WHIZLABS

Auditing Resource Compliance with AWS config

Level: Intermediate

AWS Config Amazon Web Services

0h 44m 14s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.26827434

Password

420a7250-094b-4b3c-9d41-a0b550d3193d

Access Key

AKIAW5SECW7OHEB43P5T

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

1. FAQs and Troubleshooting

Need help?

How to use Hands on Lab

Troubleshooting Lab

FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation

Security

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 **User Name** 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: Create S3 and SNS

1. Click on services and type config and navigate to **Config** dashboard.
2. Make sure you are in the N.Virginia Region.
3. Click on **Get Started**.
4. Now complete the **settings** using below details

- Recording strategy:
    - Select : **All resource types with customizable overrides**
    - Keep rest things as default

- Delivery Method:
    - Select the **Create a bucket** and enter your bucket name.
    - Bucket name : **Enter Unique bucket name** (Ex: whizlabs34567)
- Amazon SNS topic:
    - Check the box **Stream configuration changes** and then configure the SNS topic
    - Select the **Create a Topic**
    - Topic name : **config_for_securitygroup_change**

- Click on **Next** button.

5. In the next screen, leave as default and then click on **Next**.
6. Finally, review your config setup and click on **Confirm.** It will take a few seconds to complete the config rule setup.

Task 3: Setting of AWS config Rules

1. In the AWS Config **Dashboard** click on **Conformance packs** in the left panel.
2. Click on **Rules** under conformance packs.
3. Then click on **Add rule** on the right top.

---

4. Configure Rule type using below details
    - Select rule type:
        - Select **Add AWS managed rule**
    - AWS Managed Rules:

- Type **sg** in the filter box and then select **vpc-sg-open-only-to-authorized-ports** as shown in the below screenshot.

---

5. Once provided the above details click on **Next**.
6. In the next screen customize the rule with the below details
    - Name : **SgauthorizingRule**
    - Description : Leave default
7. Trigger:
    - Scope of changes: select **Resources**
8. Resources: Leave the default **AWS EC2 SecurityGroup**.
9. Parameters: select the ports you need to add in the rule.In your existing security group you will be added with the ports 22 and 80.

    - In case of adding a new rule, you can click on **Add another row.**
10. It will take 4 to 5 minutes for the rule to become available.
11. After providing above details click on **Next**.
12. Finally click on **Save.**

Task 4: Creating and subscribe SNS topic

1. Click on services and navigate to **Simple Notification Service**.
2. Click on **Topics** in the left panel.
3. Click on the config rule **config_for_securitygroup_change** created the earlier step
4. Click on **Create Subscription** in the right bottom.
5. Complete the subscription using below details
    - Topic ARN : Leave Default
    - Protocol : Select **Email** in the drop down.

- Endpoint : Enter the **Email address for subscription** (ex: test@gamail.com)
- Finally click on **Create Subscription** .

6. Now go to the Inbox of the email provided in the above step and click on **confirm subscription** to get the alerts as shown below

---

Task 5: Checking the status of AWS config

1. To check the status of your config rule navigate to **AWS config dashboard** and then click on **Conformance packs**
2. Click on **Rules** under conformance packs and click on the rule create by you.
3. Now, scroll down to the **Resources in scope** and select **Compliant** in filter, and you will see one security group with **Compliant** status.

- Thus the above screenshot states that the ports opened in the Security group attached with our running instance satisfy the rule given in the config.

Task 6: Testing the working of AWS config

1. Now click on **Services** and then navigate to the EC2 **dashboard.**
2. Click on **Security Groups** and select the security group named **AWS-congig-sg.**
3. Click on **Inbound** and then **Edit** to add some custom ports. (Ex: 20-21)

---

4. Now add the new port with below details

- Type : select **Custom TCP**
- Protocol : **TCP**
- Port Range : Enter **20-21**
- Source : **0.0.0.0/0**
- Click on **Save**

5. Now navigate to **AWS config dashboard** and then click on **Conformance packs** wait for **1 or 2 minutes**, and you could see the status of your rule as **Noncompliant**

resource(s) as shown below

---

6. To check the **detailed status,** click on the **SgauthorizingRule** and scroll down a bit and then click on **Resources in scope** and then click on your **security group ID** of your noncompliant security group
7. In the next step click **Resource Timeline** in the right corner.

---

9. To confirm Alert via **SNS topic,** navigate to the inbox of the email provided at the time of creating SNS topic, and you could see the Alert email from AWS regarding change in your AWS config rule.

---

12. Now click on **Services** and then navigate to the EC2 **dashboard** and click on **Security Groups** and select the security group named **AWS-congig-sg** and remove the port number 20-21 from the security group and save.
13. Once removed navigate to **AWS config dashboard** and then click on **Conformance packs** and check the status of the rule, and you could see the status as **Compliant**

---

14. Now navigate to the Inbox of your email and you could see AWS have sent the email that the rules are under **complaint**

Task 7 : Validation of the Lab

1. Once The Lab Steps Are Completed, Please Click On The **Validation** 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 :

Do You Know ?

AWS Config can be used to audit resources for compliance with a variety of standards, including CIS AWS Foundations Benchmark and HIPAA.

Completion and Conclusion

1. You have successfully created the Config rule along with the SNS topic.
2. Modified the security group by adding custom port to get the alert from AWS regarding change in config rule.
3. Successfully tested the working of config rule.
4. Revert back the changes by removing the ports added to make the rule complaint.
5. Successfully received the email from AWS stating the AWS config rules with non compliant. resources.

End Lab

1. Sign out from the AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps click on **End Lab** from your whizlabs dashboard