

AWS Cost Explorer

 dev.classmethod.jp/articles/sending-aws-cost-explorer-logs-to-sumo-logic

HemanthKumar R

October 22, 2023



目次

Introduction

Hemanth from the Alliance Department here. Today, I'm excited to share insights on how to easily integrate your AWS Cost Explorer logs with Sumo Logic by streamlining your log management process.

Sumo Logic

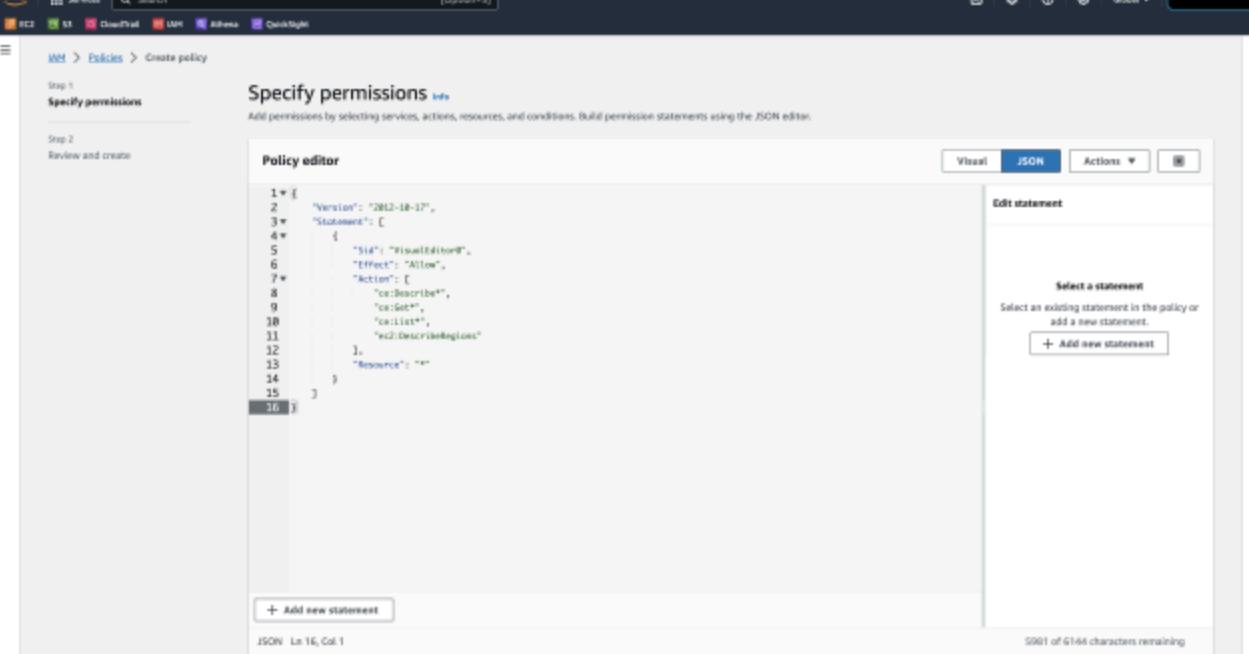
A cloud-based log management and analytics software called Sumo Logic which enables businesses to exploit their machine data for useful insights. Sumo Logic's flexible capabilities make log data analysis simple and offer real-time visibility into operational and security insights.

An AWS Service that'll assist you in managing and optimizing your AWS consumption and costs is AWS Cost Explorer. Use forecasts, reports, and graphs to see and analyze your data. Make personalized reports by utilizing filters, groups, and time intervals. Use the API

to retrieve your data programmatically. Find pricing anomalies and receive recommendations for Reserved Instances. Make a budget and project your future consumption and spending.

