Home / AWS / Guided Lab / Check the Compliance status of Security group using AWS Config

Check the Compliance status of Security group using AWS Config

Level: **Fundamental**

AWS Config Amazon Web Services

WHIZLABS 0 K

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.86345838

Password

ed971c82-2bbb-44f7-809f-19e0f13ec633

Access Key

AKIAUOEQJSKAHDQJOVO6

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

ns

No Support Documents Found

Need help?

- How to use Hands on Lab
- Troubleshooting Lab
- FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation

Cloud Security Engineer

Management & Governance

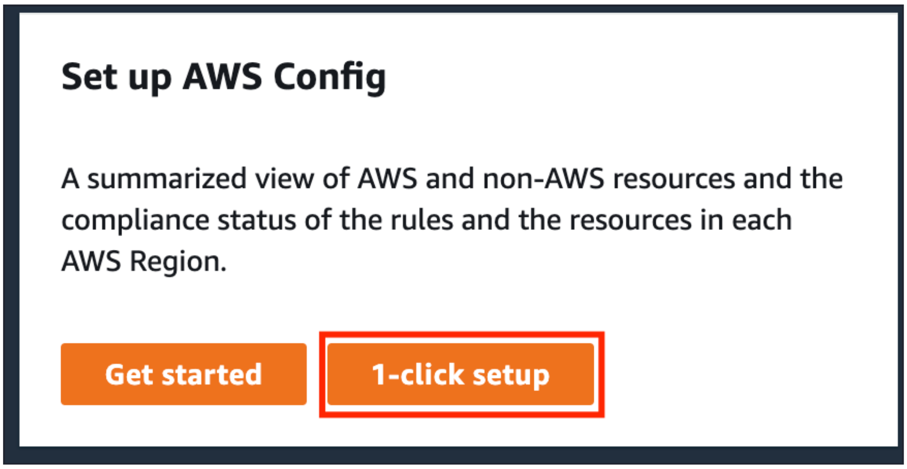
Lab Steps

Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
   - Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. Otherwise, you cannot proceed with the lab.
   - Now copy your **Username** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign-in** button.
3. Once Signed In to the AWS Management Console, make the default AWS Region as **US East (N. Virginia) us-east-1.**

Task 2: Setup Config with 1 Click option

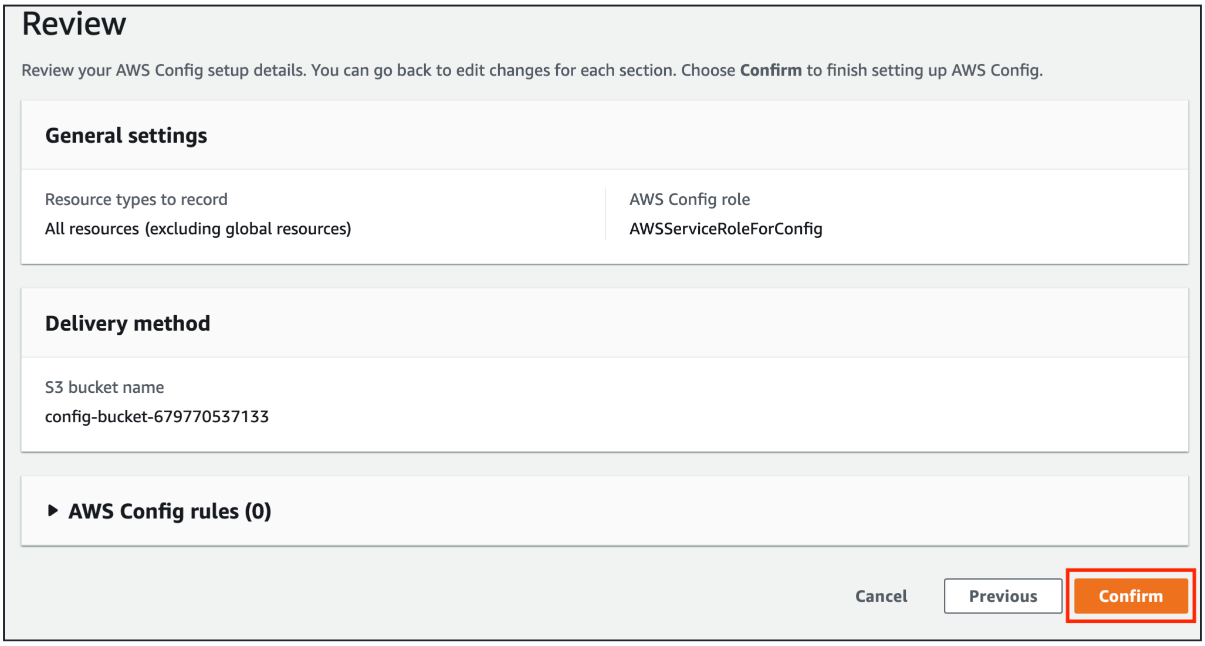
1. Make sure you are in the **N.Virginia** Region.
2. Navigate to **Config** by clicking on the **Services** menu available under the **Management & Governance** section.
3. On the Home page of AWS Config, click on the **1-click setup** option.



Set up AWS Config

A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.

