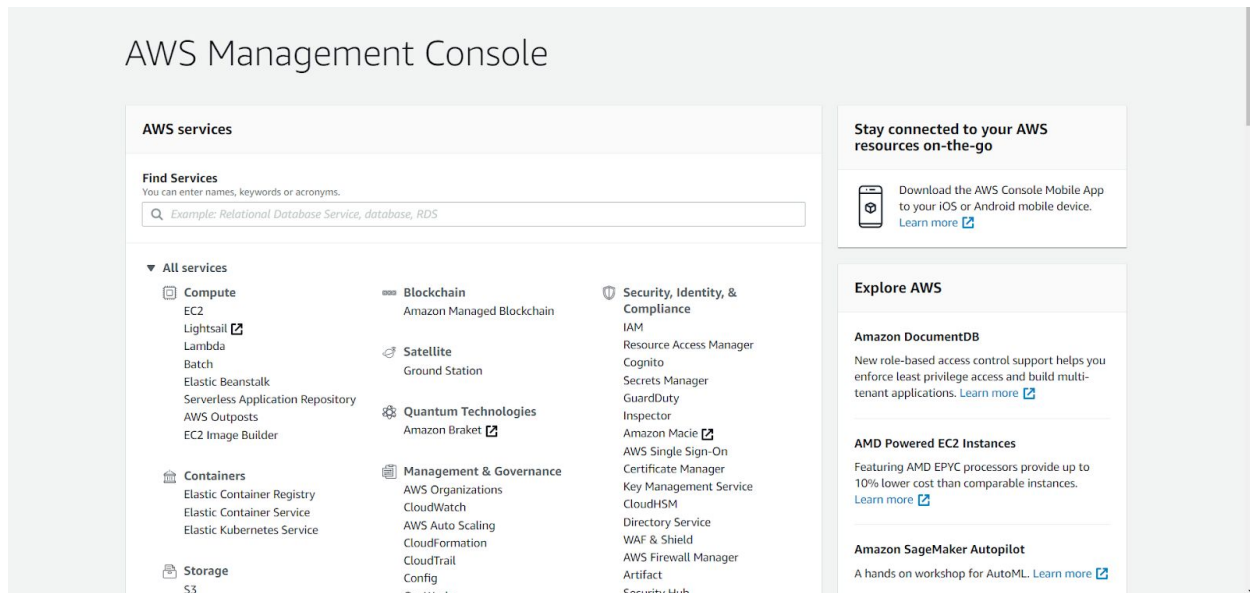
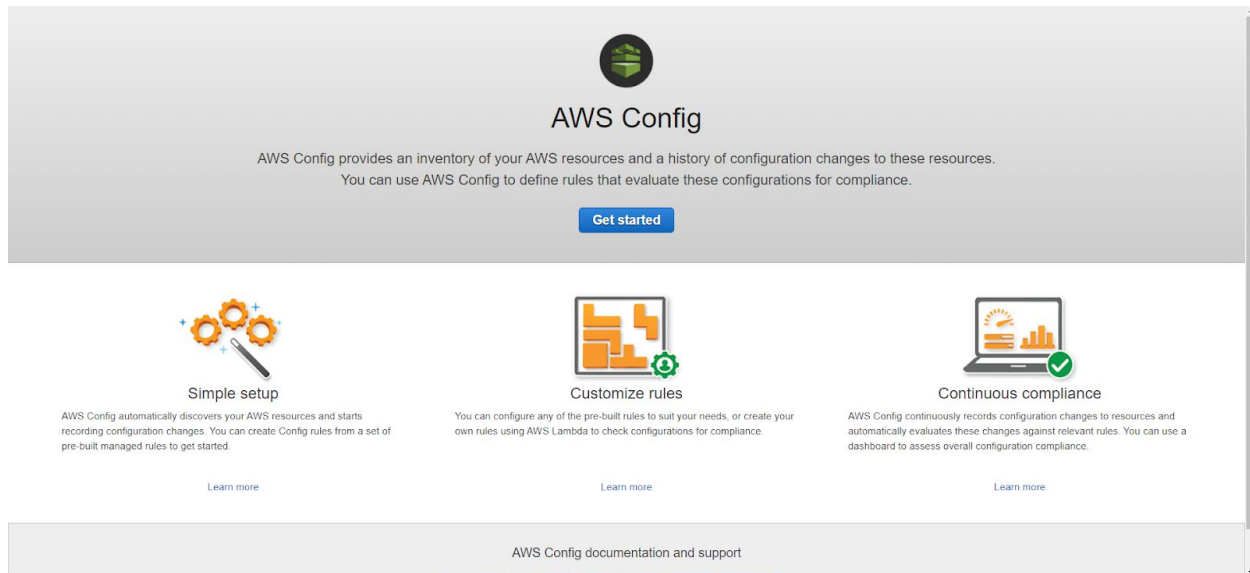


