AWS Solutions Architect Associate

Session 1102

Auditing and Compliance

August/2024

Auditing Tools

- Management & Governance:
  - CloudTrail
  - Config
  - Trusted Advisor
  - Cloudwatch Logs
- Security, Identity, & Compliance:
  - GuardDuty
  - Inspector


AWS CloudTrail


AWS Config


AWS Trusted Advisor


Amazon CloudWatch


Logs

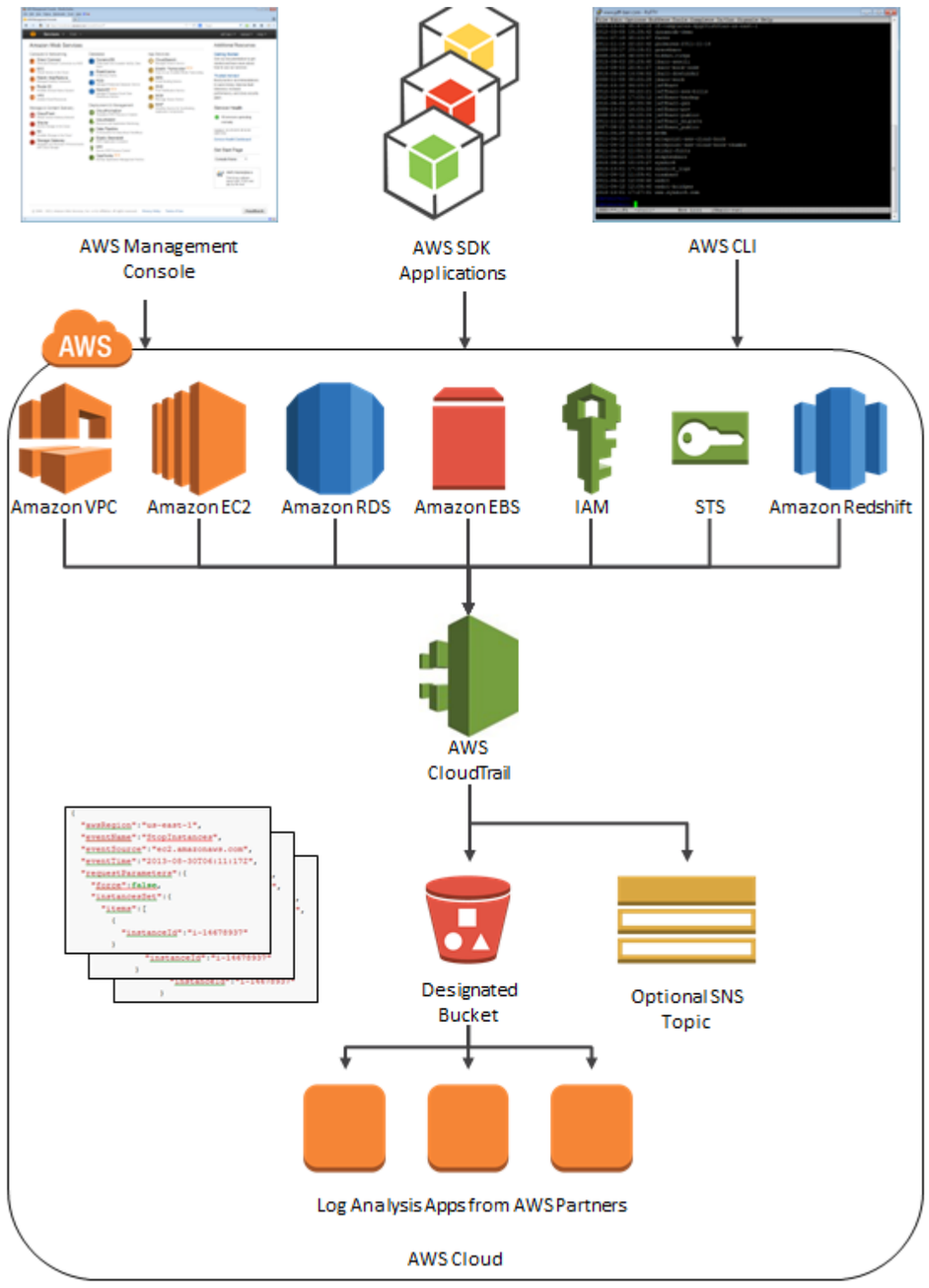

Amazon GuardDuty


Amazon Inspector

AWS CloudTrail

- Allow continuously monitor and retain account activity related to actions across your AWS infrastructure (Upto Multiregion).
- Data Integrity and Encryption.
- Integration with services to flow changes (Lambda, Cloudwatch Logs, Cloudwatch Events).
- Cloudtrail Insigths: Detect Inusual Activity on your AWS Account.
- Cloudtrail Lake: capturing, storing, accessing, and analyzing user and API activity on AWS for audit and security purposes.
- Separate Data Events (Data Plane): Object Level on S3, invoke Lambda Functions, Item level on DynamoDB and Management Events (Control Plane).
- **Pricing:** Default Free for events last 90 days. If you need to more time or specify more features (Additional copy on S3, Management Events, Insigths) you have to able a Trail