4. Review everything and click on the **Confirm** button to complete the setup.



Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

General settings

Resource types to record
All resources (excluding global resources)

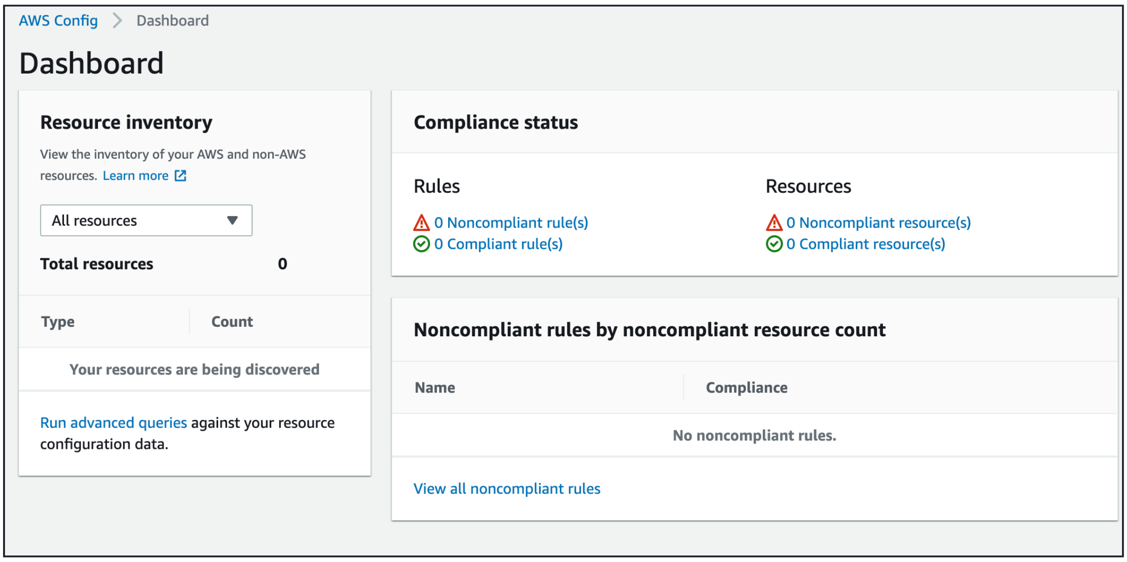
AWS Config role
AWSServiceRoleForConfig

Delivery method

S3 bucket name
config-bucket-679770537133

AWS Config rules (0)

5. Once the setup is done, Config will discover all the resources present in the account.



AWS Config > Dashboard

Dashboard

Resource inventory

View the inventory of your AWS and non-AWS resources. Learn more

All resources ▼

Total resources 0

Type	Count
Your resources are being discovered	

Run advanced queries against your resource configuration data.

Compliance status

Rules
⚠ 0 Noncompliant rule(s)
✓ 0 Compliant rule(s)

Resources
⚠ 0 Noncompliant resource(s)
✓ 0 Compliant resource(s)

Noncompliant rules by noncompliant resource count

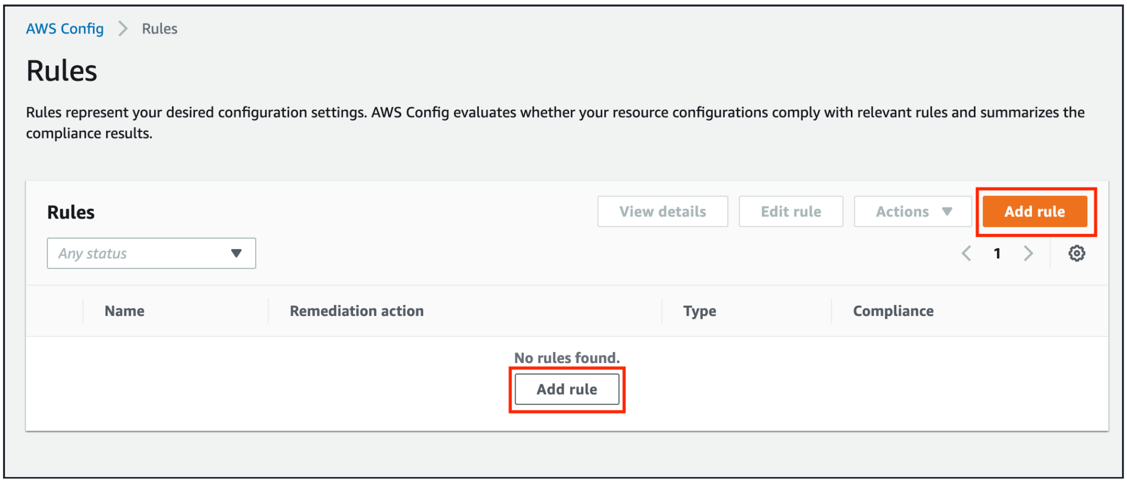
Name	Compliance
No noncompliant rules.	

View all noncompliant rules

Task 3: Create a Config Rule

1. On the left side panel, click on the **Rules** under **AWS Config**.

2. Click on the **Add rule** button.



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 ▼

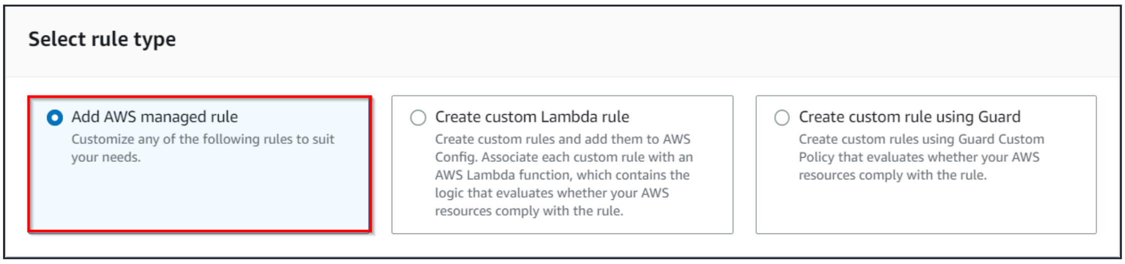
	Name	Remediation action	Type	Compliance

No rules found.

