS.
2014-09-26	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart Splunk Enterprise after deleting or modifying an AWS account.
2014-09-28	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
2014-09-26	ADDON-2116/ SPL-91709	On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page.
2014-09-25	ADDON-2113	The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in `app.conf`.
2014-09-16	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.
2014-09-09	ADDON-1983 / ADDON-1938 / SPL-81771	Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination. Checkpoint and retry time do not log correctly when Splunkd stops.
2014-08-26	ADDON-1919	If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account.
2014-08/17	ADDON-1854	After initial configuration, adjusting Max trackable items might cause data loss.
2014-08-14	ADDON-1827	Checkpoints are not cleared after data inputs are removed or the add-on is uninstalled, thus if you create a new input with the same name as the deleted one, the add-on uses the checkpoint from the old input. Workaround: create unique input names to avoid picking up old checkpoint files.

Third-party software attributions

Version 2.0.0 of the Splunk Add-on for Amazon Web Services incorporates the following third-party libraries.

- Bootstrap
- boto - AWS for Python
- jqBootstrapValidation
- Httplib2
- SortedContainers
- select2

Version 1.1.1

Version 1.1.1 of the Splunk Add-on for Amazon Web Services is compatible with the following software, CIM versions, and platforms.

Splunk Enterprise versions	6.2, 6.1

CIM	4.2, 4.1, 4.0
Platforms	Platform independent
Vendor Products	AWS Billing, CloudTrail, CloudWatch, Config, S3

Fixed issues

Version 1.1.1 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
04/24/15	ADDON-3512	Timeout error on new account definition. Users can now set splunkdConnectionTimeout = 3000 in $SPLUNK_HOME/etc/system/local/web.conf to avoid setup timeout problems.
04/21/15	ADDON-3612	Add-on cannot parse multi-account message format from SQS and CloudTrail.
04/21/15	ADDON-3577	Input configuration timeout on retrieving bucket/key list from S3.
03/01/15	ADDON-3119	Add-on fails to collect payloads from GovCloud region.

Known issues

Version 1.1.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date	Defect number	Description
08/27/15	ADDON-5158	CloudTrail data missing some CIM tagging.
08/06/15	ADDON-4822 / CO-4581	Some instances of Splunk Cloud show blank screens for all data input pages. Workaround: Set up a heavy forwarder on-prem to handle data inputs and forward the data to Splunk Cloud.
04/10/15	ADDON-3652	Billing reports are not performant.
04/03/15	ADDON-3578	Uppercase bucket name causes errors.
01/22/15	ADDON-3050/ SPL-96729/ SPL-64904	S3 input is breaking lines incorrectly and inconsistently indexing only partial events. Workaround: Disable the persistent queue for the S3 input by changing `persistentQueueSize = 24MB` to `persistentQueueSize = 0` in `local/inputs.conf`.
01/25/15	ADDON-3070	The add-on does not index the Configuration.State.Code change from SQS that is reported to users on the AWS Config UI. Splunk Enterprise only indexes configuration snapshots from S3 as new events, and only after a "ConfigurationHistoryDeliveryCompleted" notification is recieved by SQS.
01/06/15	ADDON-2910	Splunk Cloud customers cannot access props.conf to configure line breaking on S3 events.
10/10/14	ADDON-2154	Billing input data has a non-ISO-8601 timestamp appended to the source field of each event. Workaround: Add a new field named "source2" in the suggested format: `..... | rex field=source "(?<source_file>s3://[^:])" | rex field=source "(?<source_date>(csv|zip):.$)" | eval source2=strftime(strptime(substr(source_date, 9),"%d %b %Y %H:%M:%S"),"%Y-%m-%dT%H:%M:%S%z") | eval source2=source_file+":"+source2.`
09/26/14	ADDON-2118	Data inputs continue to work after user deletes the account used for that input. Workaround: Restart Splunk Enterprise after deleting or modifying an AWS account.
09/28/14	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
09/26/14	ADDON-2116/ SPL-86716	On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page.

