UPDATE SECURITY GROUPS AUTOMATICALLY USING AWS LAMBDA

TABLE OF CONTENTS

Table of Contents

PURPOSE

Purpose

The purpose of this training is to have users to get experience with automation of security implementations.

INTENDED AUDIENCE

The intended audience for training is people who are interested in understanding security and compliance in AWS. To be successful, attendees should have some understanding of or experience with:

- AWS Security Groups
- AWS Lambda
- AWS Config

SET UP

Set Up

TRAINING ACCOUNT ACCESS

You should have received an email with credentials to the 1Strategy Training Account. If you haven't received these credentials, send an email to Training@1strategy.com.

LOG INTO THE TRAINING ACCOUNT

Log into the 1strategy training account by using the credentials provided before starting this lab.

Hands-on Instructions

TASK 1: CREATE SECURITY GROUP

In this task you will create a Security Group in the AWS Management Console.

1. Log into the Training AWS account.

2. Ensure that you are located in the **Oregon** region.

3. In the **AWS management Console,** on the **Services** menu, click **EC2**.

4. In the left navigation pane, click **Security Groups**.

5. Click **Create Security Group**, then enter these values:

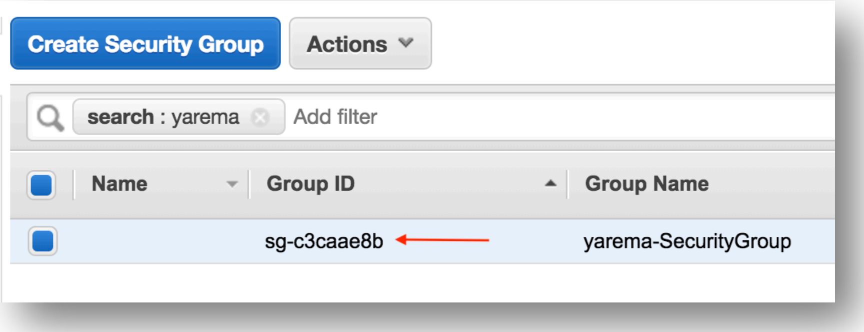
- **Security group name:** <LastName>-SecurityGroup (Replace <LastName> with your actual last name.)

- **Description:** <LastName>-SecurityGroup (Replace <LastName> with your actual last name.)

- **VPC:** Training_VPC

6. Click **Create.**

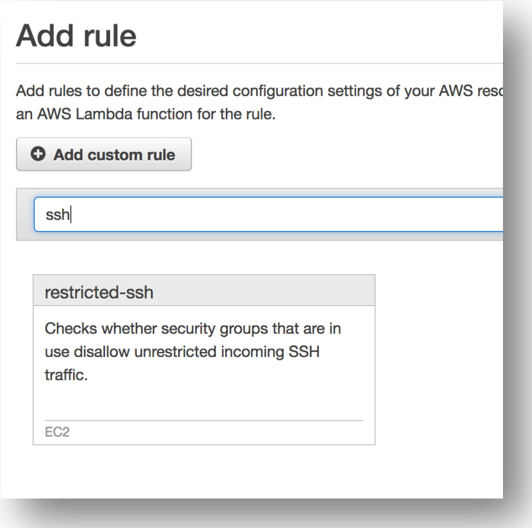
7. Find the Security Group that you created by typing in your last name into the search bar. Take note or copy the Group ID. This ID will be necessary in future steps.



Name	Group ID	Group Name
	sg-c3caae8b	yarema-SecurityGroup

TASK 2: CREATE AN AWS CONFIG RULE.