Add rule

3. For step-1, Specify the rule type, select the rule type and choose one of the AWS Managed rules.

- **Select rule type:** Select **Add AWS managed rule**



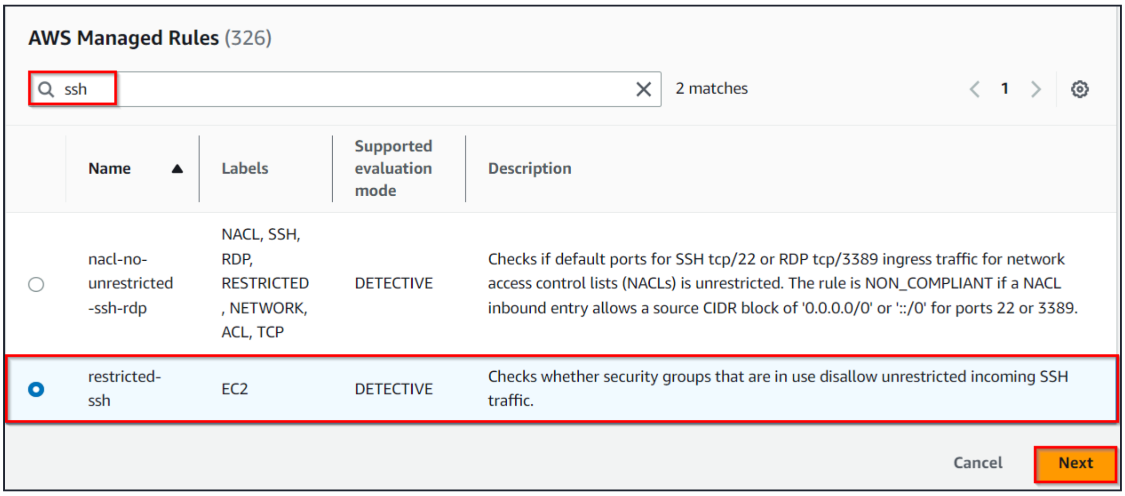
Select rule type

● Add AWS managed rule
Customize any of the following rules to suit your needs.

○ Create custom Lambda rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

○ Create custom rule using Guard
Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

- **AWS Managed Rules**: In the search box, type **ssh** and hit enter.
- Select the rule with the name **restricted-ssh** and click on the **Next** button.



AWS Managed Rules (326)

ssh ✕ 2 matches

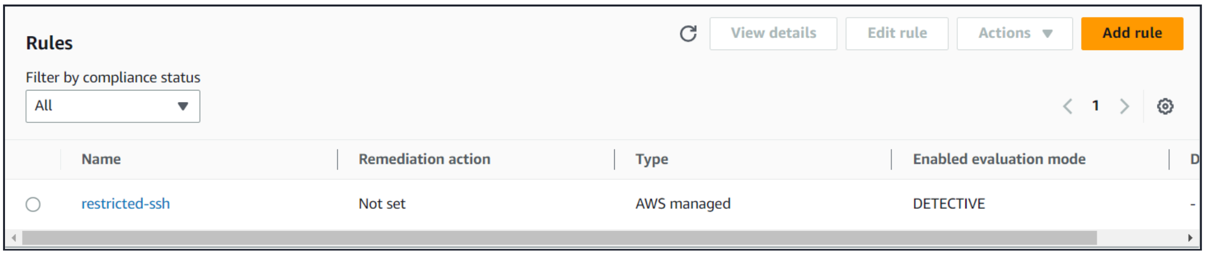
	Name ▲	Labels	Supported evaluation mode	Description
○	nacl-no-unrestricted-ssh-rdp	NACL, SSH, RDP, RESTRICTED, NETWORK, ACL, TCP	DETECTIVE	Checks if default ports for SSH tcp/22 or RDP tcp/3389 ingress traffic for network access control lists (NACLs) is unrestricted. The rule is NON_COMPLIANT if a NACL inbound entry allows a source CIDR block of '0.0.0.0/0' or '::/0' for ports 22 or 3389.
●	restricted-ssh	EC2	DETECTIVE	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Cancel | Next

4. For Step-2, Configure rule, keep all the options as default, and click on the **Next** button.

5. For Step-3, Review and create, review the settings and click on the **Save** button.

6. The rule is now added to our account.

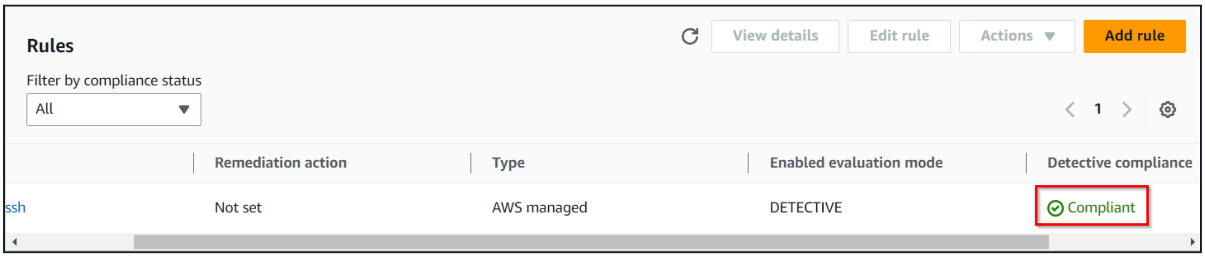


	Name	Remediation action	Type	Enabled evaluation mode	D
○	restricted-ssh	Not set	AWS managed	DETECTIVE	-

7. Wait for 2–3 minutes, config rule named restricted-ssh, will check all the security groups and let you know the compliance status.