Module 2 Lab: AWS Config & S3 Rule

AWS Management Console

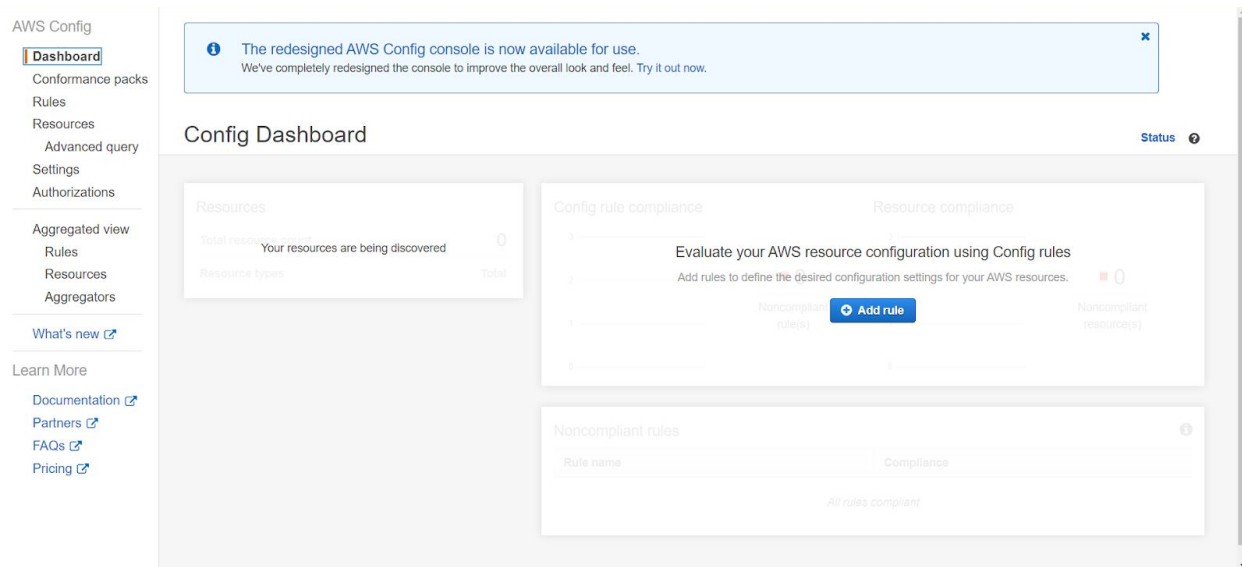


Starting from the AWS Management Console, select AWS Config



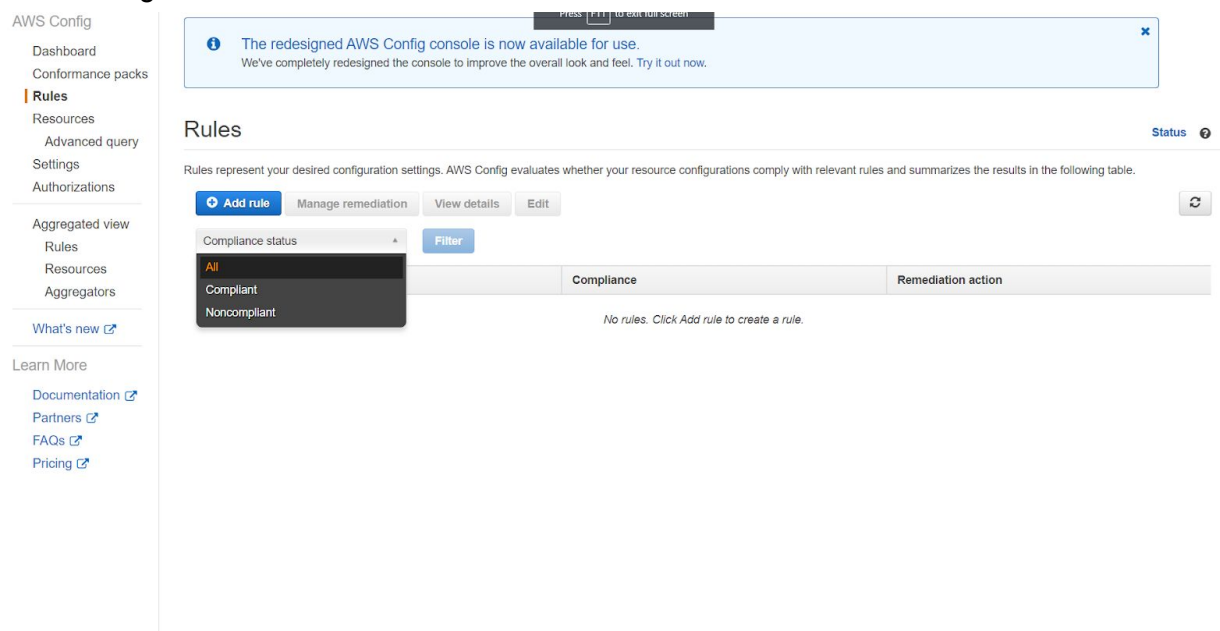
Since this is the first time starting AWS Config, this welcome screen is displayed.

Config Dashboard



After selecting the S3 bucket (cali818), enabling SNS, and creating a service role for config, the Config Dashboard is activated.

AWS Config - Rules



During the setup step for AWS Config, no Rules were set in place. This can be done after AWS Config is activated.

AWS Config - Add Rule

AWS Config

Rules > Add rule

The redesigned AWS Config console is now available for use. We've completely redesigned the console to improve the overall look and feel. Try it out now.

Add rule

Add rules to define the desired configuration settings of your AWS resources. Customize any of the following rules to suit your needs, or add a custom rule. To add a custom rule, you must create an AWS Lambda function for the rule.

[Add custom rule](#)

Filter by rule name, label or description

« < Viewing 1 - 9 of 119 AWS managed rules > »

access-keys-rotated Checks whether the active access keys are rotated within the number of days specified in <code>maxAccessKeyAge</code> . The rule is non-compliant if the access keys have not been rotated for IAM - Periodic	acm-certificate-expiration-check Checks whether ACM Certificates in your account are marked for expiration within the specified number of days. Certificates provided by ACM are automatically renewed. ACM	alb-http-to-https-redirection-check Checks whether HTTP to HTTPS redirection is configured on all HTTP listeners of Application Load Balancers. The rule is NON_COMPLIANT if one or more HTTP EC2 - ELB
