

CloudTrail – Criação de uma trilha de auditoria

1) Acesse o serviço CloudTrail

Management & Governance

AWS CloudTrail

Continuously log your AWS account activity


Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.

Create a trail with AWS CloudTrail

Get started with AWS CloudTrail by creating a trail to log your AWS account activity.

[Create a trail](#)

How it works



Pricing [↗](#)

[Pricing](#)

Getting started [↗](#)

[What is AWS CloudTrail?](#)

2) Navegue até o menu de Trilhas. Clique em “Create Trail” para criar uma trilha nova

CloudTrail ×

Dashboard
Event history
Insights
Lake [New](#)
Trails

CloudTrail > Trails

Trails


[↻](#) [Delete](#) [Create trail](#) [⚙](#)

Name ▲	Home region ▼	Multi-region trail ▼	Insights ▼	Organization trail ▼	S3 bucket ▼	Log file prefix ▼	CloudWatch Logs log group ▼	Status ▼
--------	---------------	----------------------	------------	----------------------	-------------	-------------------	-----------------------------	----------

3) Insira um nome para a sua trilha de auditoria e um nome para o seu bucket.

Choose trail attributes

General details

A trail created in the console is a multi-region trail. [Learn more](#) 

Trail name

Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ Enable for all accounts in my organization

To review accounts in your organization, open AWS Organizations. [See all accounts](#) 

Storage location [Info](#)



Create new S3 bucket

Create a bucket to store logs for the trail.



Use existing S3 bucket

Choose an existing bucket to store logs for this trail.

Trail log bucket and folder

Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in aws-cloudtrail-logs-730471154539-9a07388c/AWSLogs/730471154539

Log file SSE-KMS encryption [Info](#)



Enabled

4) Configure a trilha para auditar somente eventos de gerenciamento

5) Aguarde alguns minutos e verifique os eventos registrados. O que eles indicam? Para que podem ser usados?

Choose log events

Events [Info](#)

Record API activity for individual resources, or for all current and future resources in AWS account. [Additional charges apply](#) [↗](#)

Event type

Choose the type of events that you want to log.

☒ **Management events**

Capture management operations performed on your AWS resources.

☒ **Data events**

Log the resource operations performed on or within a resource.

☐ **Insights events**

Identify unusual activity, errors, or user behavior in your account.

Management events [Info](#)

Management events show information about management operations performed on resources in your AWS account.

[i](#) Charges apply to log management events on this trail because you are logging at least one other copy of management events in your account.

API activity

Choose the activities you want to log.

☒ **Read**

☒ **Write**

☐ **Exclude AWS KMS events**

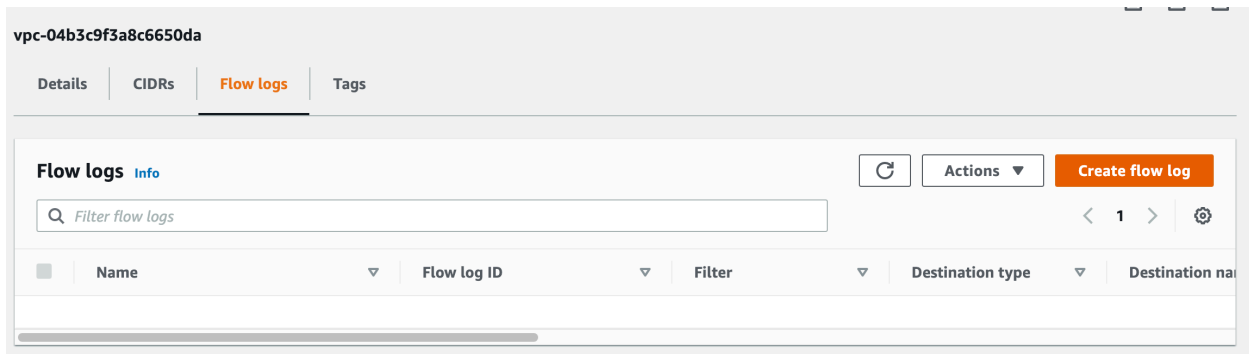
VPC Flowlogs: Criação de um flowlog de VPC

