

Data Manager: Seamless Onboarding Comes to Splunk Enterprise



PLA1513



Forward- looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

splunk>

.conf25

Data Manager: Seamless Onboarding Comes to Splunk Enterprise



**Kasia
Szulc**

Staff Product Manager | Splunk



**Antoni
Komorowski**

Staff Product Manager | Splunk

What makes Data Manager so great?



Time To Value

Spend your time using the data, not just getting it in



No cloud expertise needed

Don't worry so much about how the data gets here, we take care of all that for you



One tool to rule them all

AWS, Azure, GCP – wherever your data comes from, you can manage it centrally

How will Data Manager simplify your job?

- No more context switching—we guide you step by step.
- We'll only ask for input when needed.
- Monitor all data ingestions from public clouds in one dashboard.

splunk > enterprise App

[Data Manager/SCDM] Dashboards App settings

Cloud Sources

All Status All Type Search by Data Input Name

General Status	Data input name	Destination	Data Volume (GB)
Issue	S3 - Configured Data Source	Main Index	30.116
Issue	CloudWatch Logs - Ingested Data	Security Events Index	25.678
Warning	Event Hub - Security Ingestion	Security Events Index	59.09
Warning	AWS Metadata - Data Configuration	Application Logs Index	2.123
Warning	Azure Event Hub - Configured Security	Web Traffic Index	79.02
Success	AWS CloudWatch - Configuration Logs	Performance Metrics Index	156.01
Success	Activity Logs - Security Monitoring	Cloud Infrastructure Index	97.611
Success	CloudWatch Logs - Activity Monitoring	Syslog Data Index	18.09
Success	CloudWatch - Security Logs	Network Logs Index	79.011
Success	Azure Microsoft Entra ID - Secure Configuration	Database Activity Index	4.01
Success	S3 - Activity Log Ingestion	Error Logs Index	112.56
Success	AWS CloudTrail - Security Logs	System Events Index	2.123
Success	Microsoft Entra ID - Secure Configuration	User Authentication Logs Index	79.011
Success	AWS S3 - Security Data	Backup Data Index	4.01

What we are going to learn today

- Challenges and solutions for acquiring public cloud data
- Key features and benefits of Data Manager on Customer-Managed Splunk on AWS

**“I want to monitor
my public cloud
infrastructure”**



**“I want to monitor
my public cloud
infrastructure”**

**What data source
do I need to select
and onboard?**



“I want to monitor my public cloud infrastructure”

What data source do I need to select and onboard?

What prerequisites must I complete before configuring data input?



“I want to monitor my public cloud infrastructure”

What data source do I need to select and onboard?

What prerequisites must I complete before configuring data input?

How do I configure the data input for this source?



“I want to monitor my public cloud infrastructure”

What data source do I need to select and onboard?

What prerequisites must I complete before configuring data input?

How do I configure the data input for this source?

How do I manage and monitor my data inputs after ingestion?



“I want to monitor my public cloud infrastructure”

Install Data Manager from Splunkbase

Get more out of Splunk with applications

Q Search for apps



Trending Apps on Splunkbase

 Splunk Enterprise Security By Splunk LLC	 Splunk DB Connect By Splunk LLC	 Splunk Security Essentials By Splunk LLC	 Splunk Add-on for Microsoft Windows By Splunk LLC
Splunk Enterprise Security (ES) solves a wide range of security analytics and operations use cases including...	Splunk DB Connect is a generic SQL database extension for Splunk that enables easy integration of database...	Get started with Splunk for Security with Splunk Security Essentials (SSE). Explore security use cases and discover securit...	*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on f...
PLATFORM Splunk Enterprise, Splunk Cloud	PLATFORM Splunk Enterprise, Splunk Cloud,...	PLATFORM Splunk Enterprise	PLATFORM Splunk Enterprise, Splunk Cloud,...
RATING ★★★★★ (222)	RATING ★★★★★ (137)	RATING ★★★★★ (56)	RATING ★★★★★ (48)
 SPLUNK SUPPORTED APP	 SPLUNK SUPPORTED ADDON	 SPLUNK SUPPORTED APP	 SPLUNK SUPPORTED ADDON



“I want to monitor my public cloud infrastructure”

Install Data Manager from Splunkbase

Provide HEC endpoint and authentication method

The screenshot shows the Splunk Enterprise interface for configuring the HEC endpoint and authentication method. The top navigation bar includes the Splunk logo, 'enterprise' app name, and user 'Wayne'. The breadcrumb trail shows 'Data Manager/SCDM' > 'Dashboards' > 'App settings'. The main content area is titled 'App settings' and contains two sections: 'HEC (HTTP Event Collector) endpoint' and 'Authentication Method'. The HEC section shows a status of 'Normal' and a 'Hec Details' link. The Authentication Method section shows 'IAM Role' as the selected method and lists four ARN roles.

splunk > enterprise App

[Data Manager/SCDM] Dashboards App settings

App settings

HEC (HTTP Event Collector) endpoint [Edit HEC endpoint](#)

The Data Manager settings for receiving data from logging agents and HTTP clients through the HTTP Event Collector (HEC).