Demo

Begin by creating an access key for an IAM user with the following policy in AWS



The screenshot shows the AWS IAM 'Create policy' wizard. The left sidebar shows 'Step 1: Specify permissions' and 'Step 2: Review and create'. The main area is titled 'Specify permissions' with a note: 'Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.' Below this is a 'Policy editor' section with a JSON code view:

```
1 * {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "#VisualEditor#",
6             "Effect": "Allow",
7             "Action": [
8                 "ec2:Describe",
9                 "ec2:List",
10                "ec2:DescribeRegions"
11            ],
12            "Resource": "*"
13        }
14    ]
15 }
16 }
```

To the right of the JSON editor is a 'Select a statement' panel with a 'Edit statement' button and a '+ Add new statement' button. At the bottom of the editor are buttons for 'Add new statement' and 'Next Step'. The status bar at the bottom indicates 'JSON: Ln 16, Col 1' and '5981 of 6144 characters remaining'.

Log in to your Sumo Logic account, navigate to "Manage Data," and click on "Add Collector"

The screenshot shows the Sumo Logic interface with a sidebar containing various collection and monitoring options. The main area displays a list of collectors, including AWS Security Hub, AWS CloudTrail, and AWS CloudWatch Metrics. A modal window titled "Select Collector Type" is overlaid on the page, offering two choices: "Installed Collector" and "Hosted Collector". The "Hosted Collector" option is highlighted.

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
AWS - CM Alliance Account	Healthy	Hosted	--	CM/SecurityHub	1	None	Add Source Edit Delete
AWS Security Hub	Healthy	Hosted	--	CM/SecurityHub	1	None	Add Source Edit Delete
AWS CloudTrail - Sakuno	Healthy	Hosted	--	CloudTrail	1	None	Add Source Edit Delete
AWS EC2 Linux - Sakuno	Healthy	Hosted	--	CloudWatch Metrics	3	None	Add Source Edit Delete
Kinesis Firehose Source - Host Logs	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
Kinesis Firehose Source - Host Metrics	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
S3Source - HostLog	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
AWS Security Hub Sakuno	Healthy	Hosted	--	CloudWatch Metrics	1	None	Add Source Edit Delete
AWS Security Hub	Healthy	Hosted	--	CloudWatch Metrics	1	None	Add Source Edit Delete
aws-observability-308914410845-3...	Healthy	Hosted	--	CloudWatch Metrics	1	None	Add Source Edit Delete
cloudtraillogs-ap-northeast-1	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
AWS CloudTrail	---	--	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
aws-observability-53355424459-5...	Healthy	Hosted	--	CloudWatch Metrics	6	3,075	Add Source Edit Delete
alb-logs-ap-northeast-1	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
classic-logs-ap-northeast-1	Healthy	---	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete
elasticsearch-metrics-ap-northeast-1	---	--	--	CloudWatch Metrics	1	None	CloudWatch Metrics Edit Delete

Select the hosted collector option, assign a name, and save your settings

The screenshot shows the Sumo Logic interface with a sidebar containing various collection and monitoring options. The main area displays a list of collectors, including AWS Security Hub, AWS CloudTrail, and AWS CloudWatch Metrics. A modal window titled "Select Collector Type" is overlaid on the page, offering two choices: "Installed Collector" and "Hosted Collector". The "Hosted Collector" option is highlighted.

Proceed to select the source for your collector. Enter the AWS access key and AWS Secret Key with the appropriate permissions, then save the configuration

The screenshot shows the Sumo Logic interface with the 'Collection' tab selected in the sidebar. A modal window titled 'AWS Cost Explorer' is open, showing configuration details for a new collector named 'Personal_AWS_Cost_Explorer'. The configuration includes:

- Name:** Personal_AWS_Cost_Explorer
- Description (optional):** AWSCostExplorerPersonalKumar
- Source Category (optional):** AWSCostExplorerPersonalKumar
- Fields:** A table with one row and two columns: 'Key' and 'Value', with a '+ Add' button.
- API Access Key:** [REDACTED]
- API Secret Key:** [REDACTED]
- Enable Regions (optional):** A note stating "If empty, all AWS enabled regions will be monitored. It is recommended to monitor only actively used regions to save AWS cost for this source."
- Cost Type:** AnnotatedCost
- Granularity:** Daily Costs (Pulled every 12h) and Monthly Costs (Pulled every day) are checked.

The screenshot shows the 'Processing Rules for Logs' section for the 'Personal_AWS_Cost_Explorer' collector. It includes:

- Filters (Optional):** A note stating "Define filters to include or exclude data sent to Sumo Logic." with a '+ Add Filter' button.
- Actions (Optional):** A note stating "Hash or Mask logs that contain sensitive information before they are sent to Sumo Logic." with a '+ Add Action' button.