8. Since there is only one security group present i.e. default Security group of default VPC present in the account, it will check whether it is having an SSH inbound port or not if there is an SSH inbound port, what is the source. If it is 0.0.0.0/0 then it will be marked as a non-compliant resource. By default, it is not open, so it will be a compliant resource.

Note: If the Compliance status is still not showing anything, refresh the page using the Ctrl + R option.



	Remediation action	Type	Enabled evaluation mode	Detective compliance
ssh	Not set	AWS managed	DETECTIVE	✓ Compliant

9. Let's create 2 sample security groups with the only SSH as an inbound port with 0.0.0.0/0 as the source and check whether Config is marking them as a non-compliant resource or not.

Task 4: Create first Security Group

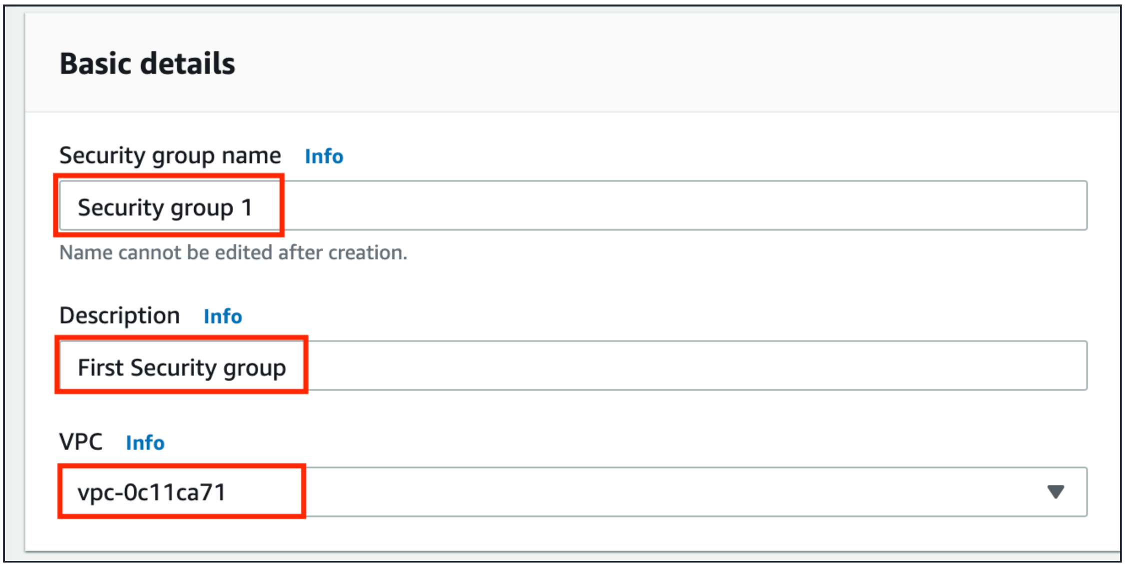
1. Navigate to **EC2** by clicking on the **Services** menu available under the **Compute** section.

2. On the left panel menu, select the security group under the **Network & Security** section.

3. Click on the **Create security group** button.

4. We are going to create a Security group for the ECS cluster.

   - Security group name: Enter **Security Group 1**
   - Description: Enter **First Security group**
   - VPC: Select **Default VPC**



Basic details

Security group name Info

Security group 1

Name cannot be edited after creation.

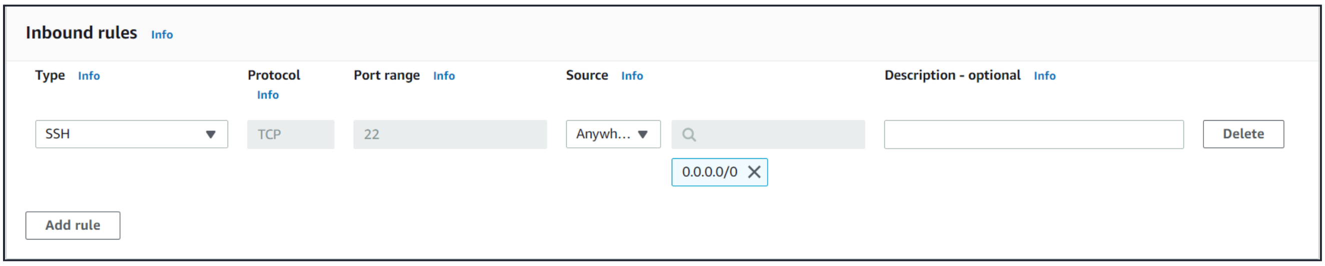
Description Info

First Security group

VPC Info

vpc-0c11ca71

- Click on the **Add rule** button under **Inbound rules.**
  - Type : Select **SSH**
  - Source : Select **Anywhere IPv4**