api-gw-cache-enabled-and-encrypted Checks that all methods in Amazon API Gateway stages have cache enabled and cache encrypted. The rule is NON_COMPLIANT if any method in Amazon API Gateway - REST API	api-gw-endpoint-type-check Checks that Amazon API Gateway APIs are of type as specified in the rule parameter 'endpointConfigurationTypes'. The rule returns COMPLIANT if any of the RestApi endpoint API Gateway - REST API	api-gw-execution-logging-enabled Checks that all methods in Amazon API Gateway stage has logging enabled. The rule is NON_COMPLIANT if logging is not enabled. The rule is NON_COMPLIANT if API Gateway - Logging

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

The following 119 AWS managed rules are available for monitoring.

Add AWS managed rule

AWS Config

Rules > Configure rule

Add AWS managed rule

AWS Config evaluates your AWS resources against this rule when it is triggered.

Name* s3-bucket-public-read-prohibited
A unique name for the rule. 128 characters max. No special characters or spaces.

Description Checks that your S3 buckets do not allow public read access. If an S3 bucket policy or bucket ACL allows public read access, the bucket is noncompliant.

Managed rule name S3_BUCKET_PUBLIC_READ_PROHIBITED

Trigger
AWS Config evaluates resources when the trigger occurs.

Trigger type* ☒ Configuration changes ☒ Periodic

Scope of changes* ☒ Resources ☐ Tags ☐ All changes

Resources* S3 Bucket
Resource identifier (optional)
This rule can be triggered only when recorded resources are created, changed, or deleted. Specify which resources are recorded on the Settings page.