09/26/14	ADDON-2115	If user does not provide a friendly name when configuring an AWS account in the setup screen, account is not configured but no error message appears
09/25/14	ADDON-2113	The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in `app.conf`.
09/25/14	ADDON-2110	In Splunk 6.2, when network is unstable, some input configuration fields fail to display in Splunk Web and no error message is shown.
09/16/14	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.
09/11/14	ADDON-2006	Unfriendly error message when user specifies invalid account.
09/09/14	ADDON-1983	If Splunk Enterprise restarts while indexing S3 data, data duplication might occur. Workaround: Use AWS command line tools.
08/28/14	ADDON-1938	Checkpoint and retry time do not log correctly when Splunkd stops.
08/28/14	ADDON-1932	Unfriendly error message when configuring proxy incorrectly.
08/26/14	ADDON-1926	Splunk Web allows you to update and delete an AWS account for the add-on simultaneously.
08/26/14	ADDON-1919	If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account.
08/24/14	ADDON-1895	If user tries to update a billing report manually using Microsoft Excel, the add-on cannot process the modified file and throws "failed to parse key" error.
08/21/14	ADDON-1885	Splunk Enterprise does not validate Amazon Web Services credentials during add-on setup.
08/17/14	ADDON-1854	After initial configuration, adjusting Max trackable items might cause data loss.
08/14/14	ADDON-1827	Checkpoints are not cleared after data inputs are removed or the add-on is uninstalled, thus if you create a new input with the same name as the deleted one, the add-on uses the checkpoint from the old input. Workaround: create unique input names to avoid picking up old checkpoint files.
03/12/14	SPL-81771	Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination.

Third-party software attributions

Version 1.1.1 of the Splunk Add-on for Amazon Web Services incorporates boto - AWS for Python.

Version 1.1.0

Version 1.1.0 had the same compatibility specifications as Version 1.1.1.

New features

Version 1.1.0 of the Splunk Add-on for Amazon Web Services has the following new features.

Date	Issue number	Description
02/12/15	ADDON-3148	Support for the SNS Subscription attributes for Raw Message Delivery for AWS Config and CloudTrail.
02/09/15	ADDON-1644	Pre-built panels for CloudWatch, CloudTrail, and Billing data.
12/18/14	ADDON-2678	Allow users to configure the log level.
11/12/14	ADDON-2202	New modular input for AWS Config data.

Fixed issues

Version 1.1.0 of the Splunk Add-on for Amazon Web Services fixes the following issues.

Resolved date	Defect number	Description
02/11/15	ADDON-2533	Internal logs are source typed as "this-too-small".
02/10/15	ADDON-2679	Process for fetching logs runs in a loop.
02/09/15	ADDON-3154	Support AssumedRole user name for CloudTrail.

Known issues

Version 1.1.0 of the Splunk Add-on for Amazon Web Services has the following known issues.

Date	Defect number	Description
01/22/15	ADDON-3050	S3 input is breaking lines incorrectly.
01/25/15	ADDON-3070	The add-on does not index the Configuration.State.Code change from SQS that is reported to users on the AWS Config UI. Splunk Enterprise only indexes configuration snapshots from S3 as new events, and only after a "ConfigurationHistoryDeliveryCompleted" notification is recieved by SQS.
01/06/15	ADDON-2910	Splunk Cloud customers cannot access props.conf to configure line breaking on S3 events.
09/28/14	ADDON-2135	The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account.
09/26/14	ADDON-2116	On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page.
09/26/14	ADDON-2115	If user does not provide a friendly name when configuring an AWS account in the setup screen, account is not configured but no error message appears
09/25/14	ADDON-2113	The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in `app.conf`.
09/25/14	ADDON-2110	In Splunk 6.2, when network is unstable, some input configuration fields fail to display in Splunk Web and no error message is shown.
09/16/14	ADDON-2029	In saved search "Monthly Cost till *" _time is displayed per day rather than per month.
09/11/14	ADDON-2006	Unfriendly error message when user specifies invalid account.
09/09/14	ADDON-1983	If Splunk Enterprise restarts while indexing S3 data, data duplication might occur. Workaround: Use AWS command line tools.
08/28/14	ADDON-1938	Checkpoint and retry time do not log correctly when Splunkd stops.
08/28/14	ADDON-1932	Unfriendly error message when configuring proxy incorrectly.
08/26/14	ADDON-1926	Splunk Web allows you to update and delete an AWS account for the add-on simultaneously.
08/26/14	ADDON-1919	If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account.
08/24/14	ADDON-1895	If user tries to update a billing report manually using Microsoft Excel, the add-on cannot process the modified file and throws "failed to parse key" error.
08/21/14	ADDON-1885	Splunk Enterprise does not validate Amazon Web Services credentials during add-on setup.

08/17/14	ADDON-1854	After initial configuration, adjusting Max trackable items might cause data loss.
08/14/14	ADDON-1827	Checkpoints are not cleared after data inputs are removed or the add-on is uninstalled, thus if you create a new input with the same name as the deleted one, the add-on uses the checkpoint from the old input. Workaround: create unique input names to avoid picking up old checkpoint files.
03/12/14	SPL-81771	Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination.

Third-party software attributions

Version 1.1.0 of the Splunk Add-on for Amazon Web Services incorporates boto - AWS for Python.