AWS CloudTrail

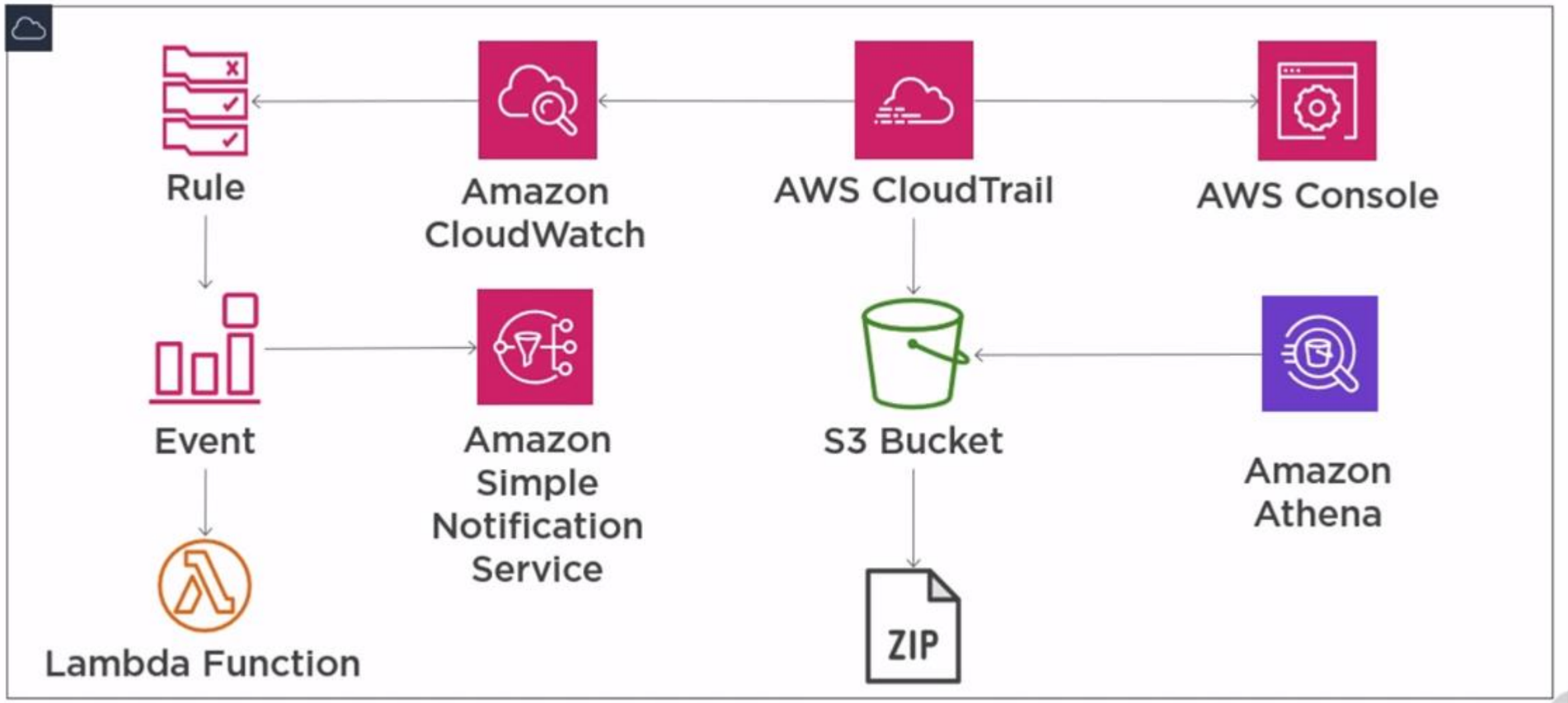


Free Tier

Event history	CloudTrail logs management events across AWS services by default and is available for no charge. You can view, search, and download the most recent 90-day history of your account's control plane activity at no additional cost using CloudTrail in the CloudTrail console. You can also use the CloudTrail lookup-events API to achieve this.
Lake	If you're a new customer, you can try CloudTrail Lake for 30 days at no additional cost. You'll have access to the full feature set during this time. During the 30-day free trial period, you'll have the following limits: • Ingest up to 5 GB of data • Scan up to 5 GB of data • Retain data at no additional cost Your free trial expires after 30 days or when you reach the free usage limits, whichever comes first. When your free trial expires, you can continue using CloudTrail Lake without interruption at the standard, pay-as-you-go service rates described in the Paid Tier section.
Trails	You can deliver one copy of your ongoing management events to your Amazon Simple Storage Service (S3) bucket for free by creating trails. Limits may apply.

Taken https://aws.amazon.com/blogs/aws/aws-cloudtrail-capture-aws-api-activity/ and https://aws.amazon.com/cloudtrail/pricing/ (20/07/2024)

Use Case



- AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account.
- Perform security analysis and detect user behavior patterns by ingesting AWS CloudTrail events into your log management and analytics solutions.
- Detect unusual activity in your AWS accounts by enabling CloudTrail Insights

Taken https://aws.amazon.com/blogs/aws/aws-cloudtrail-capture-aws-api-activity/ and https://aws.amazon.com/cloudtrail/pricing/ (24/06/2021)

Use Case

aws Servicios cvallada35 Norte de Virginia

CloudTrail

- Dashboard
- Event history
- Insights
- Trails

- Pricing
- Documentation
- Forums
- FAQs

Use the old console

CloudTrail > Event history

Event history (9) Info

Download events | Create Athena table

Resource type: AWS::S3::Bucket | 30m | 1h | 3h | 12h | Custom | 1

Event name	Event time	User name	Event source
PutBucketWebsite	September 27, 2020, 18:29:14 (UTC-05:00)	root	s3.amazonaws.com
PutBucketWebsite	September 27, 2020, 18:28:52 (UTC-05:00)	root	s3.amazonaws.com
PutBucketReplication	September 27, 2020, 17:27:34 (UTC-05:00)	root	s3.amazonaws.com
PutBucketAcl	September 27, 2020, 17:17:00 (UTC-05:00)	root	s3.amazonaws.com
CreateBucket	September 27, 2020, 17:16:59 (UTC-05:00)	root	s3.amazonaws.com
PutBucketVersioning	September 27, 2020, 17:16:59 (UTC-05:00)	root	s3.amazonaws.com

CloudTrail

We're continuing to improve the CloudTrail Lake console experience to make it easier to use. Let us know what you think.

New CloudTrail event data store pricing tier
View the new pricing page to find out which event data store pricing tier best fits your use cases, and how to get the most out of your CloudTrail Lake setup!

Create event data store

- Dashboard
- Event history
- Insights
- Lake
  - Dashboard
  - Query
  - Event data stores
  - Integrations
- Trails

- Settings

- Pricing
- Documentation
- Forums
- FAQs

CloudTrail > Event history

Event history (50+) Info

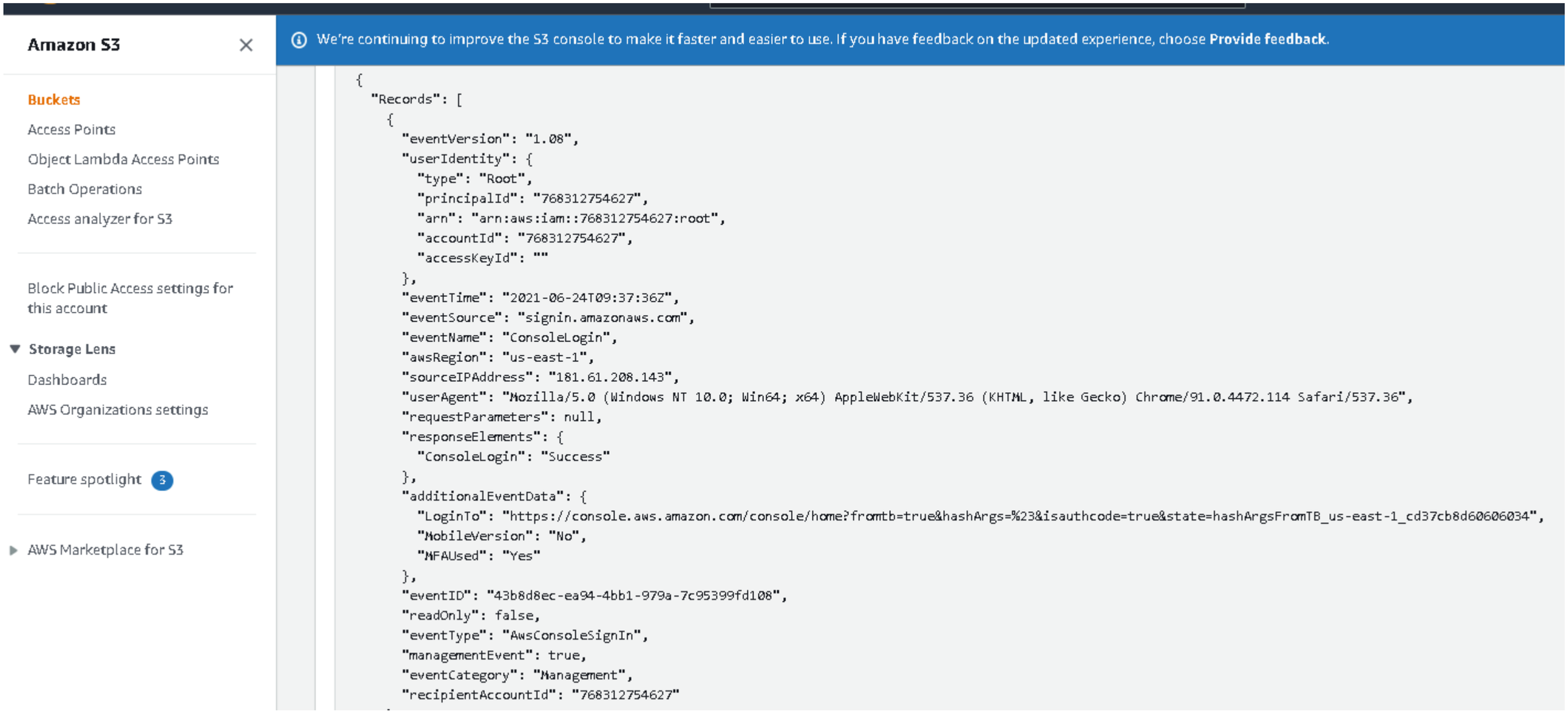
Event history shows you the last 90 days of management events.