1) Acesse o serviço VPC

The screenshot shows the AWS Management Console interface for the VPC service. The top navigation bar includes the AWS logo, a search bar, and the region 'N. Virginia'. The left sidebar contains the navigation menu, with 'VIRTUAL PRIVATE CLOUD' expanded and 'Your VPCs' selected. The main content area is titled 'Your VPCs (1)' and includes a search bar and a table of VPCs. The table has columns for Name, VPC ID, State, IPv4 CIDR, and IPv6 CIDR. One VPC is listed: vpc-04b3c9f3a8c6650da, which is in the 'Available' state with an IPv4 CIDR of 172.31.0.0/16. The 'Actions' button is visible in the top right corner.

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-04b3c9f3a8c6650da	Available	172.31.0.0/16	-

2) Identifique uma VPC e navegue até “Flow Logs”



2) Durante o processo de criação, capture todo o tráfego, agregue no menor intervalo possível e armazene no CloudWatch.

Create flow log [Info](#)

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

Selected resources Info		
Name	Resource ID	State
	vpc-04b3c9f3a8c6650da	✓ Available

Flow log settings

Name - *optional*

Filter

The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

- ☐ Accept
- ☐ Reject
- ☒ All

Maximum aggregation interval [Info](#)

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

- ☒ 10 minutes
- ☐ 1 minute

Destination

The destination to which to publish the flow log data.

- ☒ Send to CloudWatch Logs
- ☐ Send to an Amazon S3 bucket

- ☒ Send to CloudWatch Logs
- ☐ Send to an Amazon S3 bucket

Destination log group [Info](#)

The name of the Amazon CloudWatch log group to which the flow log is published. A new log stream is created for each monitored network interface.



IAM role [Info](#)

The IAM role that has permission to publish to the Amazon CloudWatch log group. [Set up permissions](#)



Log record format

Specify the fields to include in the flow log record.

- ☒ AWS default format
- ☐ Custom format

Format preview

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

Copy

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Remove

Add new tag

You can add 49 more tags.