1. In the **AWS management Console,** on the **Services** menu, click **Config**.
2. In the left navigation pane, click **Rules.** Then click on the **Add Rule** button.
3. Search "ssh" in the filter bar, then select **restricted-ssh** template



Add rule

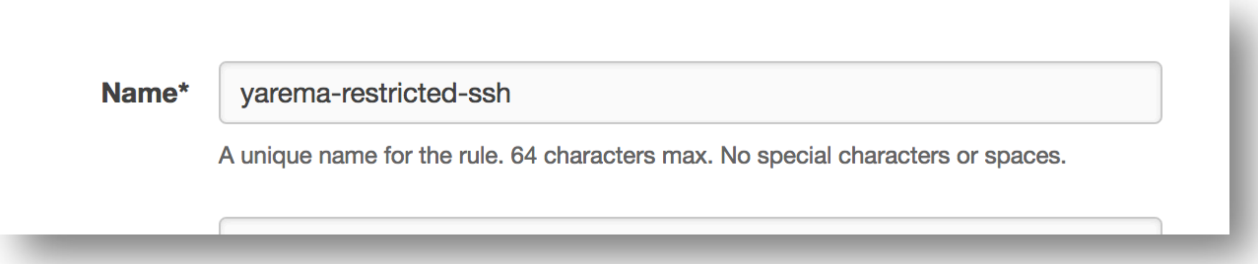
Add rules to define the desired configuration settings of your AWS resc
an AWS Lambda function for the rule.

restricted-ssh

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

EC2

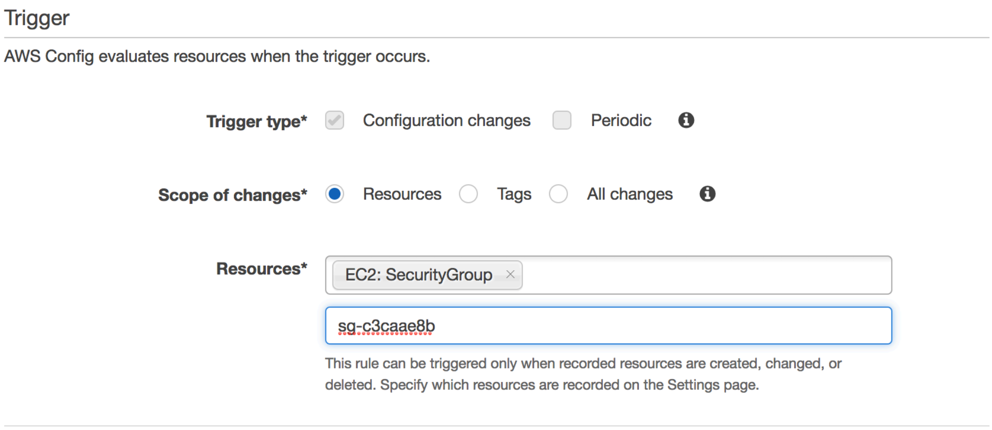
4. Modify the rule name include your last name: <LastName>-restricted-ssh



Name* yarema-restricted-ssh

A unique name for the rule. 64 characters max. No special characters or spaces.

5. Within the **Trigger** section, in the *Resource Identifier* field, place the Security Group ID that was retrieved in Task 1 on step 7.



Trigger

AWS Config evaluates resources when the trigger occurs.

Trigger type* ☑ Configuration changes □ Periodic

Scope of changes* ● Resources ○ Tags ○ All changes

Resources* EC2: SecurityGroup ×

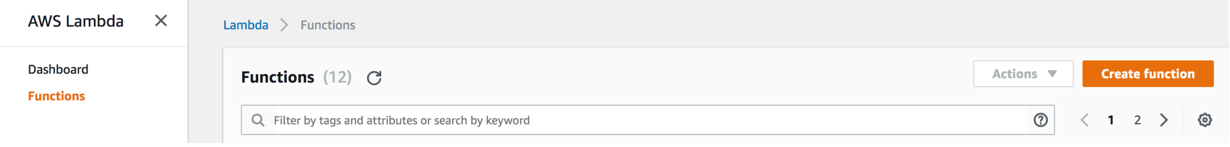
sg-c3caae8b

This rule can be triggered only when recorded resources are created, changed, or deleted. Specify which resources are recorded on the Settings page.