Download events | Create Athena table

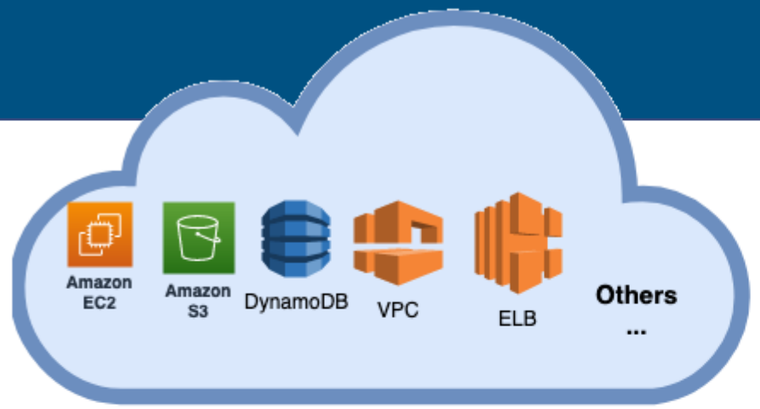
Lookup attributes

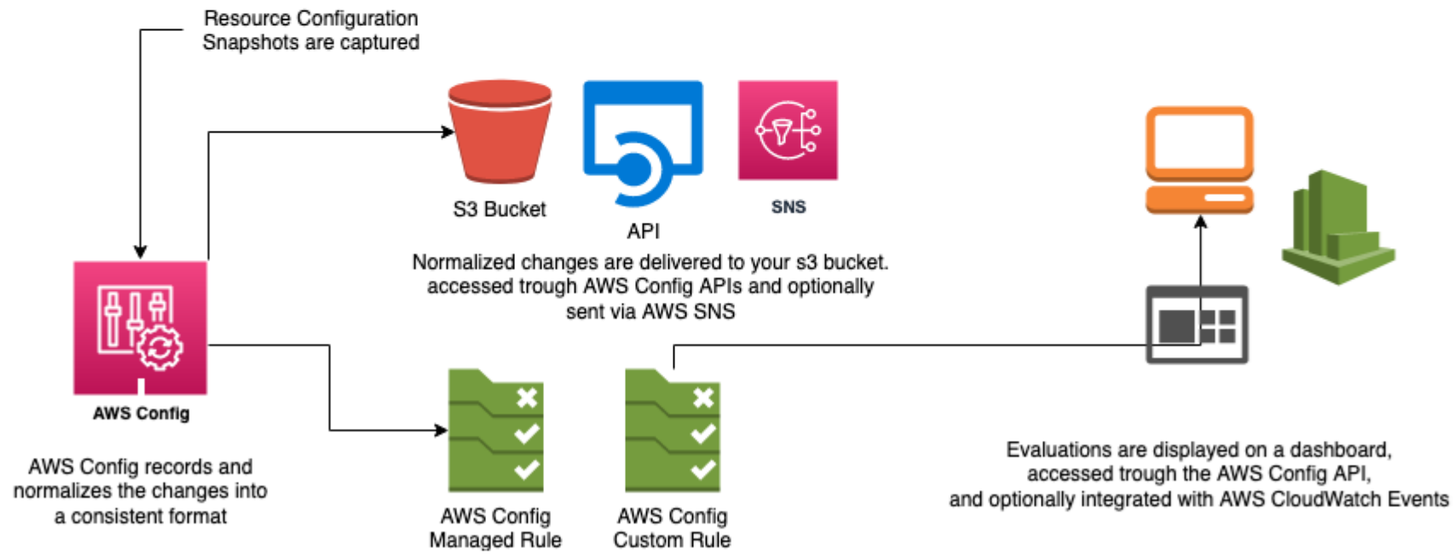
Resource type: AWS::S3::Bucket | Filter by date and time | 1 2 ...

Event name	Event time	User name	Event source	Resource type	Resource name
CreateBucket	July 27, 2024, 06:16:15 (UTC-05:00)	root	s3.amazonaws.com	AWS::S3::Bucket	cf-templates-4j96stmv...
DeleteBucket	July 25, 2024, 04:37:53 (UTC-05:00)	fmorenod@gmail....	s3.amazonaws.com	AWS::S3::Bucket	www.ocidemo1280.re...
DeleteBucket	July 25, 2024, 04:37:31 (UTC-05:00)	fmorenod@gmail....	s3.amazonaws.com	AWS::S3::Bucket	www.ocidemo1280.re...
DeleteBucket	July 25, 2024, 04:36:47 (UTC-05:00)	fmorenod@gmail....	s3.amazonaws.com	AWS::S3::Bucket	www.ocidemo1280.re...
DeleteBucket	July 25, 2024, 04:36:09 (UTC-05:00)	fmorenod@gmail....	s3.amazonaws.com	AWS::S3::Bucket	www.ocidemo1280.re...
DeleteBucketWebsite	July 25, 2024, 04:36:08 (UTC-05:00)	fmorenod@gmail	s3.amazonaws.com	AWS::S3::Bucket	www.ocidemo.online


Amazon S3
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
Buckets
Access Points
Object Lambda Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
{
"Records": [
{
"eventVersion": "1.08",
"userIdentity": {
"type": "Root",
"principalId": "768312754627",
"arn": "arn:aws:iam::768312754627:root",
"accountId": "768312754627",
"accessKeyId": ""
},
"eventTime": "2021-06-24T09:37:36Z",
"eventSource": "signin.amazonaws.com",
"eventName": "ConsoleLogin",
"awsRegion": "us-east-1",
"sourceIPAddress": "181.61.208.143",
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36",
"requestParameters": null,
"responseElements": {
"ConsoleLogin": "Success"
},
"additionalEventData": {
"LoginTo": "https://console.aws.amazon.com/console/home?fromtb=true&hashArgs=%23&isauthcode=true&state=hashArgsFromTB_us-east-1_cd37cb8d60606034",
"MobileVersion": "No",
"MFAUsed": "Yes"
},
"eventID": "43b8d8ec-ea94-4bb1-979a-7c95399fd108",
"readOnly": false,
"eventType": "AwsConsoleSignIn",
"managementEvent": true,
"eventCategory": "Management",
"recipientAccountId": "768312754627"