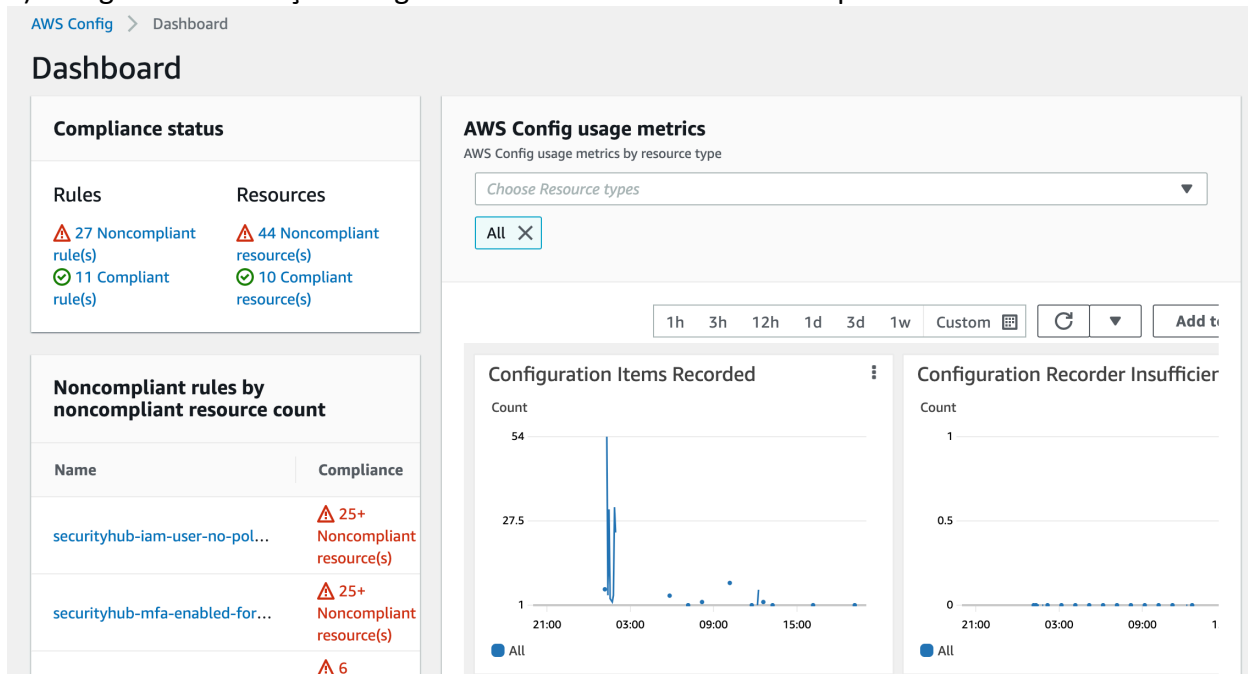
Cancel

Create flow log

3)Aguarde alguns minutos e verifique o CloudWatch para visualizar os logs. Que tipo de análise pode ser feita?

AWS Config: Identificando recursos mal configurados

1) Navegue até o serviço Config. Observe o Dashboard e identifique os dados exibidos



2) Acesse o menu “Rules”. Observe as regras gerenciadas e customizadas

AWS Config > Rules

Rules

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

Rules View details Edit rule Actions ▼ Add rule

Any status ▼

< 1 2 3 ... > [gear icon]

	Name	Remediation action	Type	Compliance
●	securityhub-api-gw-cache-encrypted-c0d3277a	Not set	Custom Lambda	-
●	securityhub-beanstalk-enhanced-health-reporting-enabled-21e935a8	Not set	AWS managed	-
●	securityhub-cloud-trail-log-file-validation-enabled-57bd240c	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)
●	securityhub-cloud-trail-encryption-enabled-f0977b0c	Not set	AWS managed	⚠️ 1 Noncompliant resource(s)

3) Agora acesse o menu “Resource”, observe os recursos listados. Busque o recurso VPC

Resource Inventory

Search existing or deleted resources recorded by AWS Config. For a specific resource, view the resource details, configuration timeline, or compliance timeline. The resource configuration timeline allows you to view all the configuration items captured over time for a specific resource. The resource compliance timeline allows you to view compliance status changes. To query your resource configurations, use the [advanced SQL query editor](#).

Resources (51) [View details](#) [Resource Timeline](#)

Resource category
All resource categories ▼

Resource type
All resource types ▼

Compliance
Any compliance status ▼

Resource identifier - optional

☐ Include deleted resources

< 1 ... 5 6 7 8 9 10 ... >

⚙

Resource identifier	Type	Compliance
<input type="radio"/> AWS::IAM::User/AIDA2UE3ZI...	Config ResourceCompliance	-
<input type="radio"/> acl-Of4697289d4aab9e7	EC2 NetworkAcl	-
<input type="radio"/> eni-003fcf8abcf7c7313	EC2 NetworkInterface	-

4)Dentro do recurso, identifique as alterações por meio do Resource Timeline. Como é possível identificar recursos que não estão configurados corretamente?

Timeline

General details

Resource ID
vpc-04b3c9f3a8c6650da

Resource type
AWS::EC2::VPC

Resource name
-

Events
All times are in America/Sao_Paulo (UTC-03:00)

Start date
2022/05/05

Now

Event type
All event types ▼

May 5, 2022

09:18:07

Configuration change

1 field change(s)

07:14:08

Configuration change

4 field change(s)

GuardDuty: Identificação de Ameaças

1) Acesse o serviço GuardDuty. Observe o dashboard.