Frequency* 24 hours

Choose remediation action
The execution of remediation actions is achieved using AWS Systems Manager Automation. Choose from a set of AWS recommended remediation actions or custom remediation actions. To remediate a rule choose all the noncompliant resources in scope from table.

Remediation action Remediation action

Auto remediation ☐ Yes ☒ No

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

The purpose of this rule is to deny public Read access to the S3 bucket.

AWS Config - Rules

The screenshot shows the AWS Config 'Rules' page. The left sidebar contains navigation links for Dashboard, Conformance packs, Rules (selected), Resources, Advanced query, Settings, Authorizations, Aggregated view, and What's new. The main content area is titled 'Rules' and includes a status indicator. Below the title, a message states: '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.' There are buttons for 'Add rule', 'Manage remediation', 'View details', and 'Edit'. A 'Compliance status' filter dropdown and a 'Filter' button are also present. The table below has three columns: 'Rule name', 'Compliance', and 'Remediation action'. The first row shows the rule 's3-bucket-public-read-prohibited' with a compliance status of 'Evaluating...' and a remediation action of 'Not set'.

Rule name	Compliance	Remediation action
s3-bucket-public-read-prohibited	Evaluating...	Not set

The S3 buckets are being evaluated for compliance after saving the policy.

AWS Config - Rules

This screenshot shows the same AWS Config 'Rules' page as the previous one, but the rule 's3-bucket-public-read-prohibited' now has a compliance status of 'Compliant'. The 'Remediation action' remains 'Not set'. The interface elements, including the sidebar and top navigation, are identical to the previous screenshot.

Rule name	Compliance	Remediation action
s3-bucket-public-read-prohibited	Compliant	Not set

Because there are currently no public S3 buckets, the Rule returns with complaint.

AWS Config - Add Rule

The screenshot shows the AWS Config 'Add Rule' page. The left sidebar contains navigation links: Dashboard, Conformance packs, Rules (selected), Resources, Advanced query, Settings, Authorizations, Aggregated view, What's new, Learn More, Documentation, Partners, FAQs, and Pricing. The main content area is titled 'Rules > Add rule'. A notification banner at the top states: 'The redesigned AWS Config console is now available for use. We've completely redesigned the console to improve the overall look and feel. Try it out now.' Below this, the 'Add rule' section explains that rules define configuration settings for AWS resources. A button 'Add custom rule' is visible. A list of 28 AWS managed rules is displayed, with 'ec2' selected. The details for the 'ec2-security-group-attached-to-eni' rule are shown, including its description and the VPC Security Group resource. Other rules shown include 'ec2-stopped-instance', 'ec2-volume-in-use-check', 'eip-attached', 'encrypted-volumes', 'required-tags', 'restricted-common-ports', 'restricted-ssh', and 'vpc-flow-logs-enabled'.

Because EC2 instances may require computers to connect to it, restricted SSH is good practice.

Add AWS managed rule

The screenshot shows the AWS Config 'Add AWS managed rule' page. The left sidebar contains navigation links: Dashboard, Conformance packs, Rules (selected), Resources, Advanced query, Settings, Authorizations, Aggregated view, What's new, Learn More, Documentation, Partners, FAQs, and Pricing. The main content area is titled 'Rules > Configure rule'. The 'Add AWS managed rule' section explains that AWS Config evaluates your AWS resources against this rule when it is triggered. The rule is titled 'restricted-ssh' and checks whether security groups that are in use disallow unrestricted incoming SSH traffic. The managed rule name is 'INCOMING_SSH_DISABLED'. The trigger is set to 'Configuration changes' and 'Periodic'. The scope of changes is set to 'Resources'. The resources are 'EC2:SecurityGroup'. The remediation action is 'Remediate action'. The auto remediation is set to 'No'. The rate limits are set to 'Concurrent Execution Rate' and 'Error Rate'. The resource ID parameter is 'id'.

A rule to check whether security groups that are in use disallow unrestricted incoming SSH traffic.

AWS Config - Rules

AWS Config

- Dashboard
- Conformance packs
- Rules**
- Resources
- Advanced query
- Settings
- Authorizations

Aggregated view

- Rules
- Resources
- Aggregators

What's new [?](#)

Learn More

- Documentation [?](#)
- Partners [?](#)
- FAQs [?](#)
- Pricing [?](#)

The redesigned AWS Config console is now available for use. We've completely redesigned the console to improve the overall look and feel. Try it out now.

