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.



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

Graphical user interface, text, application, email

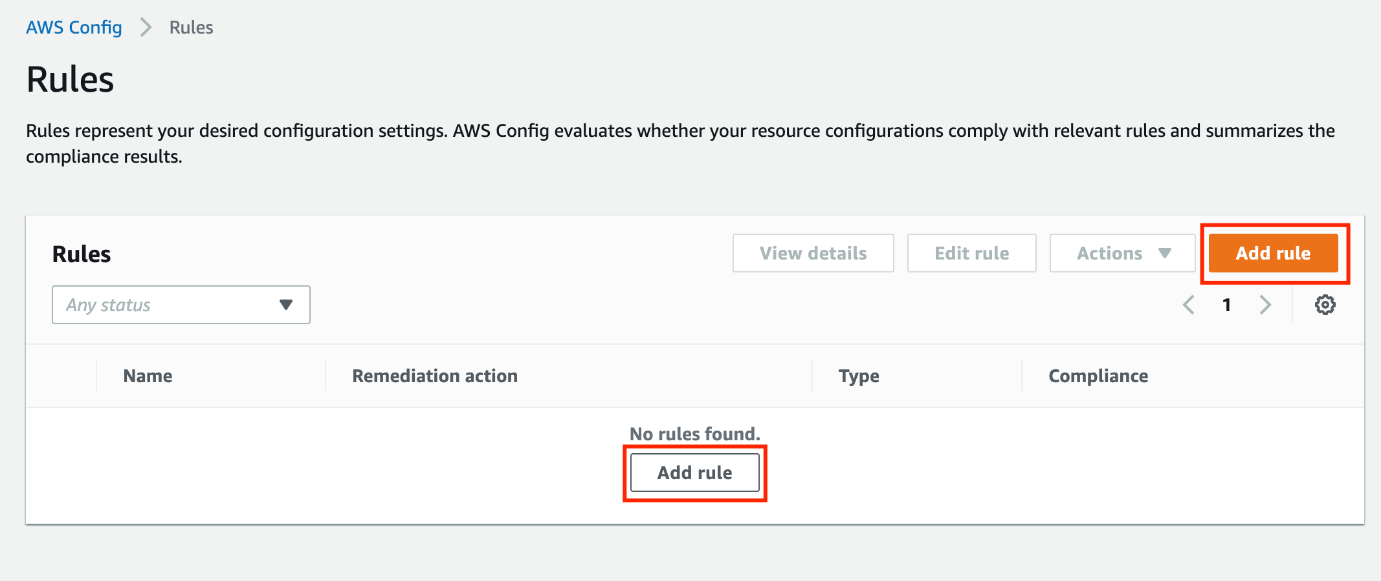
Description automatically generated

1. Once the setup is done, Config will discover all the resources present in the account. It will take up to 10 minutes for Config to complete the discovery.