Status	Hec Details
● Normal	?

Authentication Method [Change Method](#)

The two authentication methods available are IAM Role and User Secret. We recommend using IAM Role for the smoothest data ingestion experience, as it helps save time and minimizes errors. However, User Secret can also be used if preferred, offering flexibility for different user needs.

Authentication	IAM Role
ARN Roles	arn:aws:iam::123456789012:role/service-*
	arn:aws:iam::123456789013:role/service-*
	arn:aws:iam::123456789014:role/service-*
	arn:aws:iam::123456789015:role/service-*

“I want to monitor my public cloud infrastructure”

Install Data Manager from Splunkbase

Provide HEC endpoint and authentication method

Define data input

2. Input AWS CloudWatch Logs Information

Enter a **Data Input Name**

HEC (HTTP Event Collector) endpoint

The Data Manager settings for receiving data from logging agents and HTTP clients through the HTTP Event Collector (HEC).

Hec details: <https://www.example.com/blog/article/search>

Provide information on the source of you data

Provide the management account ID or the delegated administrator account ID for your AWS organization.

Enter a Single **AWS Control Account ID**

Manage discovered **Organizational Units**

Data Manager will automatically onboard new AWS accounts that are added to the selected organizational units (OUs) in the future, and start collecting data from those accounts. Alternatively, when accounts are removed from the selected OUs, Data Manager will stop collecting data from those accounts.

Select Organizational Units

Choose **AWS Control Account ID**

Select region

Select **IAM Roles region**

Choose the region allowed by your company policies and for other compliance reasons for setting the IAM roles

Select region

Selected **Data Sources**

Mke sure your data sources are configured as described in the Data Sources section of the Instructions panel. To edit your selected data source, click the "Edit" link next to your chosen Selected Service. If you made any changes to your data destinations after reaching this page, click "Refresh" to get the latest destinations.

Data Source Edit	Destination Refresh
All Selected Services	Select destination
Amazon API Gateway	Select destination
AWS CloudHSM	Select destination
Amazon DocumentDB	Select destination
Amazon EKS	Select destination
AWS Lambda	Select destination
Amazon RDS	Select destination

Provide **HEC Tokens**

To grant Data Manager access to your data, you need to create a token that will be used during the onboarding process. Note: Tokens can be used for multiple data sources. You can update them later from global settings. Follow these steps to generate and configure your token [Content needs to be updated]:

Define **Token 1**

Expand to view instruction

Follow these parameters to create [Token 1] for [Data Source X] and [Data Source Y].

Here's what you need to enter:

1. Name: scdm-hec-token_123125-123213-123123
2. Source Name Override: aws_cloudtrail_1232123-1232131-123213
3. Enable Indexer Acknowledge: Yes
4. Source Type: aws:cloudtrail
5. Default Index: main

Enter Token Value

“I want to monitor my public cloud infrastructure”

Install Data Manager from Splunkbase

Provide HEC endpoint and authentication method

Define data input

You're all set! Your public cloud data is ready to roll.

splunk > enterprise App

[Data Manager/SCDM] Dashboards App settings

Cloud Sources

All Status All Type Search by Data Input Name

General Status	Data input name	Cloud Provider	Destination	Da
Issue	S3 - Configured Data Source	Amazon Web Services	Main Index	30
Issue	CloudWatch Logs - Ingested Data	Amazon Web Services	Security Events Index	25
Warning	Event Hub - Security Ingestion	Microsoft Azure	Security Events Index	59
Warning	AWS Metadata - Data Configuration	Amazon Web Services	Application Logs Index	2
Warning	Azure Event Hub - Configured Security	Microsoft Azure	Web Traffic Index	79
Success	AWS CloudWatch - Configuration Logs	Amazon Web Services	Performance Metrics Index	15
Success	Activity Logs - Security Monitoring	Microsoft Azure	Cloud Infrastructure Index	97
Success	CloudWatch Logs - Activity Monitoring	Amazon Web Services	Syslog Data Index	18
Success	CloudWatch - Security Logs	Amazon Web Services	Network Logs Index	79
Success	Azure Microsoft Entra ID - Secure Configuration	Microsoft Azure	Database Activity Index	4
Success	S3 - Activity Log Ingestion	Amazon Web Services	Error Logs Index	11
Success	AWS CloudTrail - Security Logs	Amazon Web Services	System Events Index	2
Success	Microsoft Entra ID - Secure Configuration	Microsoft Azure	User Authentication Logs Index	79
Success	AWS S3 - Security Data	Amazon Web Services	Backup Data Index	4

Hello World—Meet Our First Release!

What's included?



Only for Splunk hosted on AWS

You're still able to bring in data from AWS, Azure, and GCP.



Push-based mechanism only

Additional features may be introduced in future releases.



Step-by-step help provided, just assist us

Your help is needed for the initial AWS setup and HEC token management.

Thank you