Rules

Status [?](#)

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.

[Add rule](#) [Manage remediation](#) [View details](#) [Edit](#)

Compliance status [Filter](#)

Rule name	Compliance	Remediation action
<input type="radio"/> restricted-ssh	3 Noncompliant resource(s)	Not set
<input type="radio"/> s3-bucket-public-read-prohibited	Compliant	Not set

Feedback [English \(US\)](#)

© 2019 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

After enabling restricted-ssh, there are 3 noncompliant resources.

AWS Config - restricted-ssh

Aggregators

What's new [?](#)

Learn More

- Documentation [?](#)
- Partners [?](#)
- FAQs [?](#)
- Pricing [?](#)

Overall rule status: Last successful invocation on April 24, 2020 at 2:10:29 PM [?](#)
Last successful evaluation on April 24, 2020 at 2:18:29 PM [?](#)

Choose resources in scope

Resources in scope represent those resources where this rule is being applied to and their compliance status.

Compliance status: [Noncompliant](#)

[Remove exceptions](#) [Resource actions](#) [Remediate](#)

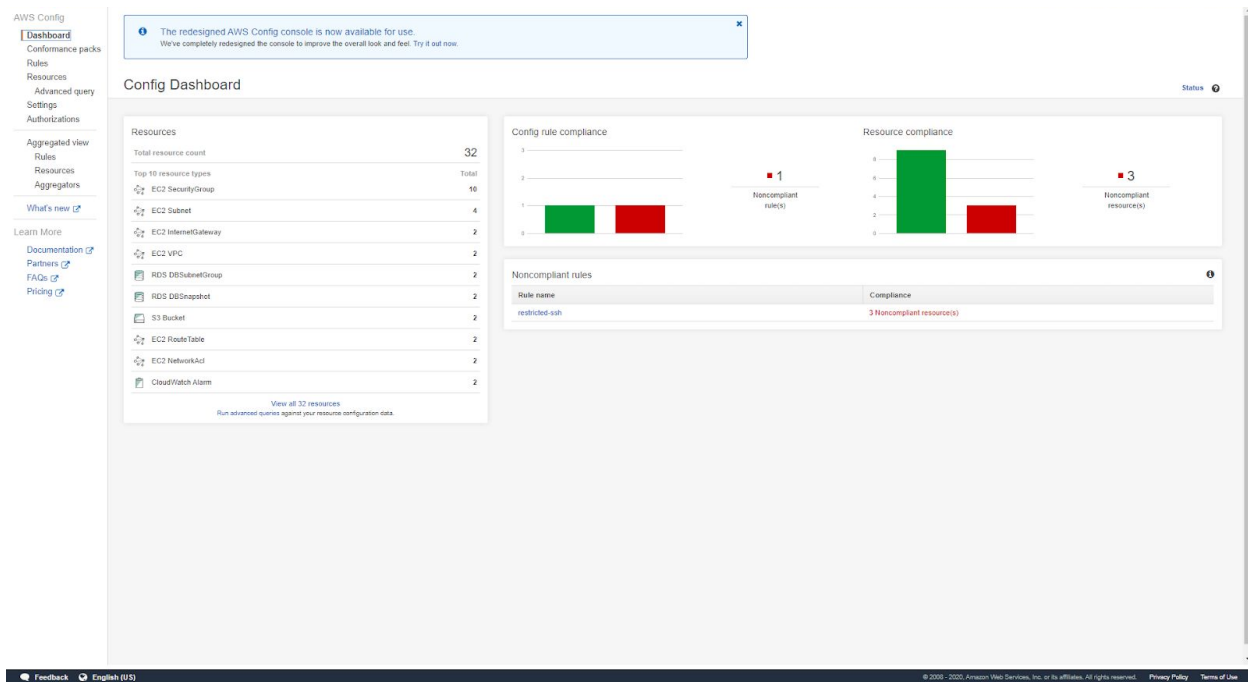
Resource ID	Resource type	Resource compliance status	Action status
<input type="checkbox"/> sg-42b5570cd710e967	EC2 SecurityGroup	Noncompliant	n/a
<input type="checkbox"/> sg-8d32a3c4a55a93164	EC2 SecurityGroup	Noncompliant	n/a
<input type="checkbox"/> sg-9a2b1219b6c4da91c	EC2 SecurityGroup	Noncompliant	n/a

Feedback [English \(US\)](#)

© 2019 - 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Each of the EC2 SecurityGroups are noncompliant.