Graphical user interface, application

Description automatically generated

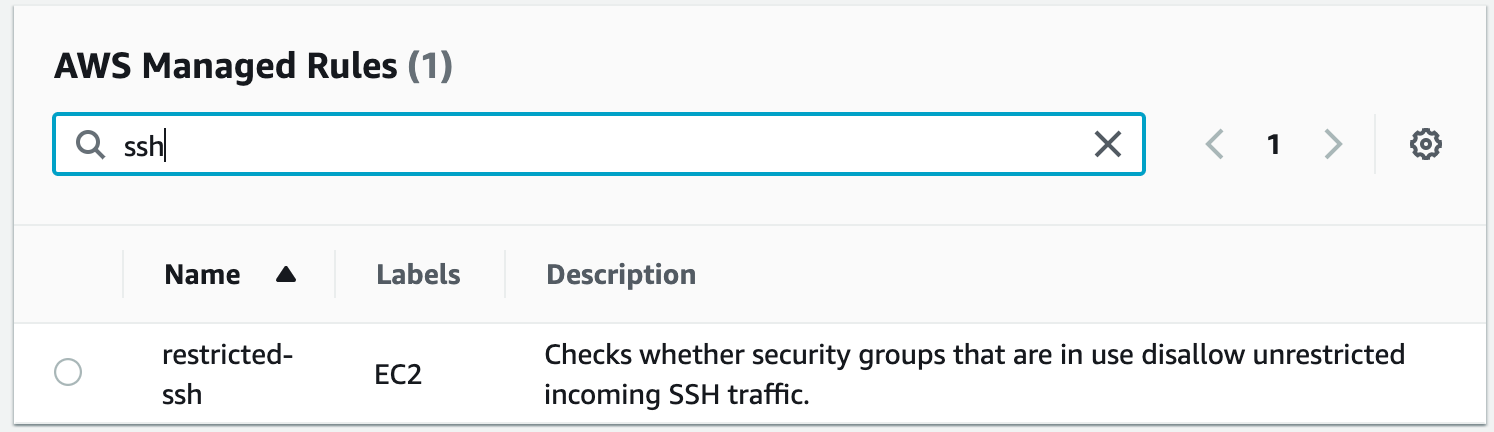
Task 3: Create a Config Rule

1. On the left side panel click on the **Rules**under **AWS Config**.
2. Click on the **Add rule** button.  
   
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**

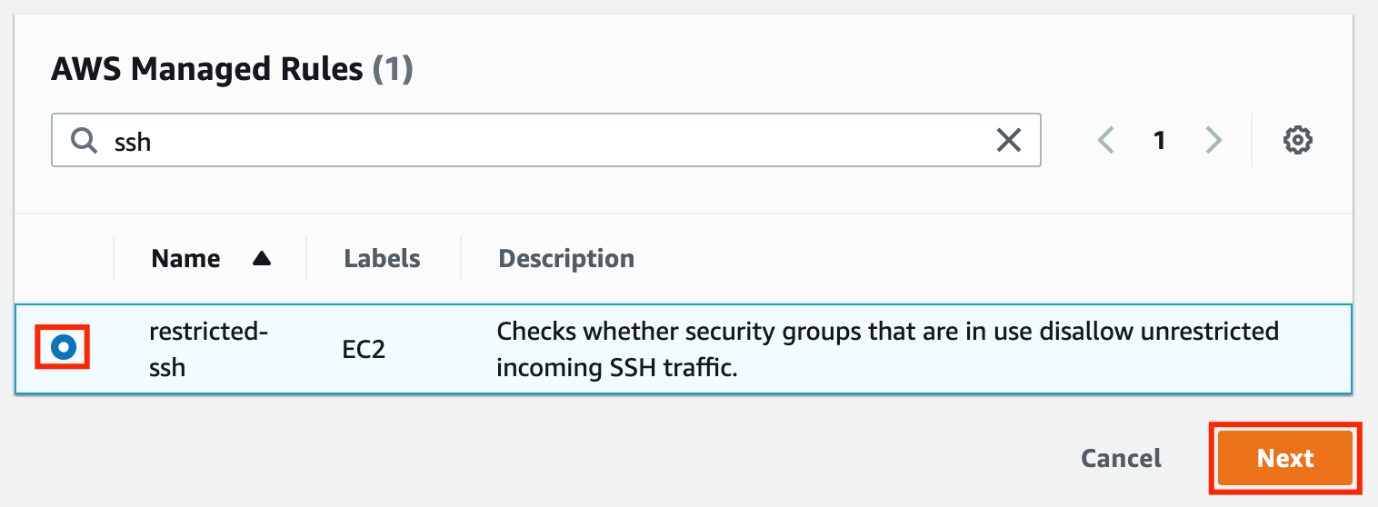
Graphical user interface, application

Description automatically generated

* + **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.