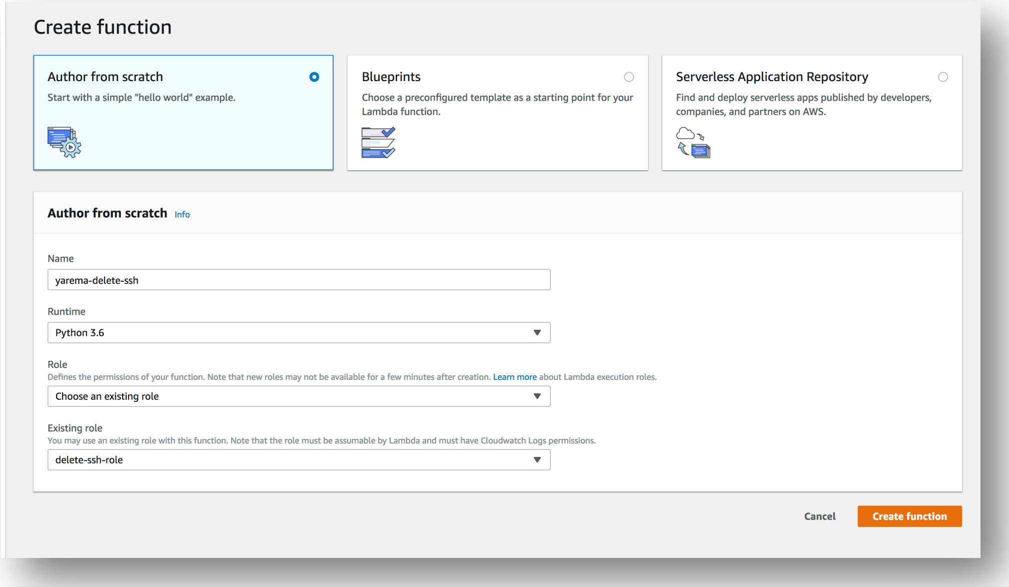
6. Review the rule and then click the **Save** button.

TASK 3: CREATE A LAMBDA FUNCTION

1. 1. In the **AWS management Console,** on the **Services** menu, click **Lambda**.
2. In the left navigation pane, click **Functions.** Then click on the **Create Function** button.



3. For the Name, specify <Last-Name>-delete-ssh. For Runtime, select Python 3.6. Choose an existing role named **delete-ssh-role**. Then click **Create Function.**



Create function

○ Author from scratch
Start with a simple "hello world" example.
○ Blueprints
Choose a preconfigured template as a starting point for your Lambda function.
○ Serverless Application Repository
Find and deploy serverless apps published by developers, companies, and partners on AWS.