At the bottom of the modal are 'Cancel' and 'Save' buttons.

Successfully created

Head over to the app catalog in Sumo Logic and search for the AWS Cost Explorer app. Install the app for further integration.

The screenshot shows the Sumo Logic App Catalog interface. On the left, there's a sidebar with navigation links like 'App Catalog', 'Manage Data', 'Administration', 'Cloud SIEM Enterprise', 'Automation', and 'Help'. The main area has a search bar at the top. Below it, there are two main sections: 'Next-Gen Apps' and 'Classic Apps'. The 'Next-Gen Apps' section contains a single item: 'No Next-Gen apps match your search'. The 'Classic Apps' section lists several AWS services with corresponding icons: AWS API Gateway, AWS Amplify, AWS App Runner, AWS AppSync, AWS Application Load Balancer, AWS Application Migration Service, AWS Backup, AWS Certificate Manager, AWS Chatbot, AWS Classic Load Balancer, AWS Client VPN, AWS CloudHSM, AWS CloudTrail, AWS CodeBuild, AWS Config, and AWS Cost Explorer. The 'AWS Cost Explorer' icon is highlighted with a blue border.

The screenshot shows the Sumo Logic App Catalog interface. On the left is a sidebar with navigation links like Audit, Data Volume, Kubernetes, Security Hub Multiaccounts, etc. The main area displays the "AWS Cost Explorer" app by Sumo Logic. It features a "Classic App" section with an "Install App" button, a note about permissions, and four preview cards: "AWS Cost Explorer - Account", "AWS Cost Explorer - Operations", "AWS Cost Explorer - Region", and "AWS Cost Explorer - Services".

Enter the folder name

This screenshot shows the first step of the "Configure AWS Cost Explorer" wizard. It's titled "Select Folder Location for your App" and has a "Folder Name" input field containing "AWS Cost Explorer V2". Below it is a "All Folders" list table with columns "Name" and "Description". The table lists several items, including "Personal", "Bill Audit", "Bill AWS Security Hub v2", "Bill Data Volume", "Bill Security Hub-Multiaccounts", and "Bill Support".

Now witness the creation of insightful dashboards for AWS Cost Explorer data analysis

SUMO LOGIC

Configure AWS Cost Explorer

Preview & Done

Success! Open one of the dashboards below to start exploring your data, or go to My Content Library.

AWS Cost Explorer - Account

This dashboard provides detailed information about cost and usage by different AWS accounts.

AWS Cost Explorer - Operations

This dashboard provides detailed information about cost and usage by operations performed by various services in AWS accounts.

AWS Cost Explorer - Region

This dashboard provides detailed information about cost and usage by different AWS Regions and accounts.

Recommended Integrations

As a AWS Cost Explorer user, you might benefit from using these other integrations. Click the tile below to get started.

- Amazon Kinesis - Streams
- Windows Performance
- Global Intelligence for AWS CloudTrail - SecOps

In the AWS Cost explorer - Account Dashboard, you can see the weekly costs and cost incurred by service

SUMO LOGIC

AWS Cost Explorer - Account

MetricType: ActualizedCost, estimated: true

Metric Type

- Metric Type
 - Refer [AWS cost checklist](#).
- Estimated
 - Use **true** to monitor estimated / forecasted cost.
 - Use **false** to monitor actual cost. Actual cost is available once in a month after invoice is generated.
- It can take up to 48 hours for AWS to generate your billing data. For accuracy Sumo Logic does not present any billing analysis for the last 48-49 hours.

Weekly Costs

Total Cost

Cost by Service

Cost by Metric Type

Cost by Region

Error!

Field LinkedAccount not found, please check the spelling and try again.