AWS Config





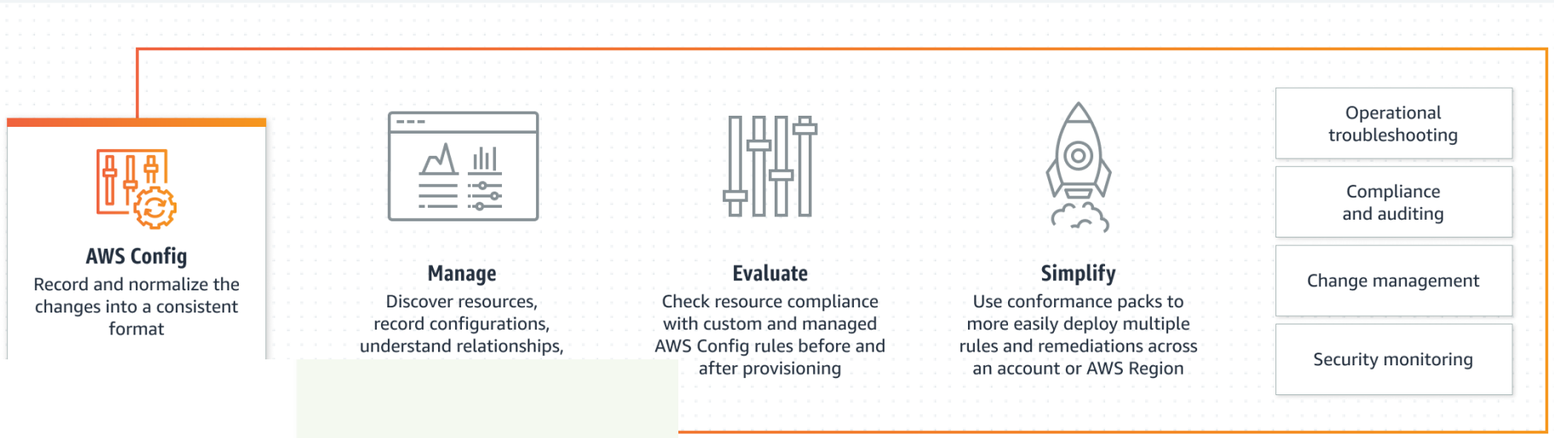
Managed Rules
Conformance Packs
Customized Rules:

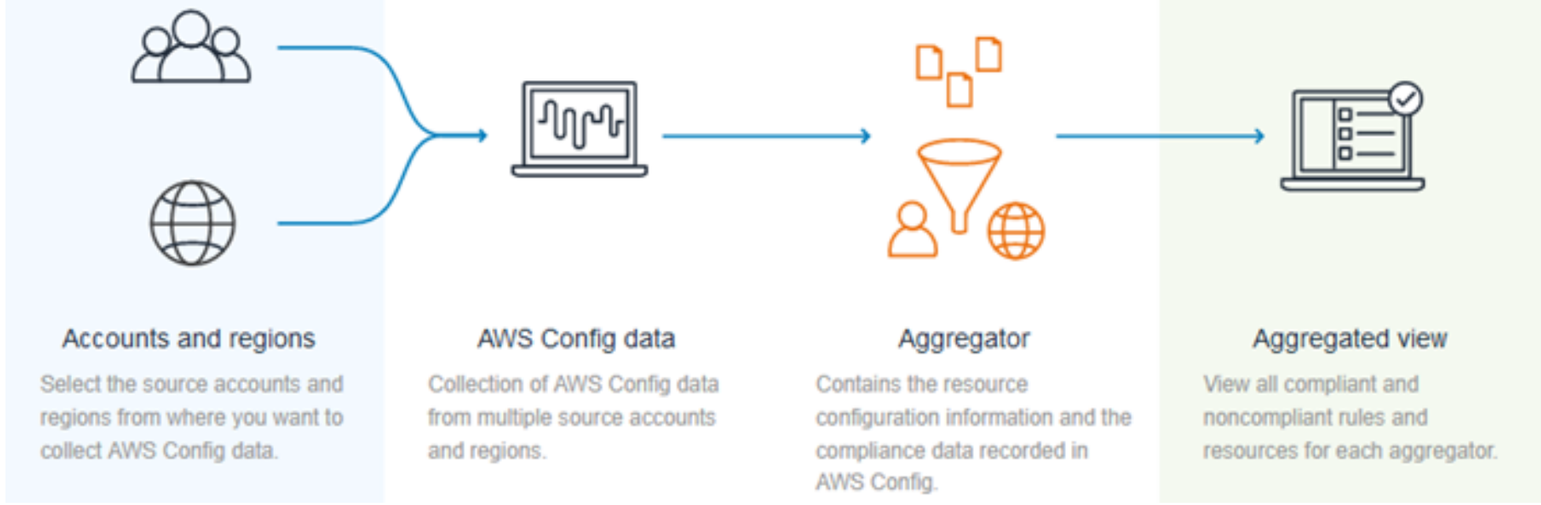
- Block Ports on Security Groups
- Tagging Policy: Cost Center

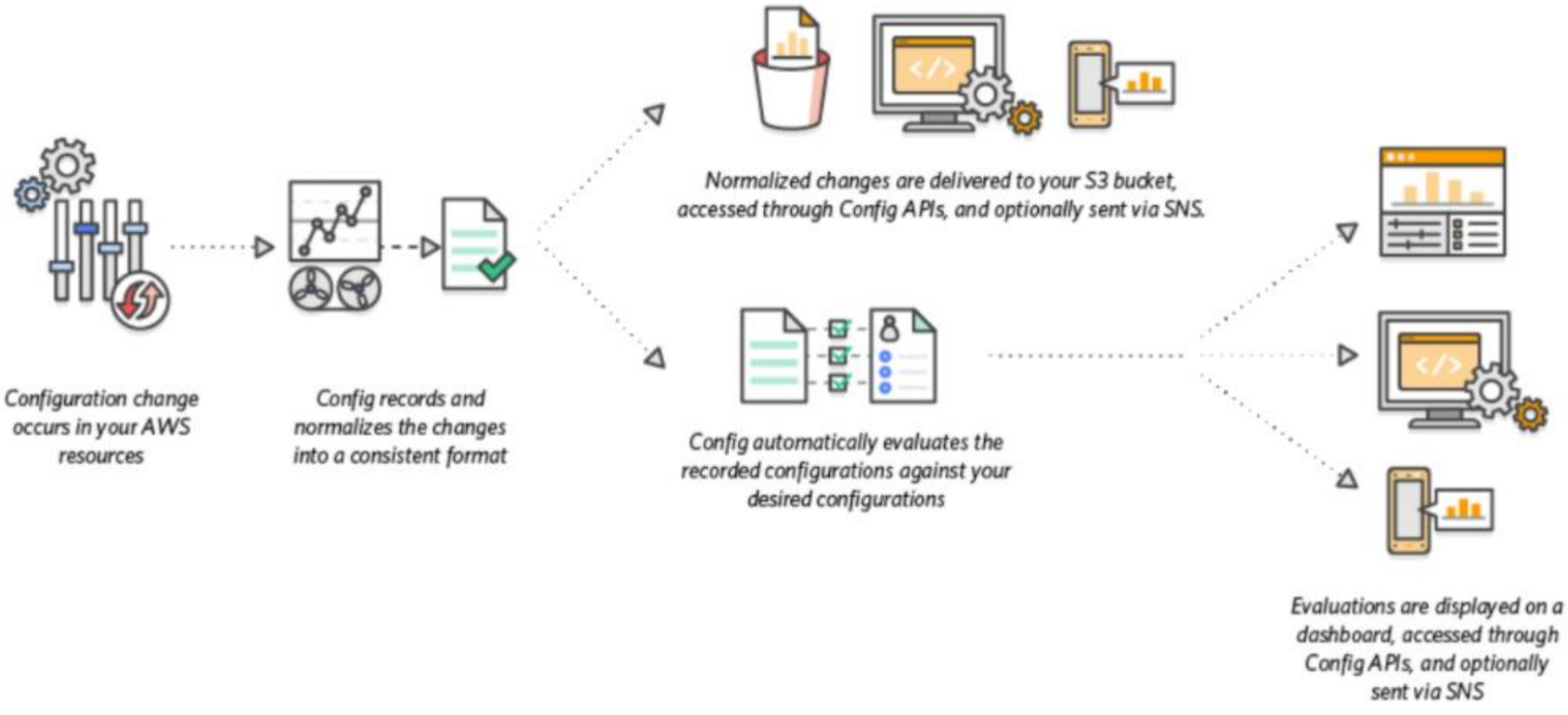
- AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources on AWS Accounts (Organizations).
- With Config, you can review changes in configurations (OS/Software) and relationships between AWS resources.
- AWS Config provides you with the ability to define rules for provisioning and configuring AWS resources.
- Config helps you identify the root cause of operational issues through its integration with AWS CloudTrail.
- Add extensibility for 3rd Party: i.e. GitHub and AD