Author from scratch Info

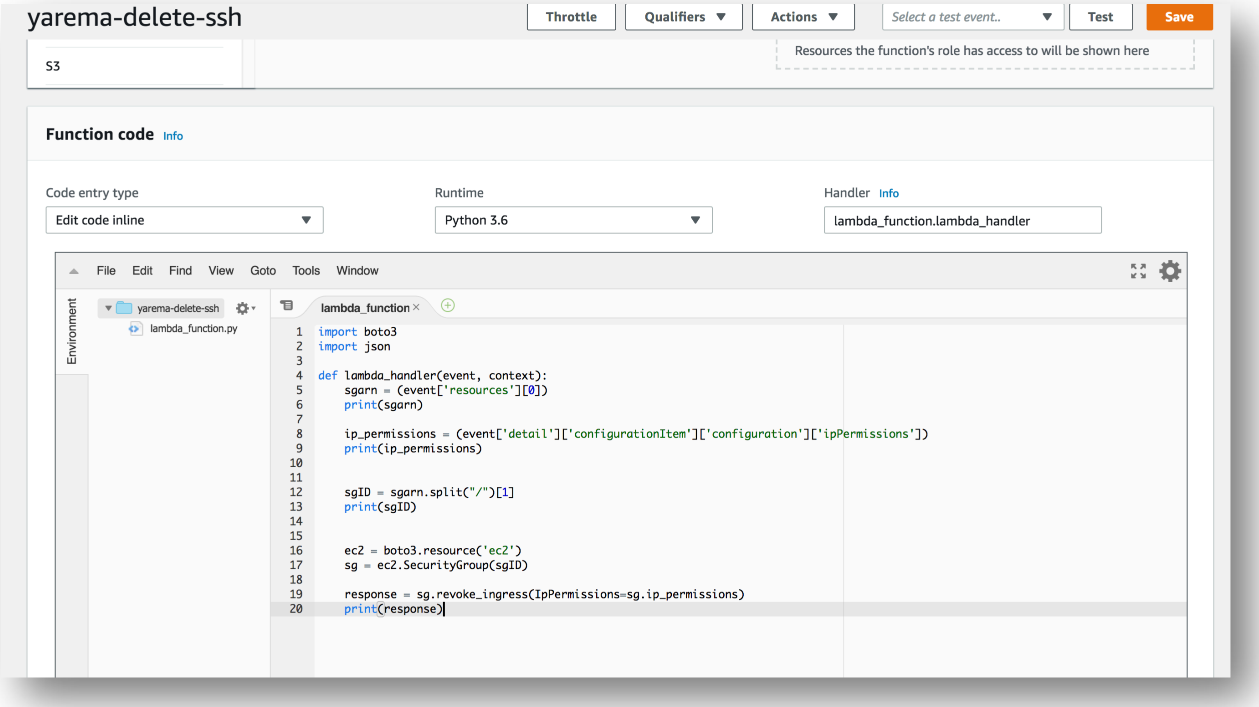
Name
yarema-delete-ssh

Runtime
Python 3.6

Role
Defines the permissions of your function. Note that new roles may not be available for a few minutes after creation. Learn more about Lambda execution roles.
Choose an existing role

Existing role
You may use an existing role with this function. Note that the role must be assumable by Lambda and must have Cloudwatch Logs permissions.
delete-ssh-role