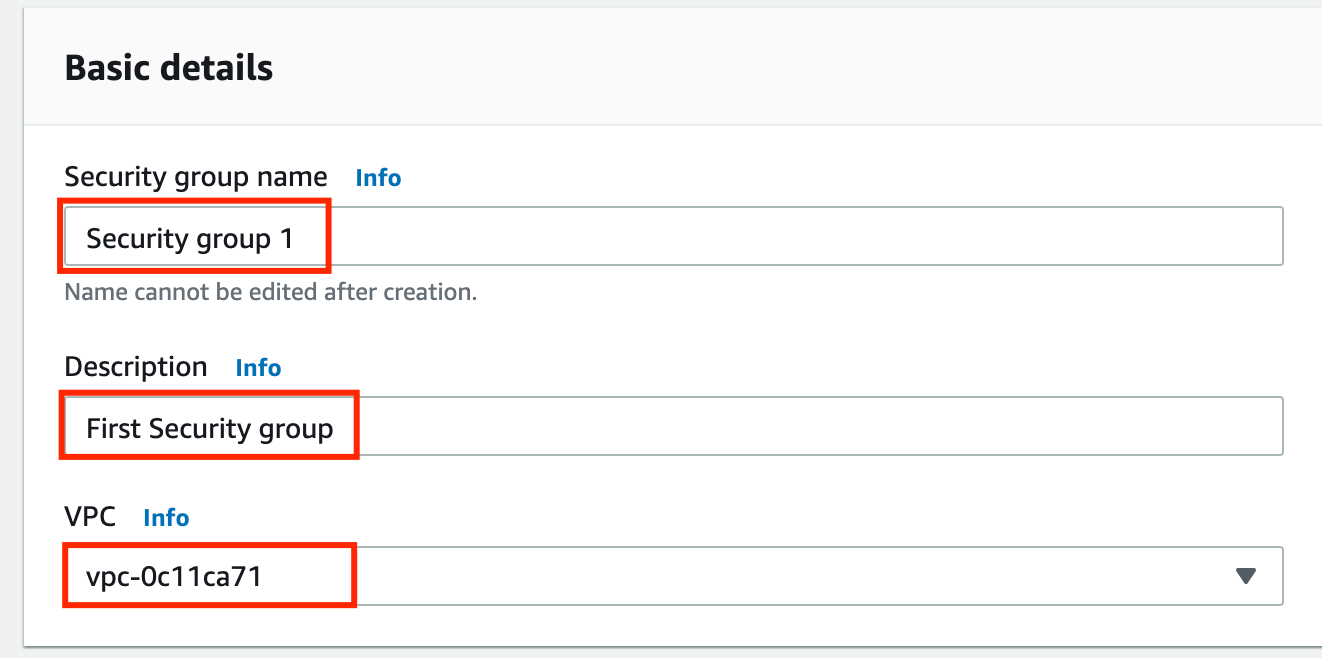


1. For Step-2, Configure rule, keep all the options as default, and click on the **Next** button.
2. For Step-3, Review and create, review the settings and click on the **Add rule** button.
3. The rule is now added to our account.  
   Graphical user interface, text, application, email

   Description automatically generated
4. Wait for 2-3 minutes, config rule named restricted-ssh, will check all the security groups and let you know the compliance status.
5. 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.**  
     
   Graphical user interface, text, application, email

   Description automatically generated
6. 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.