AWS Config - Dashboard



All non compliant resources are listed.

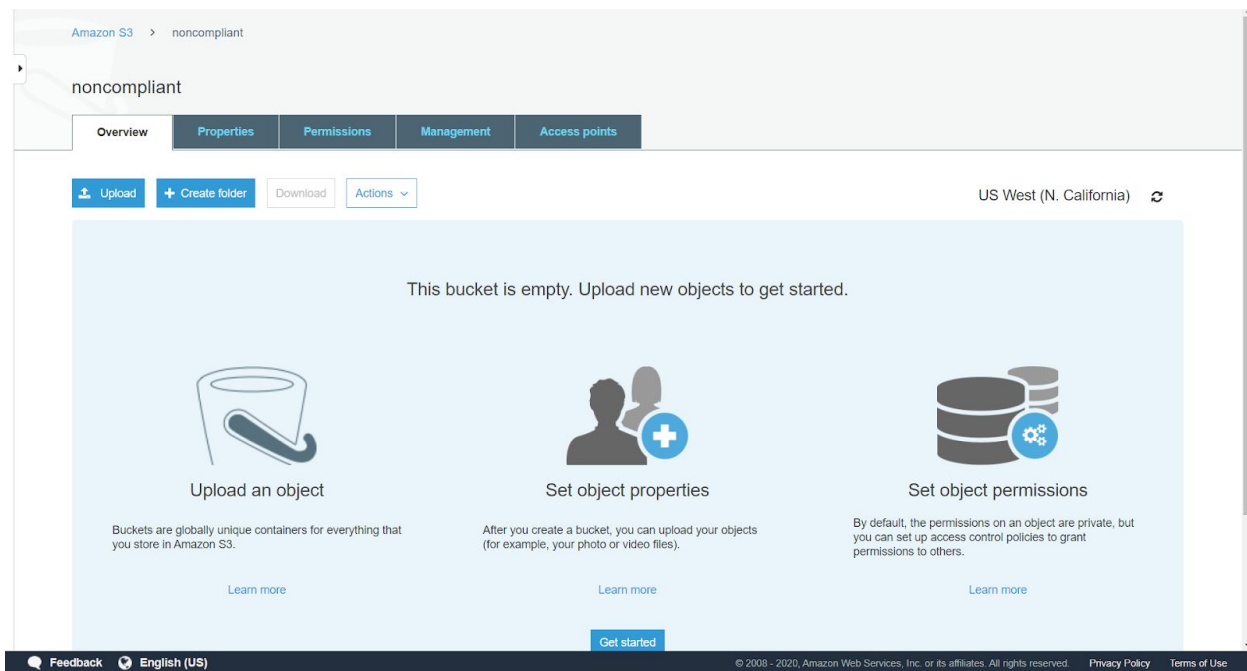
AWS Config - Resource Inventory

The screenshot shows the AWS Config Resource Inventory page. A notification at the top states: "The redesigned AWS Config console is now available for use. We've completely redesigned the console to improve the overall look and feel. Try it out now." The page includes a search bar and a table of resources.

Resource identifier	Resource type	Compliance
aws:ec2:MyAutoScalingGroup2-CPU-Utilization	CloudWatch Alarm	--
aws:ec2:MyAutoScalingGroup2-High-CPU-Utilization	CloudWatch Alarm	--
AWS-EC2: SecurityGrouping-628557bdc710e967	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-654c4e5a496819b5a	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-666a3cd805b19ae4	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-66a25ea0b41e0dc7	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-6c02a3c4a5d53194	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-6c02b12186a4d4b1c	Config ResourceCompliance	--
AWS-EC2: SecurityGrouping-6d6e58a7019e110f	Config ResourceCompliance	--