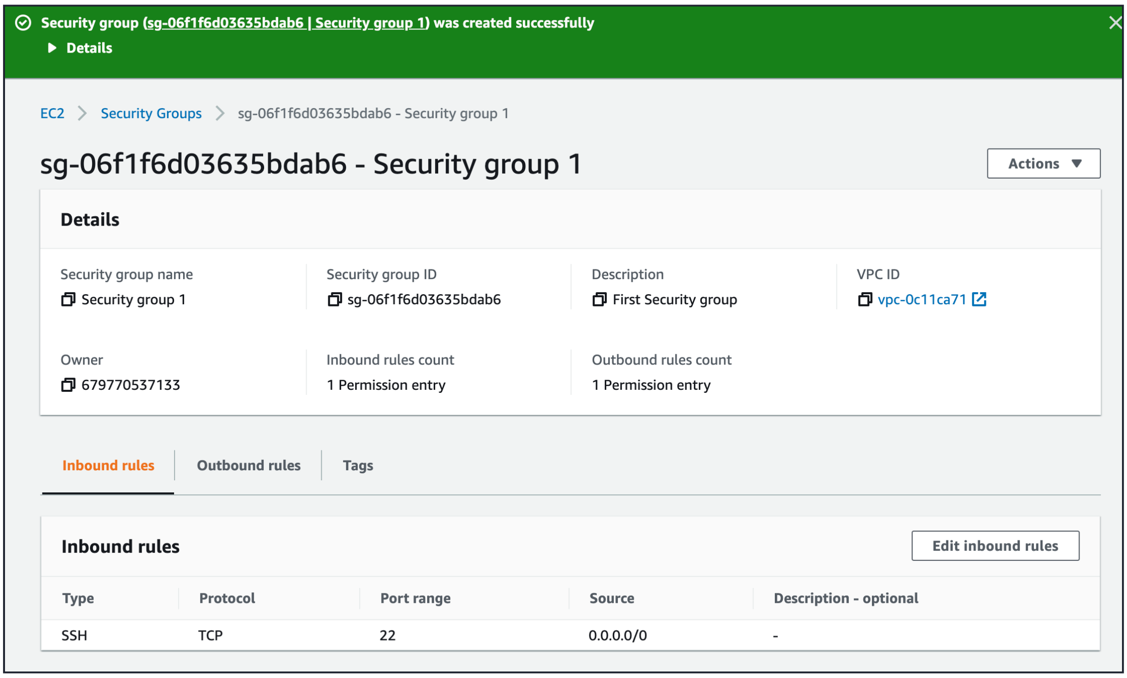


Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
SSH	TCP	22	Anywh...	0.0.0.0/0		Delete

5. Leave everything as default and click on the **Create security group** button.

6. Security group name, **Security group 1** is now created.



Security group (sg-06f1f6d03635bdab6 | Security group 1) was created successfully

Details
EC2 > Security Groups > sg-06f1f6d03635bdab6 - Security group 1

sg-06f1f6d03635bdab6 - Security group 1

Details

Security group name	Security group ID	Description	VPC ID
Security group 1	sg-06f1f6d03635bdab6	First Security group	vpc-0c11ca71
Owner	**Inbound rules count**	**Outbound rules count**	
679770537133	1 Permission entry	1 Permission entry	

Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-

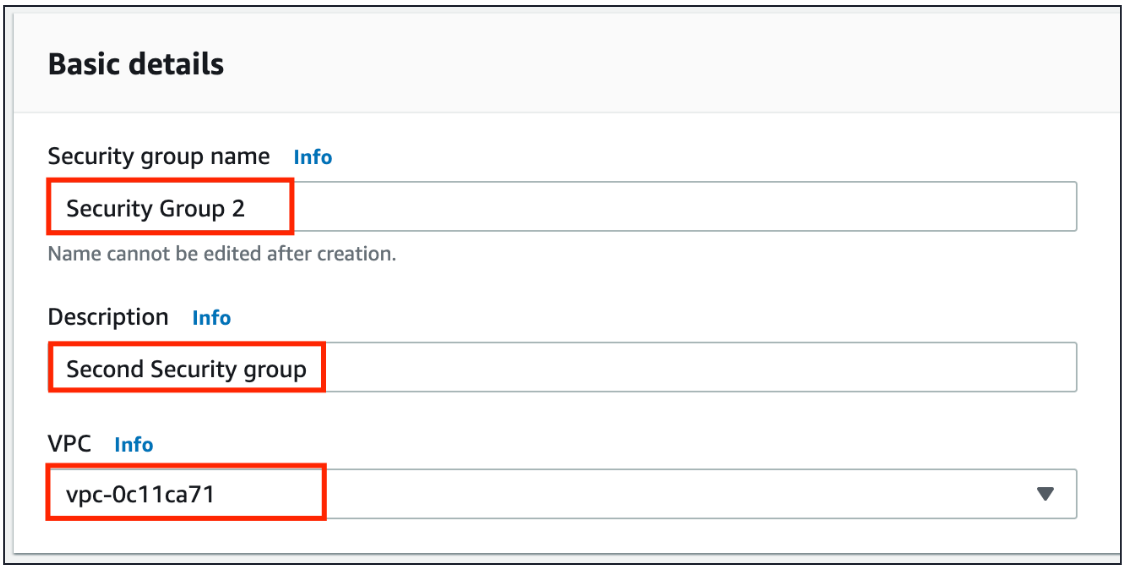
Task 5: Create second Security Group

1. On the left panel menu, select the **Security groups** under the **Network & Security** section.

2. Click on the **Create security group** button.

3. We are going to create a Security group for the ECS cluster.

    - Security group name: Enter **Security Group 2**
    - Description: Enter **Second Security group**
    - VPC: Select **Default VPC**



Basic details

Security group name Info

Security Group 2

Name cannot be edited after creation.