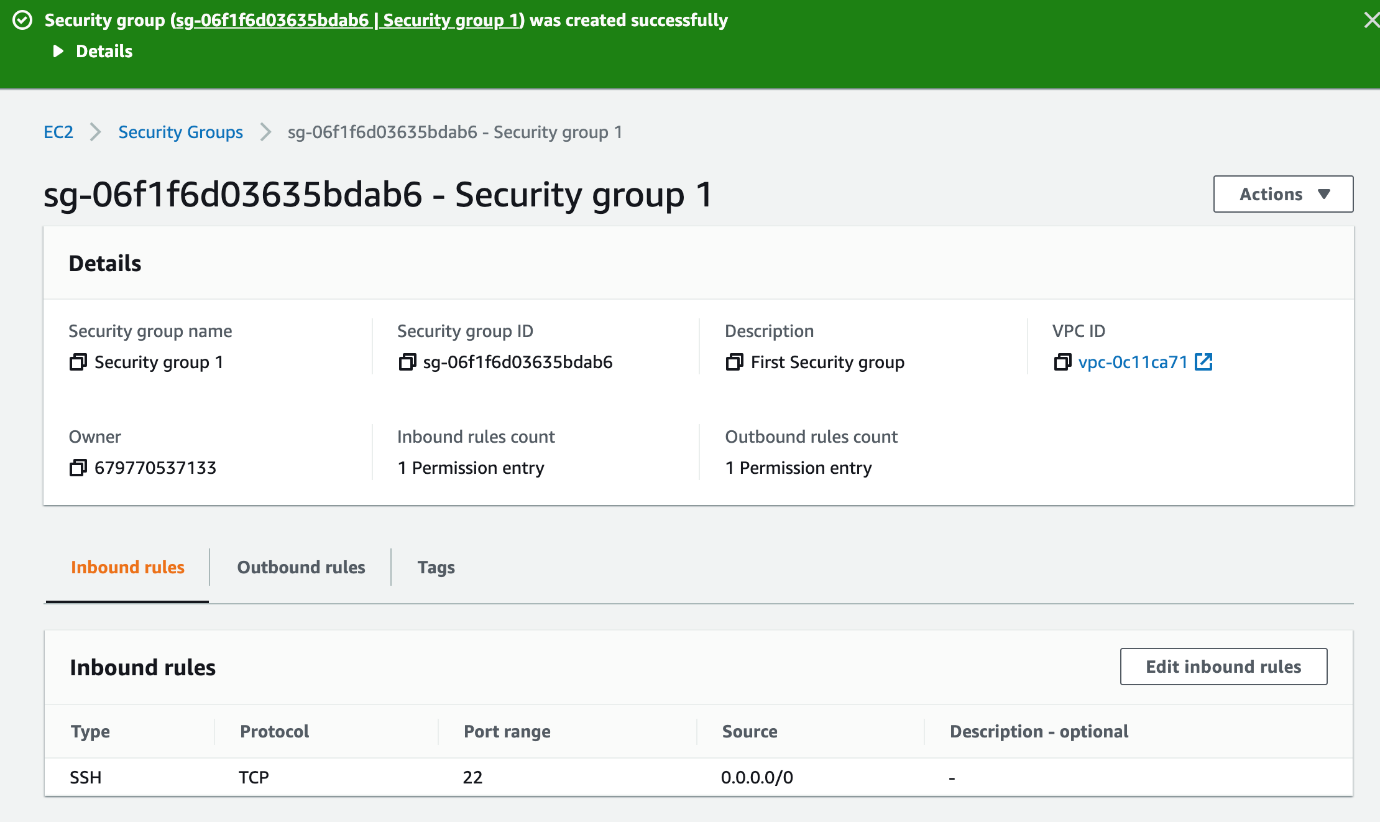
Task 4: Create first Security Group

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  .
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  
     **