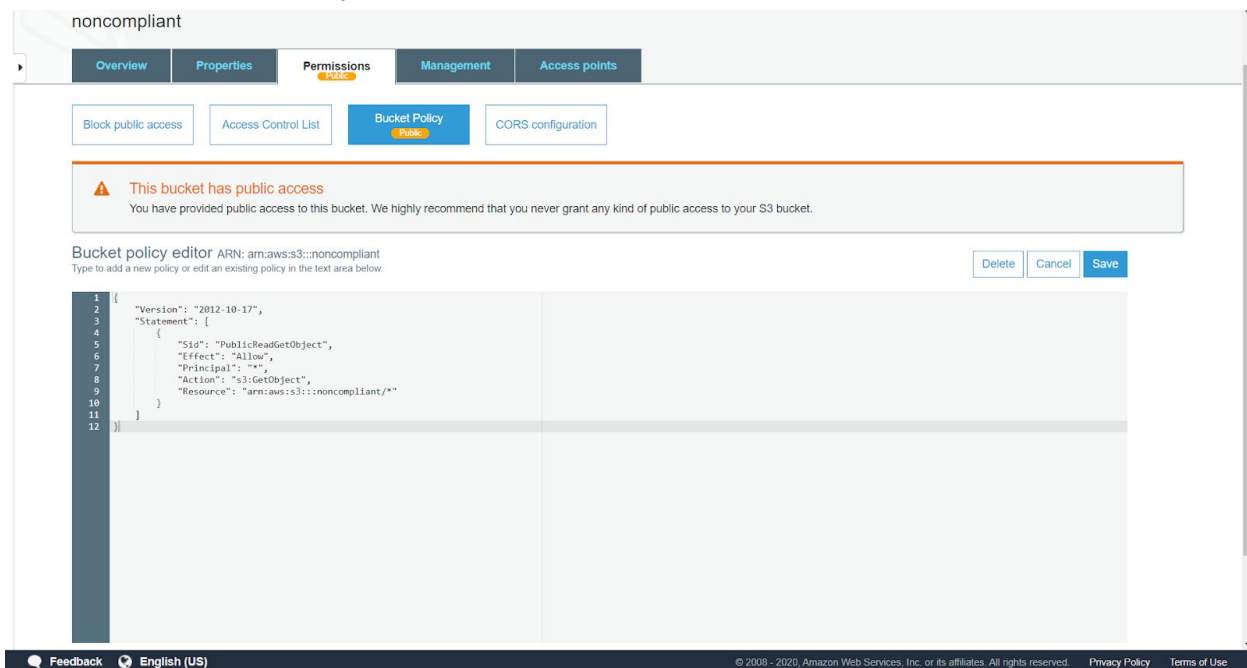
All the resources of the account recorded by AWS Config.

AWS Config - Dashboard



At this point there are 3 noncompliant resources (SSH related), to test for noncompliance in S3, a public S3 bucket was created.

Amazon S3 - Bucket Policy



The noncompliant test bucket is issued "PublicReadGetObject". A noncompliance action according to AWS Config.

AWS Config - Rules

AWS Config

Dashboard

Conformance packs

Rules

Resources

Advanced query

Settings

Authorizations

Aggregated view

Rules

Resources

Aggregators

What's new

Learn More

Documentation

Partners

FAQs

Pricing

The redesigned AWS Config console is now available for use.
We've completely redesigned the console to improve the overall look and feel. Try it out now.

Rules

Status

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.

Add rule

Manage remediation

View details

Edit

Compliance status

Filter

Rule name	Compliance	Remediation action
<input type="radio"/> restricted-ssh	3 Noncompliant resource(s)	Not set
<input type="radio"/> s3-bucket-public-read-prohibited	1 Noncompliant resource(s)	Not set

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

After about fifteen minutes, the noncompliant test S3 bucket shows up in AWS Config.

AWS Config - Dashboard

AWS Config

Dashboard

Conformance packs

Rules

Resources

Advanced query

Settings

Authorizations

Aggregated view

Rules

Resources

Aggregators

What's new

Learn More

Documentation

Partners

FAQs

Pricing

The redesigned AWS Config console is now available for use.
We've completely redesigned the console to improve the overall look and feel. Try it out now.

Config Dashboard

Status

Resources

Total resource count

33

Top 10 resource types

Total

EC2 SecurityGroup

10

EC2 Subnet

4

S3 Bucket

3

EC2 InternetGateway

2

EC2 VPC

2

RDS DBSubnetGroup

2

RDS DBSnapshot

2

EC2 RouteTable

2

EC2 NetworkAcl

2

CloudWatch Alarm

2

View all 33 resources

Run advanced queries against your resource configuration data.