Description Info

Second Security group

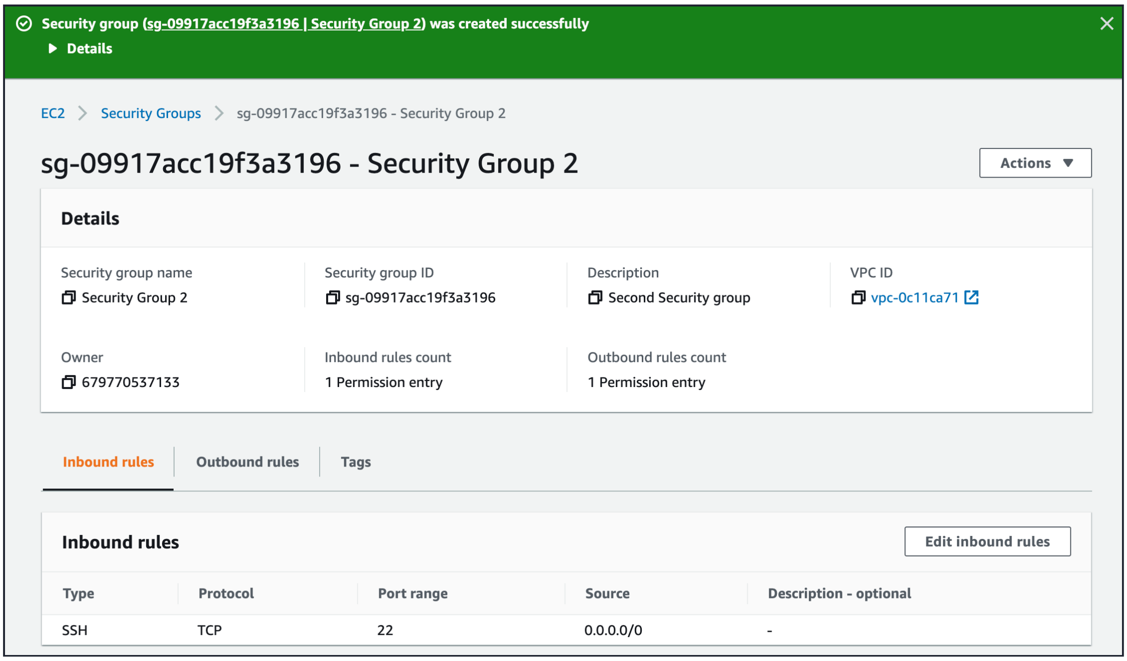
VPC Info

vpc-0c11ca71

- Click on the **Add rule** button under **Inbound rules.**
    - Type : Select **SSH**
    - Source : Select **Anywhere IPv4**

4. Leave everything as default and click on the **Create security group** button.

5. Security group name, **Security group 2** is now created.



Security group (sg-09917acc19f3a3196 | Security Group 2) was created successfully

EC2 > Security Groups > sg-09917acc19f3a3196 - Security Group 2

sg-09917acc19f3a3196 - Security Group 2

Details

Security group name	Security group ID	Description	VPC ID
Security Group 2	sg-09917acc19f3a3196	Second Security group	vpc-0c11ca71
Owner	Inbound rules count	Outbound rules count	
679770537133	1 Permission entry	1 Permission entry	

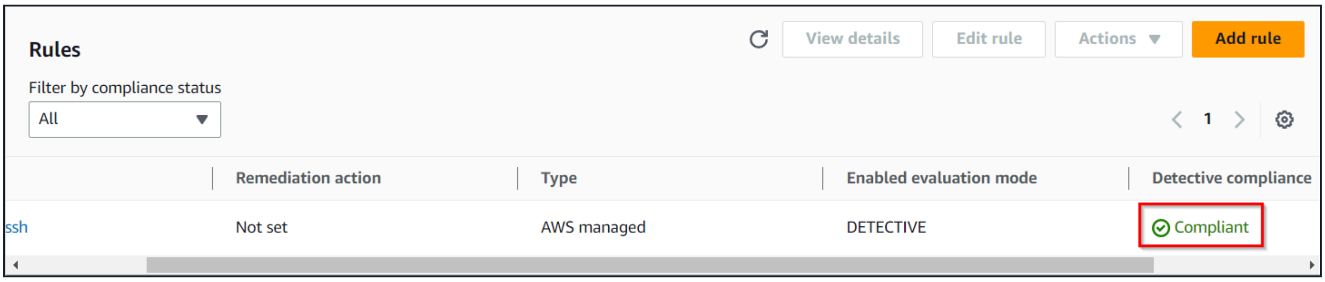
Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	0.0.0.0/0	-

Task 6: Test the compliance status of the Security groups

In this task, we are going to check if the security groups are marked as compliant or non-compliant by the AWS Config rule.

1. Navigate to **Config** by clicking on the **Services** menu available under the **Management & Governance** section.
2. On the left side bar, click on the **Rules**, and you will be able to see the rule is still in **compliant** status.

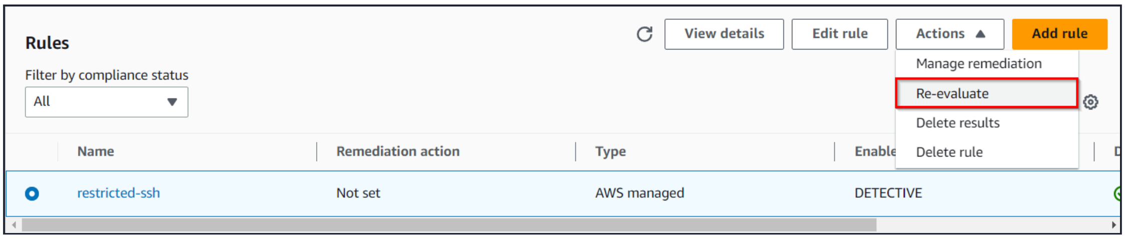


Rules

Filter by compliance status: All

	Remediation action	Type	Enabled evaluation mode	Detective compliance
ssh	Not set	AWS managed	DETECTIVE	Compliant

3. To get the latest compliance status of the rule, we need to refresh them. In terms of Config, it is called Re-evaluate.
4. Perform the following task to Re-evaluate:
   - Select the rule present,
   - Click the **Actions** button,
   - And, Choose **Re-evaluate** option.