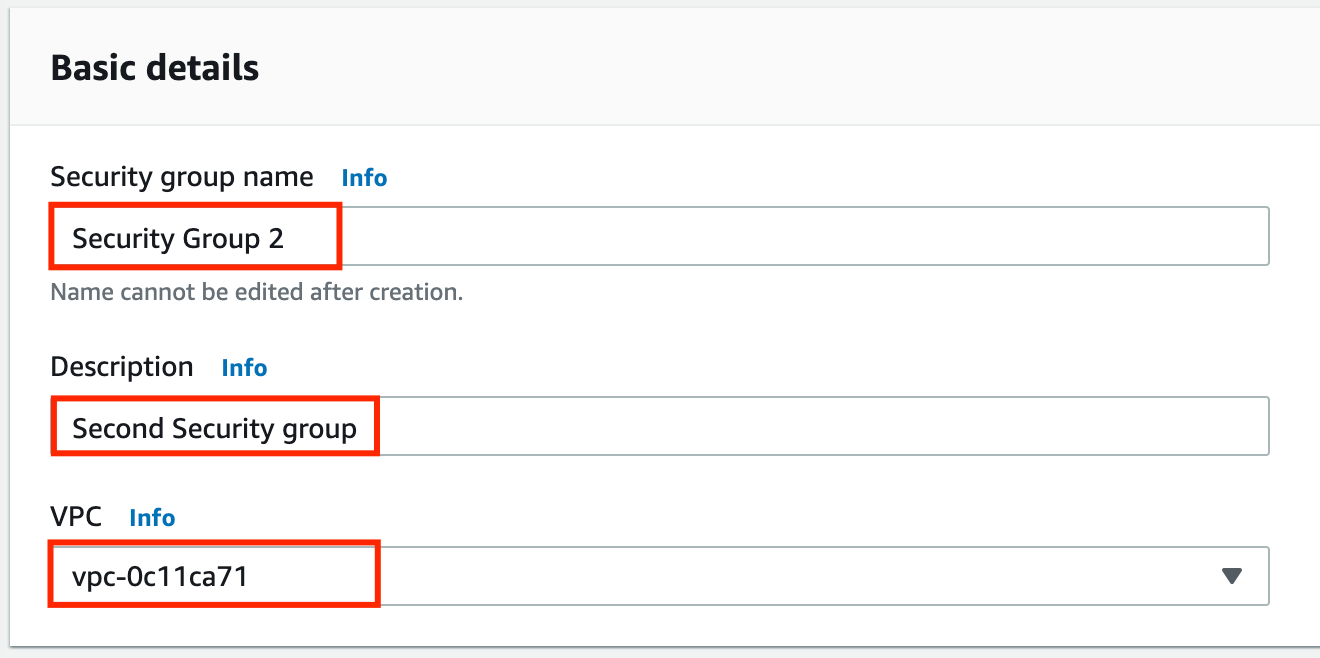
* Click on the  button under **Inbound rules.**
  + Type : Select **SSH**
  + Source : Select **Custom**
  + In the textbox add ***0.0.0.0/0***