2) Navegue pelos findings, o que é possível detectar? Consegue identificar os diferentes tipos de findings?

Finding type	Resource	L.	C...
[SAMPLE] Impact:Kubernetes/Torl...	EKSCluster: GeneratedFinding	2 min...	1
[SAMPLE] InitialAccess:IAMUser/An...	GeneratedFindingUserName:	2 min...	1
[SAMPLE] DefenseEvasion:IAMUser...	GeneratedFindingUserName:	2 min...	1
[SAMPLE] UnauthorizedAccess:IAM...	GeneratedFindingAWSService	2 min...	1
[SAMPLE] Exfiltration:IAMUser/Ano...	GeneratedFindingUserName:	2 min...	1
[SAMPLE] Behavior:EC2/NetworkP...	Instance: i-999999999	2 min...	1
[SAMPLE] DefenseEvasion:Kuberne...	EKSCluster: GeneratedFinding	2 min...	1
[SAMPLE] CredentialAccess:Kubern...	EKSCluster: GeneratedFinding	2 min...	1

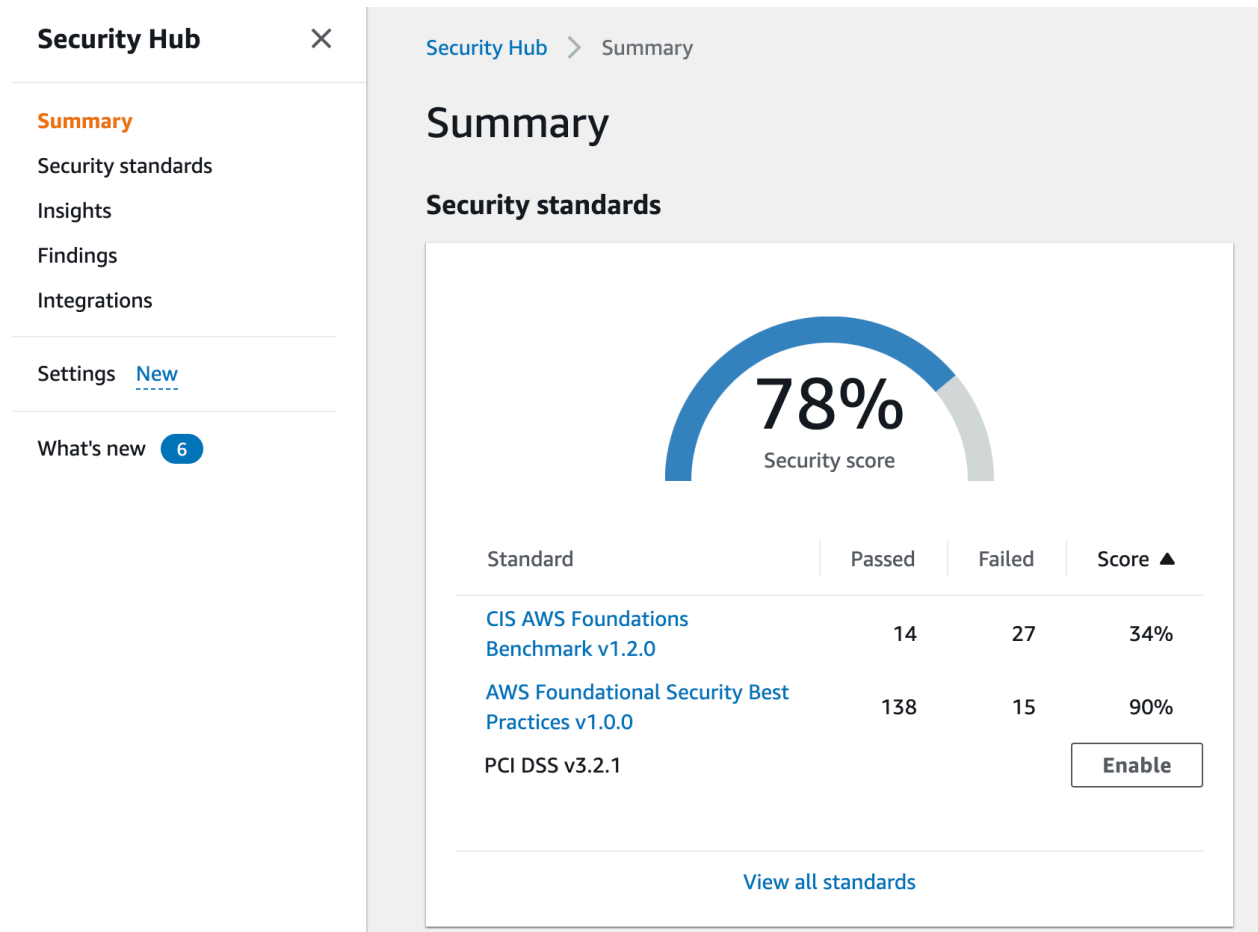
Overview		
Severity	HIGH	🔍
Region	us-east-1	
Count	1	
Account ID	730471154539	🔍
Resource ID	i-999999999	
Created at	05-05-2022 17:09:54 (2 mi...	
Updated at	05-05-2022 17:09:54 (2 mi...	