4. Copy and paste the sample Python code from here into the inline code editor and then click **Save**



yarema-delete-ssh

Resources the function's role has access to will be shown here

Function code Info

Code entry type
Edit code inline

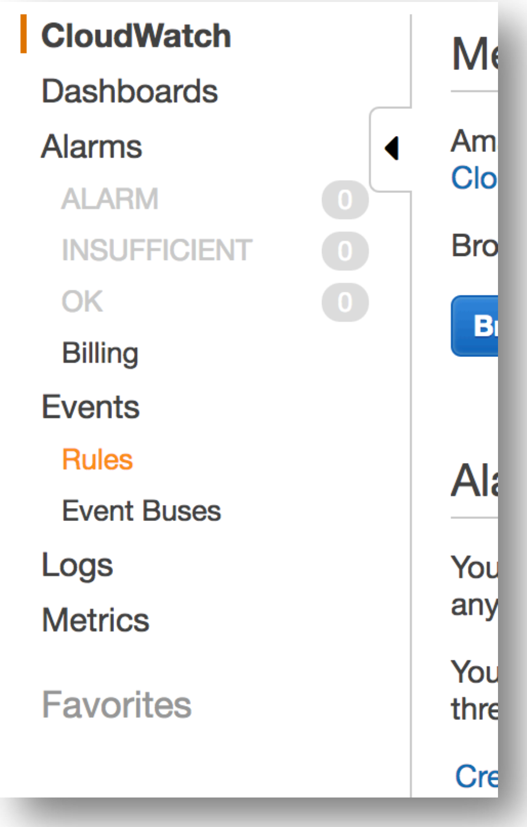
Runtime
Python 3.6

Handler Info
lambda_function.lambda_handler

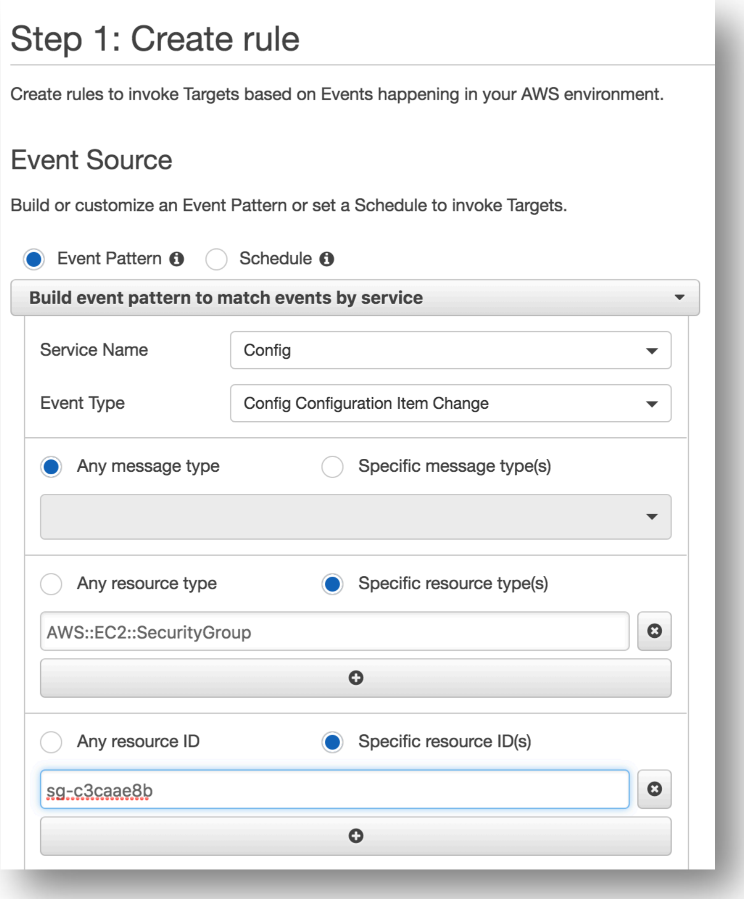
```python
import boto3
import json

def lambda_handler(event, context):
    sgarn = (event['resources'][0])
    print(sgarn)

    ip_permissions = (event['detail']['configurationItem']['configuration']['ipPermissions'])
    print(ip_permissions)


    sgID = sgarn.split("/")[1]
    print(sgID)


    ec2 = boto3.resource('ec2')
    sg = ec2.SecurityGroup(sgID)

    response = sg.revoke_ingress(IpPermissions=sg.ip_permissions)
    print(response)
```

TASK 4: CREATE A CLOUDWATCH EVENT

1. In the **AWS management Console,** on the **Services** menu, click **CloudWatch**.
2. In the left navigation pane, click **Rules.** Then click on the **Create Rule** button.



3. Configure the rule with the following changes:
   a. Select **Event Pattern.**
   b. For Service Name, select **Config.**
   c. Select the Event Type to be **Config Configuration Item Change**.
   d. Select **Specific resource type(s)** instead of "All resource type", and then input the **AWS::EC2::SecurityGroup** value into the text box.
   e. Select **Specific resource ID(s)** instead of "Any resource ID", and then input your security group id that was retrieved in Task 1 on step 7 into the text box.



Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event Pattern ○ Schedule

Build event pattern to match events by service

Service Name: Config

Event Type: Config Configuration Item Change

● Any message type ○ Specific message type(s)