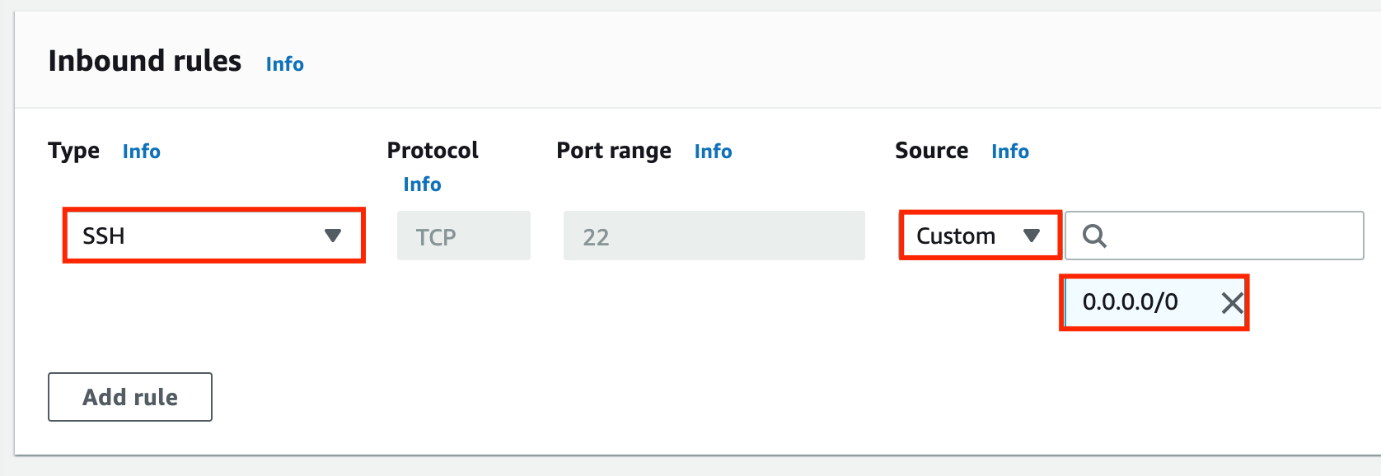
Graphical user interface, application

Description automatically generated

1. Leave everything as default and click on the  .
2. Security group name, **Security group 1** is now created.  
   

Task 5: Create second Security Group

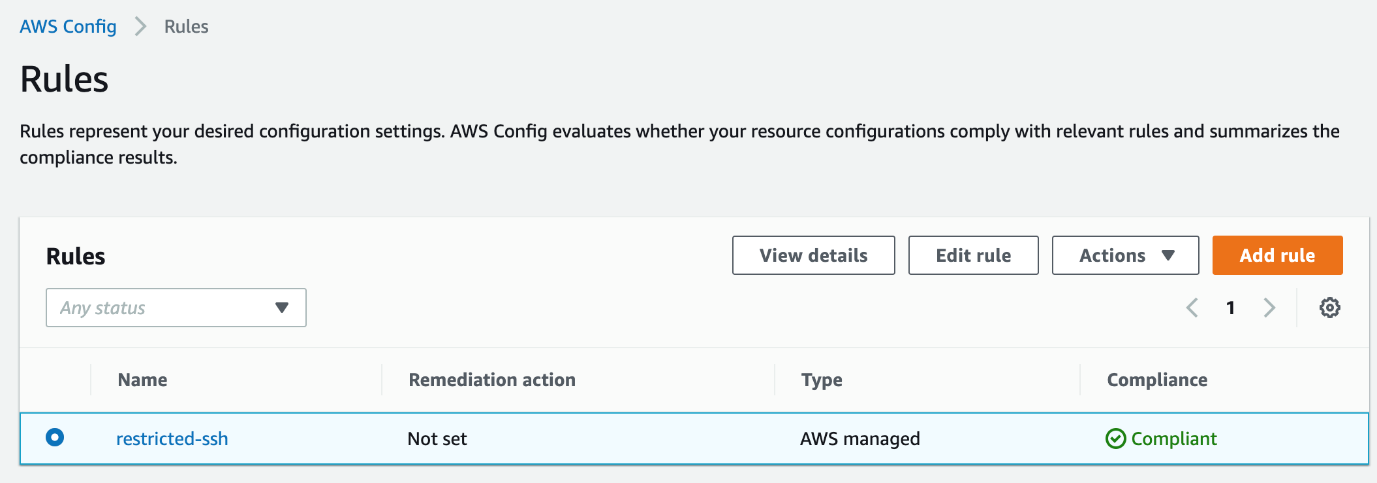
1. On the left panel menu, select the **Security groups** under the **Network & Security**section.
2. Click on the  .
3. We are going to create a Security group for the ECS cluster.
   * Security group name: Enter ***Security Group 2***
   * Description: Enter ***Second Security group***
   * VPC: Select **Default VPC  
     **