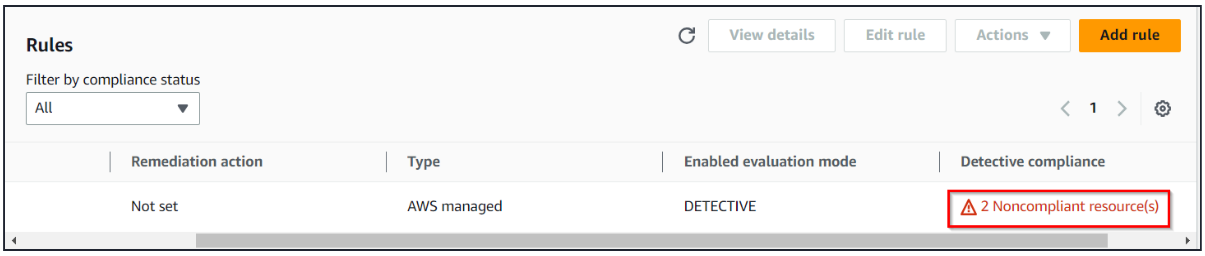
Filter by compliance status: All

Name	Remediation action	Type	Enable
● restricted-ssh	Not set	AWS managed	DETECTIVE

5. It may take up to 5 minutes for the config to get the compliance status of the created security groups.

6. Compliance status is now refreshed, it is showing 2 Noncompliant resource(s).

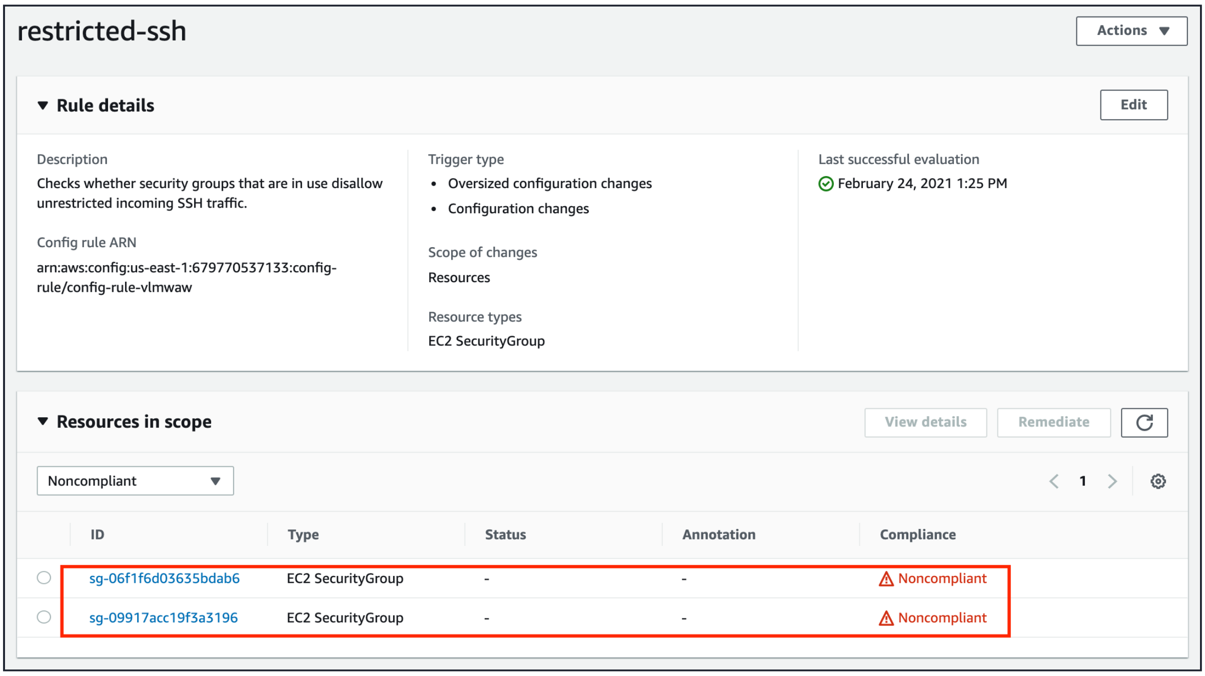
Note: If the Compliance status is still now showing anything, refresh the page using the Ctrl + R option.



Filter by compliance status: All

Remediation action	Type	Enabled evaluation mode	Detective compliance
Not set	AWS managed	DETECTIVE	⚠ 2 Noncompliant resource(s)

7. Click on the rule name to check the Noncompliant resources.



restricted-ssh

▼ Rule details

Description
Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.