Config rule compliance

2 Noncompliant rule(s)

Resource compliance

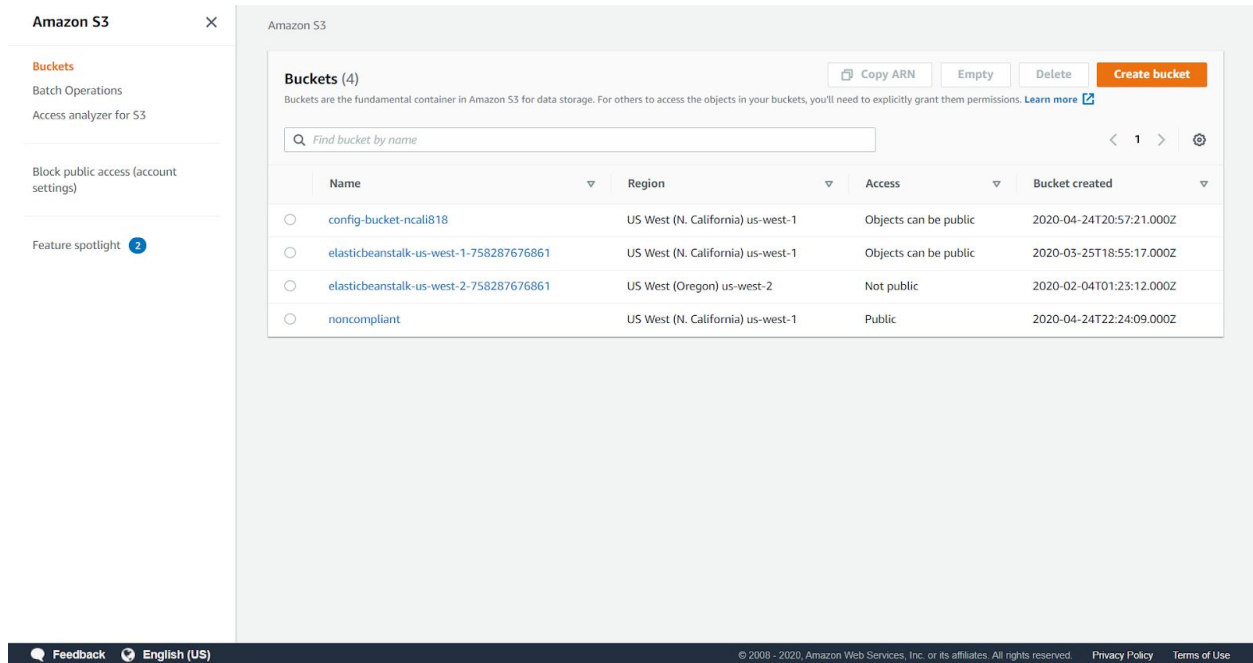
4 Noncompliant resource(s)

Noncompliant rules

Rule name	Compliance
restricted-ssh	3 Noncompliant resource(s)
s3-bucket-public-read-prohibited	1 Noncompliant resource(s)

Dashboard is confirming the new non-compliant S3 bucket.

Amazon S3 - Buckets



The screenshot shows the Amazon S3 console interface. On the left is a navigation sidebar with links for Buckets, Batch Operations, Access analyzer for S3, Block public access (account settings), and Feature spotlight (2). The main content area is titled 'Amazon S3' and 'Buckets (4)'. It includes buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. Below these is a search bar 'Find bucket by name' and a pagination control showing '1'. A table lists the buckets with columns for Name, Region, Access, and Bucket created.

	Name	Region	Access	Bucket created
<input type="radio"/>	config-bucket-ncali818	US West (N. California) us-west-1	Objects can be public	2020-04-24T20:57:21.000Z
<input type="radio"/>	elasticbeanstalk-us-west-1-758287676861	US West (N. California) us-west-1	Objects can be public	2020-03-25T18:55:17.000Z
<input type="radio"/>	elasticbeanstalk-us-west-2-758287676861	US West (Oregon) us-west-2	Not public	2020-02-04T01:23:12.000Z
<input type="radio"/>	noncompliant	US West (N. California) us-west-1	Public	2020-04-24T22:24:09.000Z

On interesting note is the elasticbeanstalk bucket created from a prior assignment. Access is set to “Objects can be public”, but AWS Config does not show this as a non-compliant bucket. This may cause confusion in other scenarios. Note the non-compliant test bucket as “Public”.