Taken from https://aws.amazon.com/blogs/mt/using-aws-config-security-analysis-resource-administration/ (20/07/2024)

How to work Config







Taken from
https://docs.aws.amazon.com/config/latest/developerguide/how-does-config-work.html
(20/07/2024)

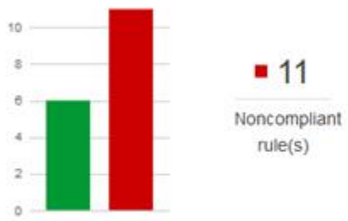
Use cases

Aggregated view

Aggregator: MyAgg | Region: All regions | Account: All accounts

Note: Data displayed in the dashboard is received from multiple aggregation sources and is refreshed at different intervals. Data might be delayed by a few minutes.

Config rule compliance



Top 5 noncompliant rules

Rule name	Region	Account	Compliance
cloudwatch-alar...	us-west-2		20 noncompliant resource(s)
iam-user-group-...	us-west-2		7 noncompliant resource(s)
s3-bucket-server...	us-west-2		7 noncompliant resource(s)
restricted-ssh	us-west-2		3 re
approved-amis-b...	us-west-2		2 re

View all noncompliant rules

Accounts by noncompliant rules

Account	Compliance
	6 noncompliant rule(s)
	5 noncompliant rule(s)

View all noncompliant rules

Rules > Rule details

s3-bucket-server-side-encryption-enabled

Region: us-west-2, Account:

Resources evaluated

Resource Type	Resource ID	Compliance	Last invocation time	Last result recorded time
S3 Bucket	-bucket2	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:36 PM
S3 Bucket	-bucket	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:37 PM
S3 Bucket	bucket	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:34 PM
S3 Bucket	bucket	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:35 PM
	cf-templates- -us-west-2	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:36 PM
	cfnconfigstack- - s7bvgto05m9c	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:36 PM
	mycloudtrail	Noncompliant	March 25, 2018 4:53:24 PM	March 25, 2018 4:53:37 PM

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

Aggregator: prod-aggregator | Region: All regions | Account: | Compliance status: All

Rule name	Compliance	Region	Account
s3-bucket-public-write-prohibited	Compliant	us-west-2	
dynamodb-autoscaling-enabled	2 noncompliant resource(s)	us-west-2	
cloudwatch-alarm-action-check	20 noncompliant resource(s)	us-west-2	
restricted-ssh	3 noncompliant resource(s)	us-west-2	
root-account-mfa-enabled	1 noncompliant resource(s)	us-west-2	
s3-bucket-public-read-prohibited	Compliant	us-west-2	
iam-user-group-membership-ch...	7 noncompliant resource(s)	us-west-2	

Taken from https://aws.amazon.com/blogs/mt/using-aws-config-security-analysis-resource-administration/ (24/06/2021)

Pricing

AWS Config

You pay per configuration item delivered in your AWS account per AWS Region. A configuration item is created whenever a resource undergoes a configuration change or a relationship change. The resource could be an AWS, third-party, or custom resource. A relationship defines how a resource is related to other resources within an AWS account. As a result, even when no new resources are created (such as when a security group is attached to an Amazon Elastic Compute Cloud [EC2] instance), a configuration item can be recorded.

There are two frequencies at which AWS Config can deliver configuration items: periodic and continuous. Periodic recording delivers configuration data once every 24 hours, only if a change has occurred, which may be useful for use cases such as operational planning or audit. Continuous recording delivers configuration items whenever a change occurs. It helps you meet security and compliance requirements to track all configuration changes.

You can stop recording configuration items at any time and still continue to access the previously recorded configuration items. Charges per configuration item are rolled up into your monthly bill.

AND

	Cost per configuration item delivered per AWS account per AWS Region
Continuous Recording	$0.003
Periodic Recording	$0.012

AWS Config rules

More info at: https://aws.amazon.com/config/pricing/ and https://www.vantage.sh/blog/aws-config-pricing (06/08/2024)

You are charged based on the number of AWS Config rule evaluations recorded. A rule evaluation is recorded every time a resource is evaluated for compliance against an AWS Config rule. Rule evaluations can be run in detective mode and/or in proactive mode, if available. Read more about detective and proactive modes here. If you are running a rule in both detective mode and proactive mode, you will be charged for only the evaluations in detective mode. Prices are as follows.

AND

AWS Config rules evaluations	Price
First 100,000 rule evaluations	$0.001 per rule evaluation per region
Next 400,000 rule evaluations (100,001-500,000)	$0.0008 per rule evaluation per region
500,001 and more rule evaluations	$0.0005 per rule evaluation per region

Conformance packs

You are charged per conformance pack evaluation in your AWS account per AWS Region based on the tier below. A conformance pack evaluation is defined as an evaluation of a resource by an AWS Config rule within the conformance pack. The following prices are effective as of September 14, 2022 and will be automatically reflected in your AWS bill.