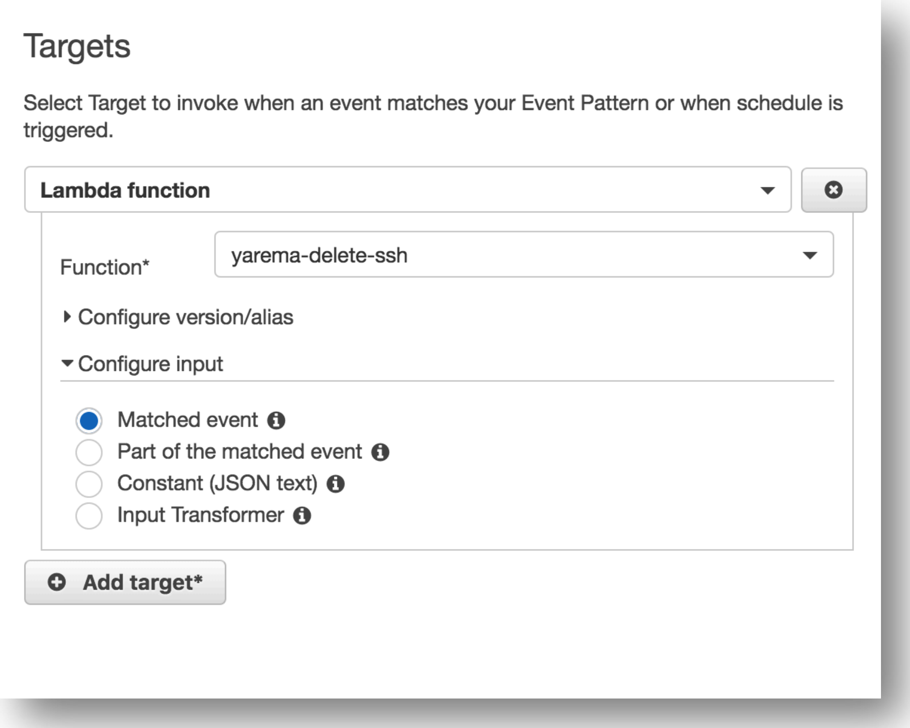
○ Any resource type ● Specific resource type(s)

AWS::EC2::SecurityGroup

○ Any resource ID ● Specific resource ID(s)

sg-c3caae8b

4. In the **Targets** section, click **Add Target**. Ensure that the target type is **Lambda Function.** Select the name of the lambda function that you created in Step 3**.** In the Configure Input section, ensure that **Matched event** is selected
5. Review the details and then select **Configure Details** button.



Targets

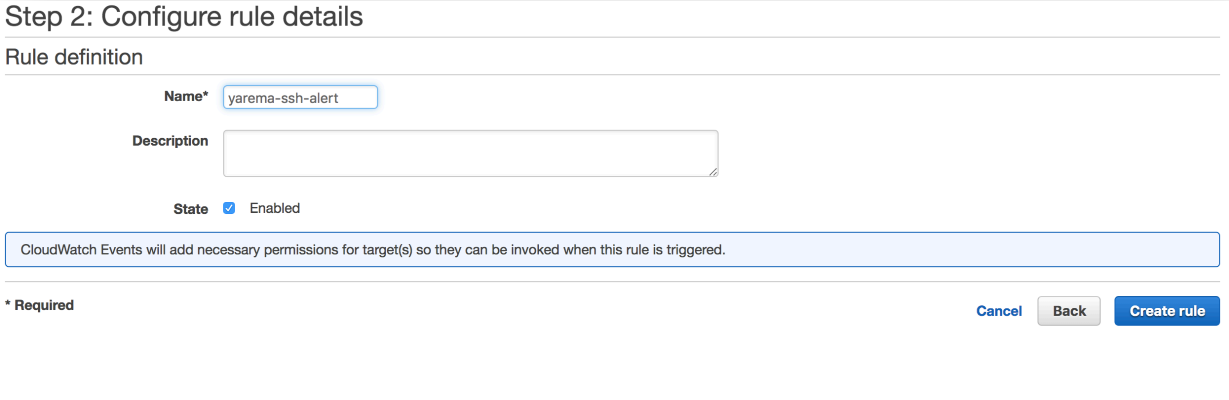
Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

Lambda function

Function* yarema-delete-ssh

● Matched event
○ Part of the matched event
○ Constant (JSON text)
○ Input Transformer