Version 1.0.1

Version 1.0.1 of the Splunk Add-on for Amazon Web Services was compatible with the following software, CIM versions, and platforms.

Splunk Enterprise versions	6.2, 6.1
CIM	4.1, 4.0, 3.0
Platforms	Platform independent
Vendor Products	AWS Billing, CloudTrail, CloudWatch, S3

Fixed issues

Version 1.0.1 of the Splunk Add-on for Amazon Web Services fixed the following issues.

Resolved date	Defect number	Description
12/16/14	ADDON-2530	New version of boto library required to support eu-central-1 region.
12/11/14	ADDON-2359	Unexpected SQS messages can block inputs.

Known issues

Version 1.0.1 of the Splunk Add-on for Amazon Web Services has the following known issues.

- Internal log files are incorrectly sourcetyped as N-too-small. (ADDON-2533)
- Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination. (SPL-81771)
- After initial configuration, adjusting Max trackable items might cause data loss. (ADDON-1854)
- Splunk Enterprise does not validate Amazon Web Services credentials during add-on setup. (ADDON-1885)
- If user tries to update a billing report manually using Microsoft Excel, the add-on cannot process the modified file and throws "failed to parse key" error. (ADDON-1895)
- If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account. (ADDON-1919)
- Splunk Web allows you to update and delete an AWS account for the add-on simultaneously. (ADDON-1926)
- Setup and configuration pages in Splunk Web give unfriendly error messages when given invalid inputs (ADDON-1932, ADDON-2006)
- If Splunk Enterprise restarts while indexing S3 data, data duplication might occur. Workaround: Use AWS command line tools. (ADDON-1983 and ADDON-1938)
- In saved search "Monthly Cost till *" _time is displayed per day rather than per month. (ADDON-2029)
- The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the

proxy field to 0 and saves an encrypted entry in `app.conf`. (ADDON-2113)
- If user does not provide a friendly name when configuring an AWS account in the setup screen, account is not configured but no error message appears (ADDON-2115)
- On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page. (ADDON-2116)
- The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account. (ADDON-2135)
- In Splunk 6.2, when network is unstable, some input configuration fields fail to display in Splunk Web and no error message is shown. (ADDON-2110)

Third-party software attributions

Version 1.0.1 of the Splunk Add-on for Amazon Web Services incorporated boto - AWS for Python.

Version 1.0.0

Version 1.0.0 of the Splunk Add-on for Amazon Web Services had the same compatibility specifications as version 1.0.1.

Known issues

Version 1.0.0 of the Splunk Add-on for Amazon Web Services had the following known issues:

- Errors can occur in checkpointing if modular input `stdout` is prematurely closed during termination. (SPL-81771)
- After initial configuration, adjusting Max trackable items might cause data loss. (ADDON-1854)
- Splunk Enterprise does not validate Amazon Web Services credentials during add-on setup. (ADDON-1885)
- If user tries to update a billing report manually using Microsoft Excel, the add-on cannot process the modified file and throws "failed to parse key" error. (ADDON-1895)
- If a user changes the configuration to use a different AWS account, Splunk Web continues to list buckets for the previously configured account. (ADDON-1919)
- Splunk Web allows you to update and delete an AWS account for the add-on simultaneously. (ADDON-1926)
- Setup and configuration pages in Splunk Web give unfriendly error messages when given invalid inputs (ADDON-1932, ADDON-2006)
- If Splunk Enterprise restarts while indexing S3 data, data duplication might occur. Workaround: Use AWS command line tools. (ADDON-1983 and ADDON-1938)
- In saved search "Monthly Cost till *" _time is displayed per day rather than per month. (ADDON-2029)
- The `app.conf` file includes a stanza for a proxy server configuration with a hashed password even if the user has not configured a proxy or password. This behavior is expected because Splunk Enterprise automatically sets the proxy field to 0 and saves an encrypted entry in `app.conf`. (ADDON-2113)
- If user does not provide a friendly name when configuring an AWS account in the setup screen, account is not configured but no error message appears (ADDON-2115)
- On Windows 2012, Splunk Web shows a timeout error when a user attempts to add or delete an AWS account on the setup page. Workaround: Refresh the page. (ADDON-2116)
- The list of regions shown in inputs configuration in Splunk Web shows all Amazon regions regardless of the permissions associated with the selected AWS account. (ADDON-2135)
- In Splunk 6.2, when network is unstable, some input configuration fields fail to display in Splunk Web and no error message is shown. (ADDON-2110)

Third-party software attributions

Version 1.0.0 of the Splunk Add-on for Amazon Web Services incorporated boto - AWS for Python.