Anomalous APIs (4)	Usual APIs
Successfully called	

3) Na sua visão, em quais cenários o GuardDuty pode ajudar?

SecurityHub: Centralizar findings e priorizar tarefas

1) Acesse o serviço SecurityHub. O que pode ser observado no dashboard?



2) Acesse os padrões de segurança. Se você precisasse explicar o conceito dos padrões de segurança para o seu gerente, como explicaria?

Security standards

AWS Foundational Security Best Practices v1.0.0 by AWS

Description

The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score



Disable

View results

CIS AWS Foundations Benchmark v1.2.0 by AWS

Description

The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score



Disable

View results

AWS Foundational Security Best Practices v1.0.0

Overview

Last updated 9 hours ago

Security score



53 of 231 checks failed



23% failed

All enabled	Failed	Unknown	No data	Passed	Disabled
153	15	0	0	138	0

All enabled controls (153)

statuses and check counts updated 9 hours ago

Download

Filter enabled controls

Compliance Status	Severity	ID	Title	Failed checks
-------------------	----------	----	-------	---------------

Compliance Status ▾	Severity ▾	ID ▾	Title ▾	Failed checks ▾
⊗ Failed	■ Critical	IAM.6	Hardware MFA should be enabled for the root user	1 of 1
⊗ Failed	■ High	EC2.9	EC2 instances should not have a public IPv4 address	3 of 3
⊗ Failed	■ High	EC2.8	EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)	2 of 3
⊗ Failed	■ High	CloudTrail.1	CloudTrail should be enabled and configured with at least one multi-Region trail that includes read and write management events	1 of 1
⊗ Failed	■ Medium	EC2.15	EC2 subnets should not automatically assign public IP addresses	6 of 6
⊗ Failed	■ Medium	SSM.1	EC2 instances should be managed by AWS Systems Manager	2 of 2
⊗ Failed	■ Medium	Config.1	AWS Config should be enabled	1 of 1
⊗ Failed	■ Medium	EC2.10	Amazon EC2 should be configured to use VPC endpoints that are created for the Amazon EC2 service	1 of 1
⊗ Failed	■ Medium	EC2.22	Unused EC2 security groups should be removed	1 of 1
⊗ Failed	■ Medium	EC2.7	EBS default encryption should be enabled	1 of 1
⊗ Failed	■ Medium	IAM.7	Password policies for IAM users should have strong configurations	1 of 1
⊗ Failed	■ Medium	S3.1	S3 Block Public Access setting should be enabled	1 of 1