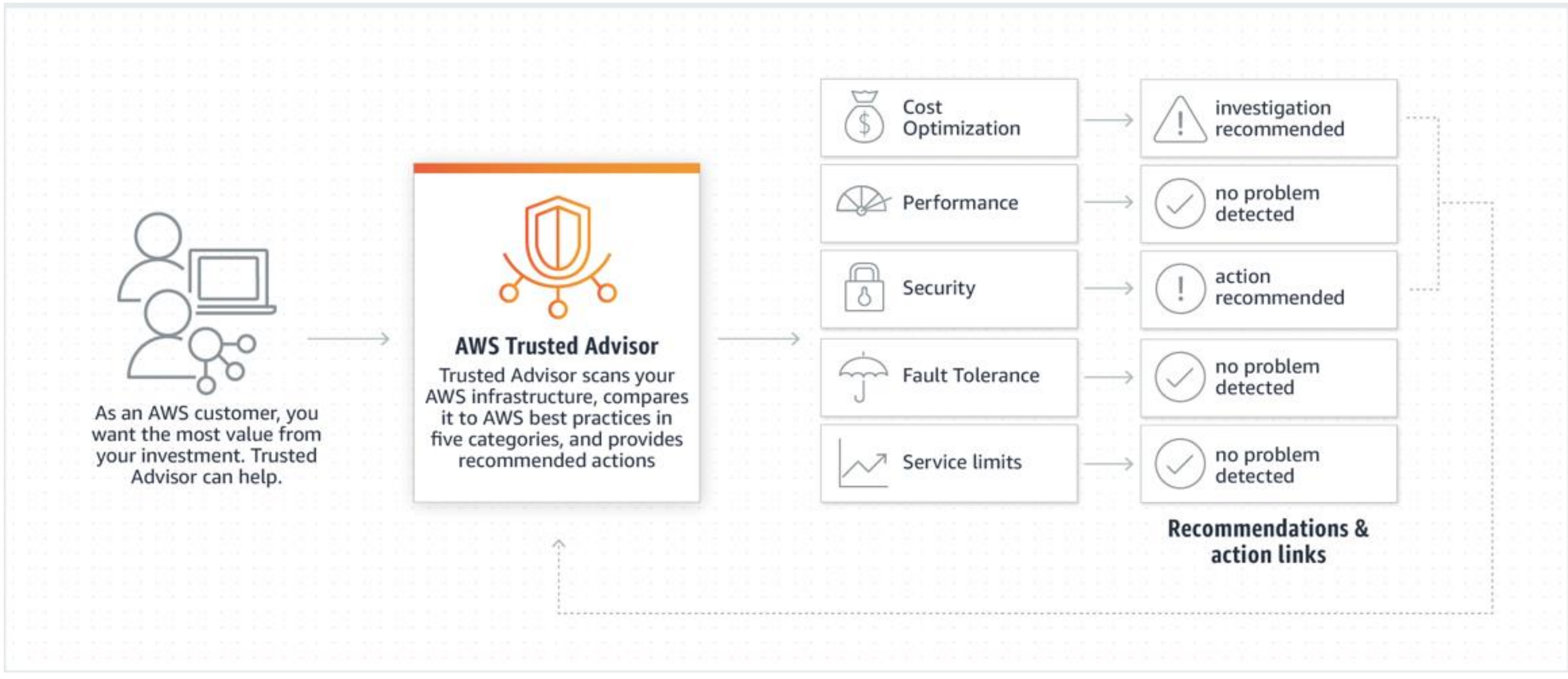
Conformance pack evaluations	Price
First 100,000 conformance pack evaluations	$0.001 per conformance pack evaluation per Region
Next 400,000 conformance pack evaluations (100,001-500,000)	$0.0008 per conformance pack evaluation per Region
500,001 and more conformance pack evaluations	$0.0005 per conformance pack evaluation per Region

Taken from https://aws.amazon.com/config/pricing/ (24/06/2021)

With consolidated billing, AWS will measure the total number of AWS Config conformance pack evaluations from all of your accounts to determine which pricing tier applies, giving you a lower overall price at the higher tiers.

AWS Trusted Advisor

The main function of AWS Trusted Advisor is to recommend improvements across your AWS account to help optimize your environment based on AWS best practices.



Taken from https://aws.amazon.com/premiumsupport/technology/trusted-advisor/ (24/06/2021)

Example and View

- **Dashboard**
  - Cost Optimization
  - Performance
  - Security
  - Fault Tolerance
  - Service Limits
- Preferences

Trusted Advisor Dashboard

Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
0 ✓ 0 ⚠ 0 !	0 ✓ 0 ⚠ 0 !	5 ✓ 1 ⚠ 0 !	0 ✓ 0 ⚠ 0 !	51 ✓ 0 ⚠ 0 !

Recommended Actions

⚠ **Amazon S3 Bucket Permissions** *Refreshed: 9 minutes ago*

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions or allow access to any authenticated AWS user. Bucket permissions that grant List access can result in higher than expected charges if objects in the bucket are listed by unintended users at a high frequency. Bucket permissions that grant Upload/Delete access create potential security vulnerabilities by allowing users that to add, modify, or remove items in a bucket.

Alert Criteria
Yellow: The bucket ACL allows List access for "Everyone" or "Any Authenticated AWS User".
Yellow: A bucket policy allows any kind of open access.
Yellow: Bucket policy has statements that grant public access. The "Block public and cross-account access to buckets that have public policies" setting is turned on and has restricted access to only authorized users of that account until public statements are removed.
Yellow: Trusted Advisor does not have permission to check the policy, or the policy could not be evaluated for other reasons.
Red: The bucket ACL allows Upload/Delete access for "Everyone" or "Any Authenticated AWS User".

Recommended Action
If a bucket allows open access, determine if open access is truly needed. If not, update the bucket permissions to restrict access to the owner or specific users. Use Amazon S3 Block Public Access to control the settings that allow public access to your data. See Setting Bucket and Object Access Permissions.

Additional Resources
Managing Access Permissions to Your Amazon S3 Resources

2 of 3 buckets have permission properties that grant global access.

Exclude & Refresh | Item View: Included items | Columns View: Columns Display

1 to 3 of 3 | View: 20

Region Name	Region API Parameter	Bucket Name	ACL Allows List	ACL Allows Upload/_	Policy Allows Access
us-east-1	us-east-1	ds4a-team54	Yes	No	Yes

	Developer	Business	Enterprise
	Recommended if you are experimenting or testing in AWS.	*Recommended if you have production workloads in AWS.*	*Recommended if you have business and/or mission critical workloads in AWS.*
AWS Trusted Advisor Best Practice Checks	7 Core checks	Full set of checks	Full set of checks

Taken from https://aws.amazon.com/premiumsupport/plans/?nc1=h_ls (24/06/2021)

Cloudwatch Logs

/aws/lambda/cwiDemo

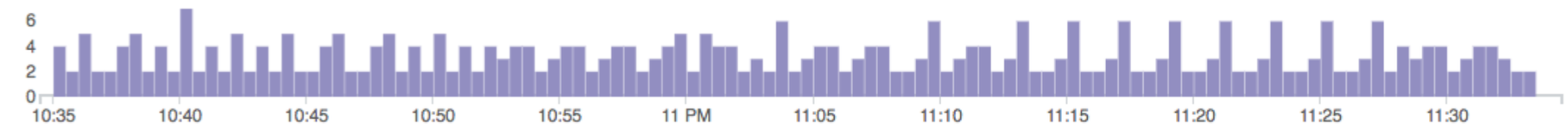
15m 30m 1h 6h 12h 1d custom

```
filter @type="REPORT"
| fields @timestamp, @message
```

Run query | Actions | Sample queries | Have feedback? Email us.