Config rule ARN
arn:aws:config:us-east-1:679770537133:config-rule/config-rule-vlmwaw

Trigger type
- Oversized configuration changes
- Configuration changes

Scope of changes
Resources

Resource types
EC2 SecurityGroup

Last successful evaluation
✓ February 24, 2021 1:25 PM

▼ Resources in scope

Noncompliant

ID	Type	Status	Annotation	Compliance
○ sg-06f1f6d03635bdab6	EC2 SecurityGroup	-	-	⚠ Noncompliant
○ sg-09917acc19f3a3196	EC2 SecurityGroup	-	-	⚠ Noncompliant

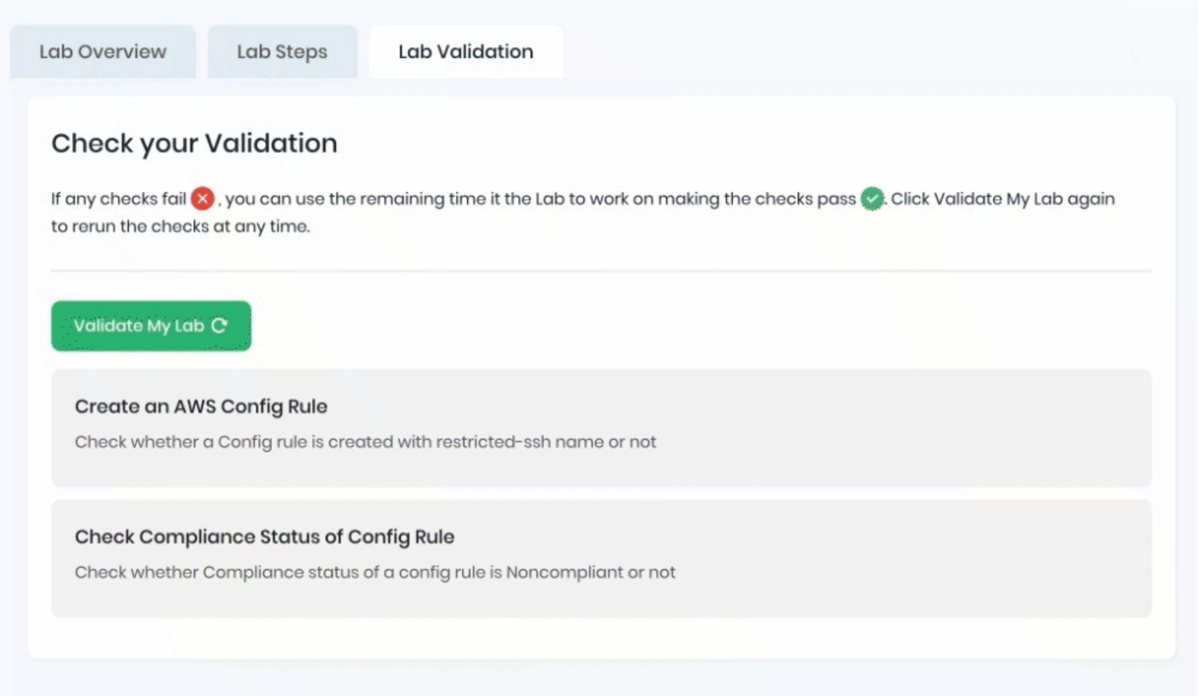
8. Optionally, you can remove all the inbound rules and recheck the compliance status.

Do You Know?

AWS Config provides a historical record of changes to your AWS resources. It allows you to view the configuration of your resources at any point in time, not just the current state. This means that you can track changes, troubleshoot issues, and perform compliance audits by accessing the historical configuration data. AWS Config provides a detailed timeline of resource configuration changes, making it a powerful tool for auditing and maintaining the desired state of your AWS environment.

Task 7: Validation Test

1. Once the lab steps are completed, please click on the **Validate** button on the right side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



Check your Validation

If any checks fail ✗, you can use the remaining time it the Lab to work on making the checks pass ✓. Click Validate My Lab again to rerun the checks at any time.

Create an AWS Config Rule

Check whether a Config rule is created with restricted-ssh name or not

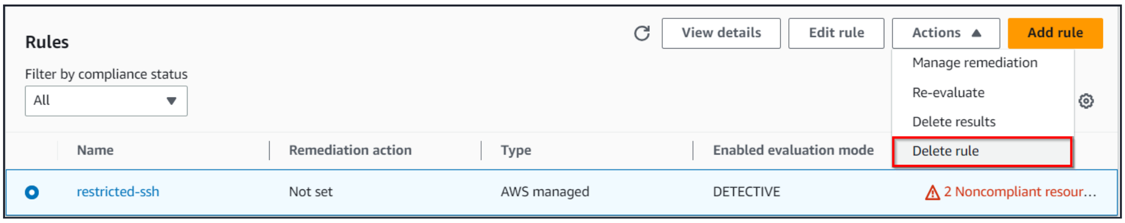
Check Compliance Status of Config Rule

Check whether Compliance status of a config rule is Noncompliant or not

Task 8: Delete AWS Resources

Deleting Config rules

1. To delete the present config rule, perform the following task:
   - Select the config rule,
   - Click on the **Actions** button,
   - Choose the **Delete rule** option.



	Name	Remediation action	Type	Enabled evaluation mode	
●	restricted-ssh	Not set	AWS managed	DETECTIVE	⚠ 2 Noncompliant resour...

2. On the confirmation pop-up, Enter **Confirm** and click on the **Delete** button.

3. It will take up to 2 minutes for the rule to be deleted, you can end the lab now.

Completion and Conclusion

1. You have successfully created and launched Amazon EC2 Instance.

2. You have successfully logged into the EC2 instance by SSH.

3. You have successfully created a webpage and published it.

End Lab

1. Sign out of AWS Account.

2. You have successfully completed the lab.

3. Once you have completed the steps, click on **End Lab** from your whizlabs lab console and wait till the process gets completed.

About Us Subscription Instructions and Guidelines FAQ's Contact Us