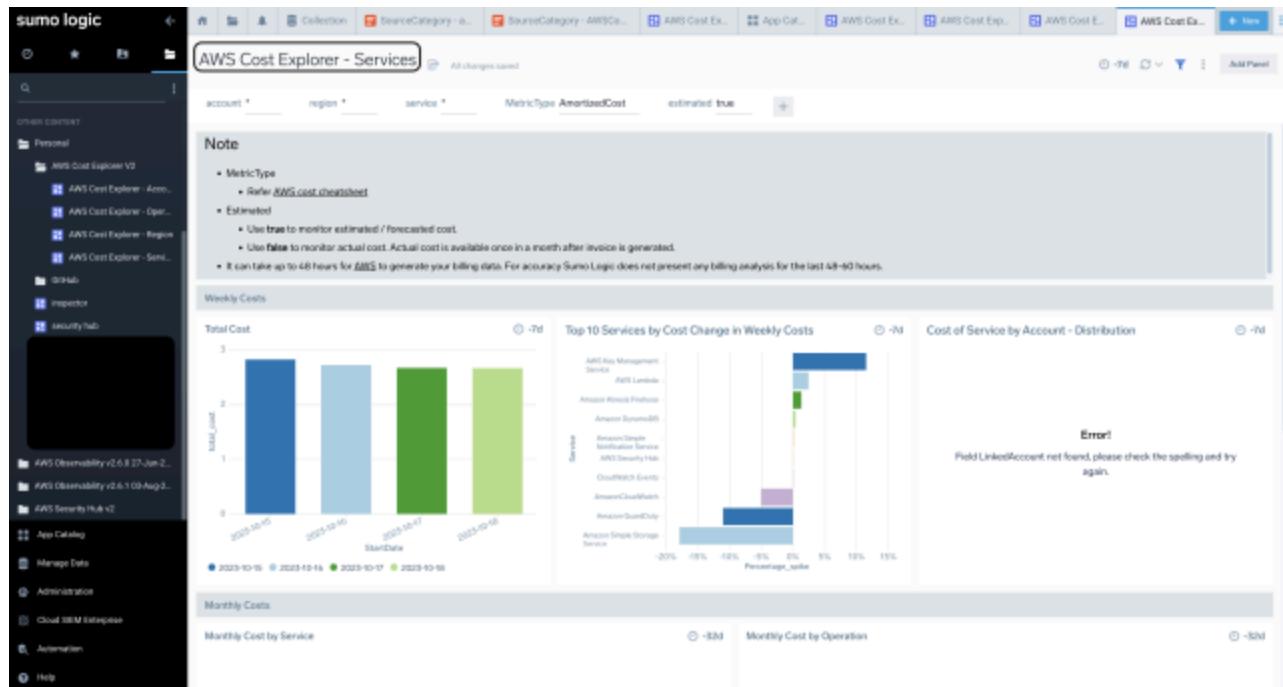
Cost by Operation

Top 10 Accounts by Costs

Error!

Field LinkedAccount not found, please check the spelling and try again.

Now checking other dashboards, here you can see a panel top 10 services by cost change in weekly costs



Conclusion

Through Sumo Logic, businesses can effortlessly manage AWS Cost Explorer logs and obtain useful insights into their AWS expenditure and consumption habits. Organizations may save expenses, improve operational effectiveness, and make data-driven decisions by utilizing the strength of these powerful capabilities, which will result in a more efficient and economical AWS management process.

いま
お探しの
解決策は
クラスメソッドに



コンサルティングからシステム構築後の運用
保守代行まで、AWSクラウド環境を支援します。

[技術支援サービスを見る](#)

classmethod

EVENTS



[【1/29（木）】クラスメソッドの会社説明会を開催します](#)

開催前



【1/28 (水)】クラスメソッドの新卒向け会社説明会を開催します

開催前



【CMグループ/エンド直案件特集】ITフリーランス向け「CMパートナーズ」説明会 by クラスメソッド

開催前



【2/5 (木) 東京】オペレーターの生産性を50%アップ！見て、聞いて、納得できるAIコールセンター実演セミナー

開催前



【2/25 (水)】AI駆動開発、実際どうなの？【実践編】～現場でぶつかる課題と乗り越え方～

[開催前](#)



[【1/29\(木\)】今日から始めるAWSセキュリティ対策 3ステップでわかる実践ガイド](#)

[開催前](#)

[セミナー一覧](#) [会社説明会一覧](#) [勉強会一覧](#)