Logs | Visualization

Distribution of log events over time



25 records matched | 128,780 records (56.3 MB) scanned in 2.9s @ 44,057 records/s (19.2 MB/s)

#	@timestamp	@message
1	2019-06-06T23:39:57.240-05:00	REPORT RequestId: 1dcac8bf-cdea-4102-a26a-5f966f5aaee3 Duration: 156.83 ms Bil
2	2019-06-06T23:39:41.660-05:00	REPORT RequestId: cda0b260-e6d1-468e-b3f4-ad682105de37 Duration: 265.90 ms Bil
3	2019-06-06T23:39:40.899-05:00	REPORT RequestId: 7bef5c91-9dc9-45a8-a103-f6d5177851e5 Duration: 177.54 ms Bil
4	2019-06-06T23:39:40.040-05:00	REPORT RequestId: 5a6e120c-7507-4831-8ca2-b2b4591b8335 Duration: 164.99 ms Bil
5	2019-06-06T23:39:39.360-05:00	REPORT RequestId: b3f1ee2e-6c52-4a4b-bea4-b890d3353113 Duration: 175.82 ms Bil
6	2019-06-06T23:39:38.699-05:00	REPORT RequestId: 06f83ea8-154b-48a6-8d94-14d2e2b2c83c Duration: 160.86 ms Bil
7	2019-06-06T23:39:37.959-05:00	REPORT RequestId: 7a8baf4f-5f62-4629-9e3e-980fcf26efd6 Duration: 155.49 ms Bil
8	2019-06-06T23:39:37.240-05:00	REPORT RequestId: 7d212ccf-14ac-4920-bae4-c054e9882051 Duration: 197.19 ms Bil
9	2019-06-06T23:39:36.520-05:00	REPORT RequestId: 0b67a7c8-f102-4c63-9e67-e9e223c2a32c Duration: 179.91 ms Bil
10	2019-06-06T23:39:35.819-05:00	REPORT RequestId: 834cc50d-9d6a-42fb-8b95-9e4393b0edd8 Duration: 152.20 ms Bil
11	2019-06-06T23:39:34.999-05:00	REPORT RequestId: 100b21c7-4ee2-4443-8129-26e298cab311 Duration: 163.53 ms Bil
12	2019-06-06T23:39:34.219-05:00	REPORT RequestId: 2a9a7533-152b-4a1b-9063-84a4a01079a7 Duration: 221.69 ms Bil

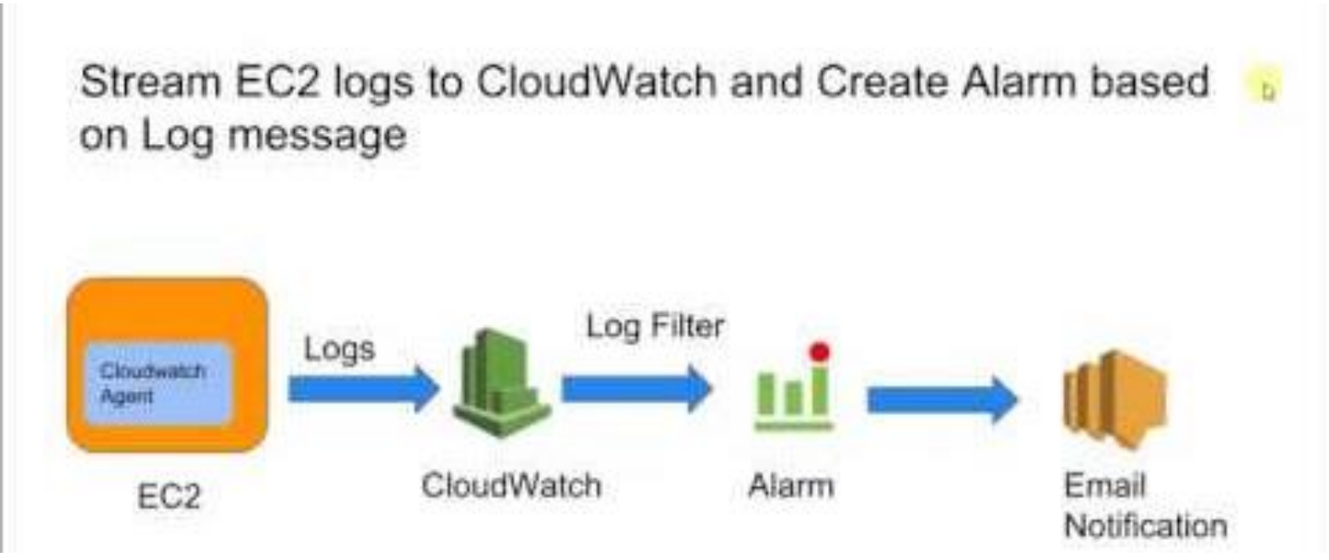
Query help Learn more

Commands
- fields
- filter
- stats
- sort
- limit
- parse

Discovered fields

Search for a field

@ingestionTime	100%
@logStream	100%
@message	100%
@requestId	100%
@timestamp	100%



2. Execute the following queries:

```
filter @type="REPORT"
| stats avg(@billedDuration) as mean_billed_duration,
min(@billedDuration) as min_billed_duration,
max(@billedDuration) as max_billed_duration,
percentile(@billedDuration, 95) as Percentile95
filter @type="REPORT"
| stats avg(@maxMemoryUsed/1024/1024) as mean_MemoryUsed,
min(@maxMemoryUsed/1024/1024) as min_MemoryUsed,
max(@maxMemoryUsed/1024/1024) as max_MemoryUsed,
percentile(@maxMemoryUsed/1024/1024, 95) as Percentile95
```

The executed queries perform the following:

- Filter out the "REPORT" logs.
- Select a key field (@duration, @billedDuration, or @maxMemoryUsed).
- Get the statistics, such as average, minimum, maximum, and percentile.

This results in the following output:

#	mean_billed_duration	min_billed_duration	max_billed_duration	Percentile95
1	30	38	46	54

#	mean_MemoryUsed	min_MemoryUsed	max_MemoryUsed	Percentile95
1	33.7255	30.5176	69.6182	33.3786

3. To gather understand

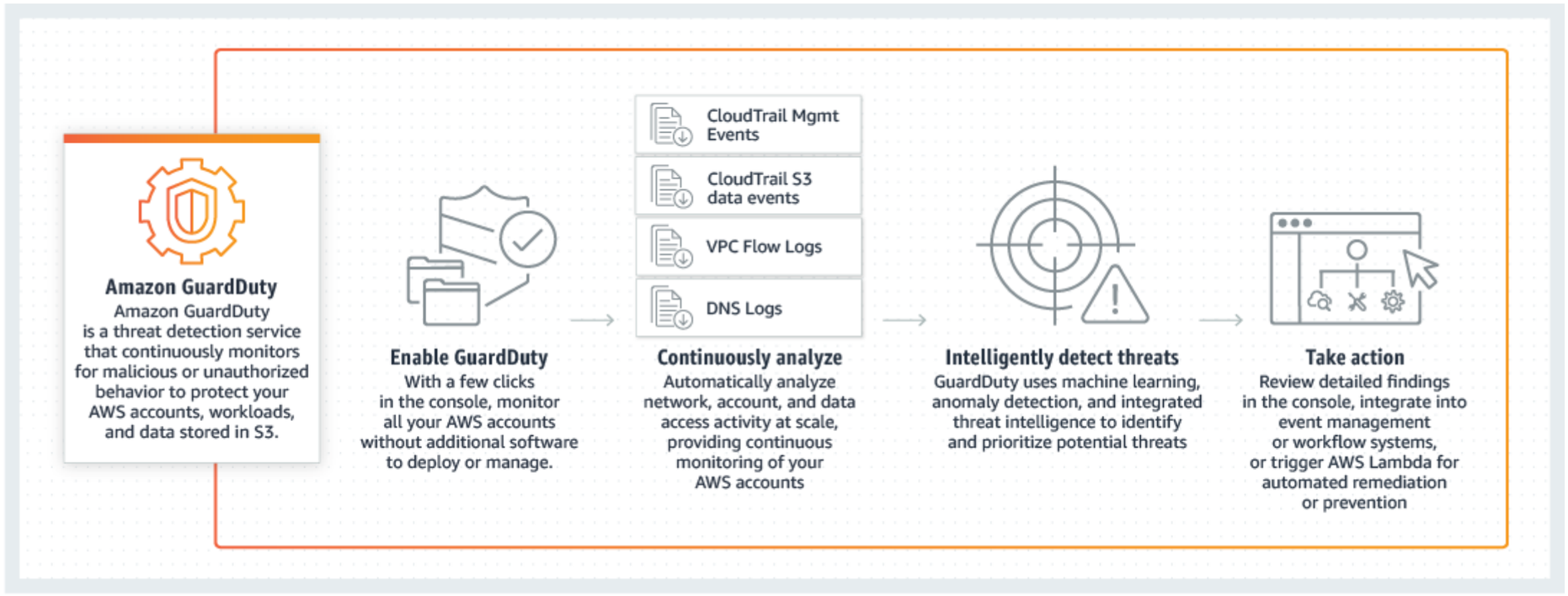
Taken from https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html and https://aws.amazon.com/blogs/mt/understanding-aws-lambda-behavior-using-amazon-cloudwatch-logs-insights/ (24/06/2021)