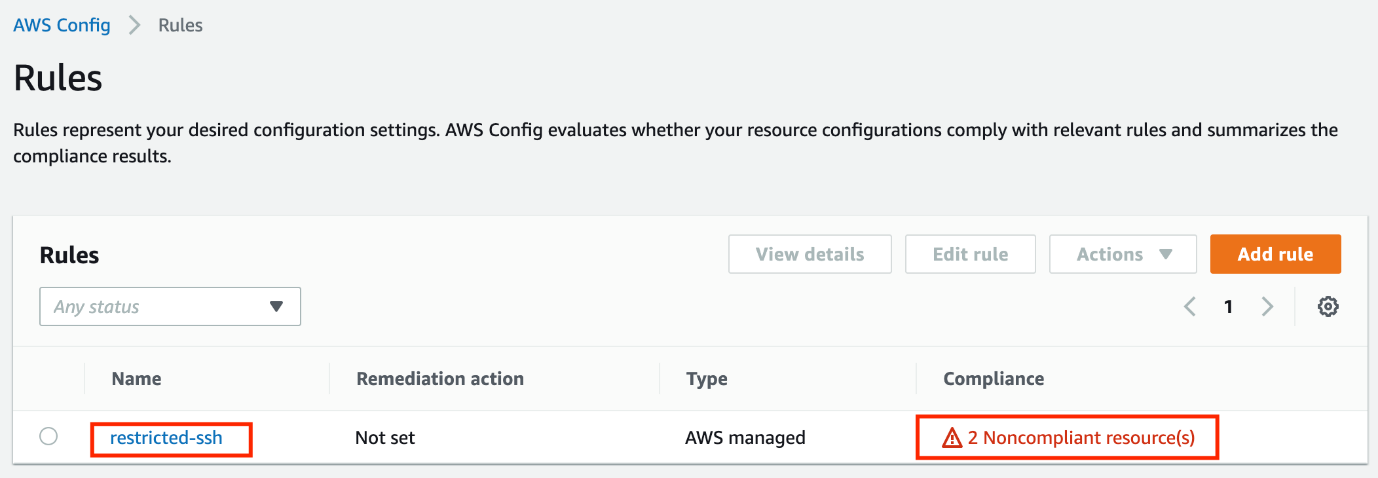
* Click on the  button under **Inbound rules.**
  + Type : Select **SSH**
  + Source : Select **Custom**
  + In the textbox add ***0.0.0.0/0*  
    **

1. Leave everything as default and click on the  .
2. Security group name, **Security group 2** is now created.  
   Graphical user interface, application

   Description automatically generated

Task 6: Test the compliance status of the Security groups

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 compliance status.   
   
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.   
     Graphical user interface, text, application, email

     Description automatically generated
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.**  
   
7. Click on the rule name to check the Noncompliant resources.  
   Graphical user interface, application

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

Task 7: Validation Test

1. Once the lab steps are completed, please click on the  button on the left 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 :

Table

Description automatically generated

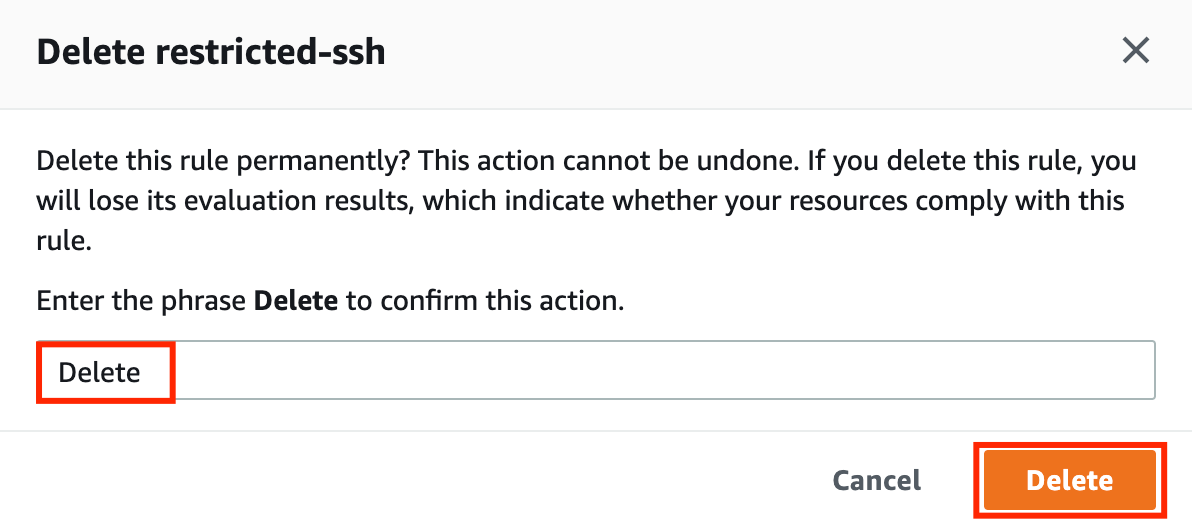
Task 8: Delete AWS Resources

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.

Graphical user interface, text, application, email

Description automatically generated

1. On the confirmation pop-up, enter **Delete** and click on the **Delete** button.  
   
2. 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**