Amazon GuardDuty

Threat detection

Continually monitors across data sources

- AWS CloudTrail
- Amazon VPC Flow Logs
- DNS Logs



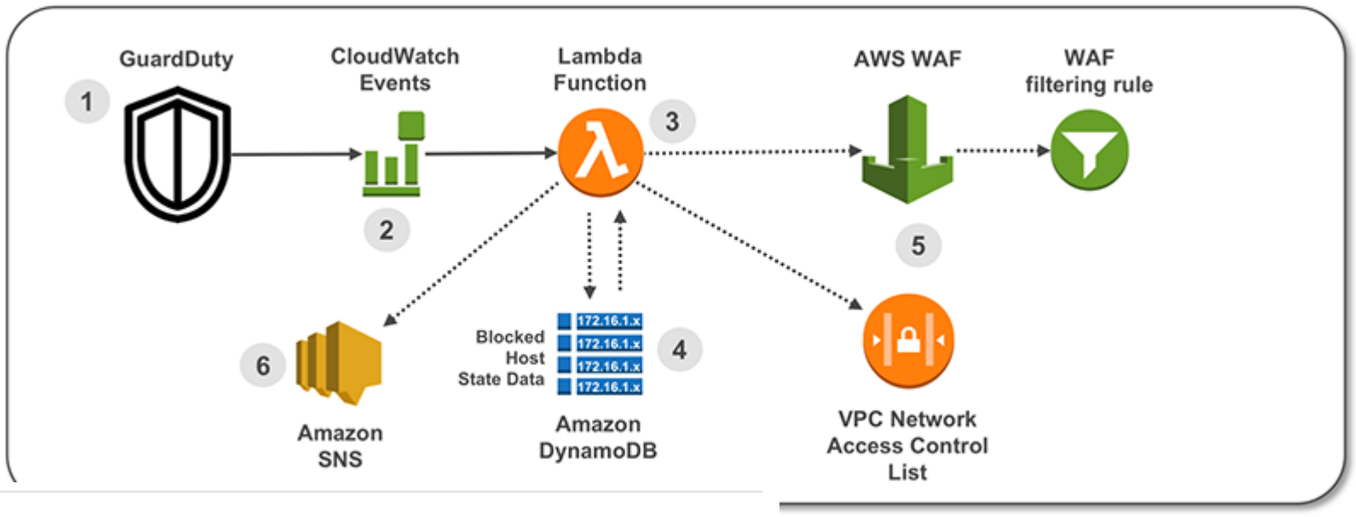
Thread Protection:
- Reconnaissance
- Instance compromise
- Account compromise
- Bucket compromise
- Etc.

Prioritization Levels.

Remediation (Integration)

Taken from https://aws.amazon.com/guardduty/getting-started/ and https://aws.amazon.com/guardduty/features/ (24/06/2021)

Use Case and Pricing



Trial for 30 days on New Accounts.

Region: US East (Ohio)

AWS CloudTrail Management Event Analysis
Per one million events / month

VPC Flow Log and DNS Query Log Analysis
First 500 GB / month
Next 2,000 GB / month
Next 7,500 GB / month
Over 10,000 GB / month

Pricing examples

CloudTrail management event analysis

In your environment, in one month, GuardDuty processes 40,000,000 CloudTrail management events in the US East (N. Virginia) Region.

Total charges:

40 management events * $4.00 (40 million management events, priced per million)

Total = $160 per month

Show less

VPC Flow Log and DNS query log analysis

In your environment, in one month, GuardDuty processes 2,000 GB of VPC Flow Logs and 1,000 GB of DNS query logs, for a total volume of 3,000 GB of logs.

Total charges:

500 GB logs * $1.00 (first 500 GB)
+ 2,000 GB logs * $0.50 (next 2,000 GB)
+ 500 GB logs * $0.25 (last 500 GB)

Total = $1,625 per month

Show less

Taken from https://aws.amazon.com/blogs/security/how-to-use-amazon-guardduty-and-aws-web-application-firewall-to-automatically-block-suspicious-hosts/ and https://aws.amazon.com/guardduty/pricing/ (06/08/2024)

Amazon Inspector

Amazon Inspector

Service of security assessment on 2 areas : Network accessibility and security state of EC2 Instance. An Agent is optional.

Benefits:

- Integrate automated security checks into your regular deployment and production processes. It can work to automate security vulnerability assessment on CI/CD Pipelines.-
- Find application security issues
- Gain a deeper understanding of your AWS resources

Key Terms:

- Amazon Inspector agent
- Assessment run
- Assessment target
- Rule
- Rules package (Common Vulnerabilities and Exposures (CVE), Center for Internet Security (CIS) benchmarks, Security Best Practices, and Runtime Behavior Analysis)
- Assessment template (Rules package, SNS topics, Duration)
- Findings (Exposure, Vulnerabilities and Deviations from Best Practices. All with level of security and mostly with remediations).
- Telemetry (Information and SW cfg)

Check OS (Linux and Windows) and Region.

Taken from https://www.clearscale.com/blog/improving-security-amazon-inspector/ and https://docs.aws.amazon.com/inspector/latest/userguide/inspector_findings.html (06/08/2024).
New version for Inspector, https://docs.aws.amazon.com/inspector/v1/userguide/inspector-migration.html (06/08/2024)

AWS Inspector Overview

Native AWS support for DevSecOps

Findings reports

Static and Dynamic Rule Packages. Continuously Improving.

The Ability to Trigger SNS Topics and Lambda

Host and Network Assessments

On-Demand Pricing Model

Rules packages:

Network Reachability (Agentless)

Common Vulnerabilities and Exposures

CIS Benchmarks

Security Best Practices as defined by AWS Inspector

Runtime Behaviour Analysis

Complete Automation Through APIs

Cross account scans through service-linked roles

Taken from https://faun.pub/shifting-security-to-the-left-ci-cd-and-aws-inspector-97463f13f837 (24/06/2021)