6. Specify a name for the CloudWatch event rule. <LastName>-ssh-alert. And then select **Create rule** button.



Step 2: Configure rule details

Rule definition

Name* yarema-ssh-alert

Description

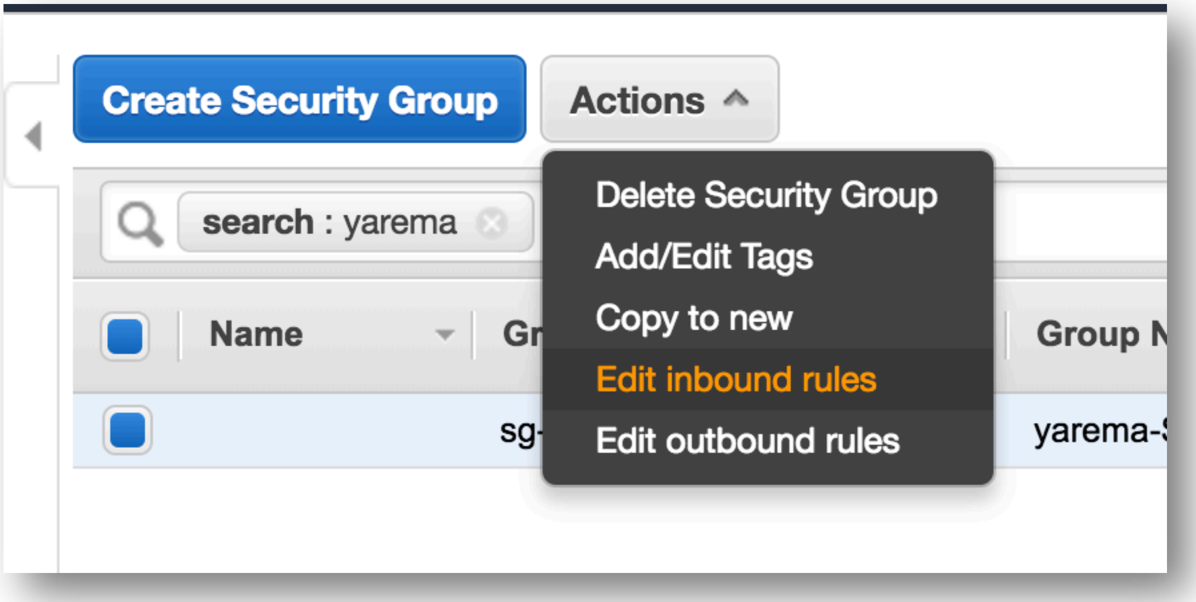
State ☑ Enabled

CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.

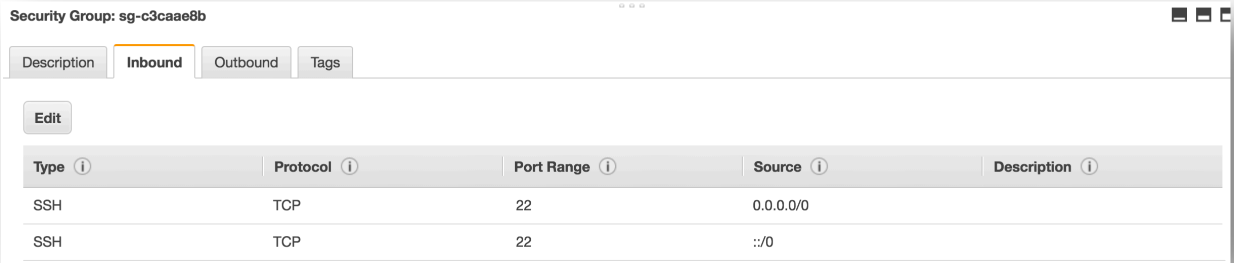
* Required

TASK 5: TEST RULE

1. In the **AWS management Console,** on the **Services** menu, click **EC2**.
2. In the left navigation pane, click **Security Groups**.
3. Search and Find your security group that was created in Task 1.
4. Select the security group that was created in Task 1. Click **Actions** and select **Edit Inbound Rules**.



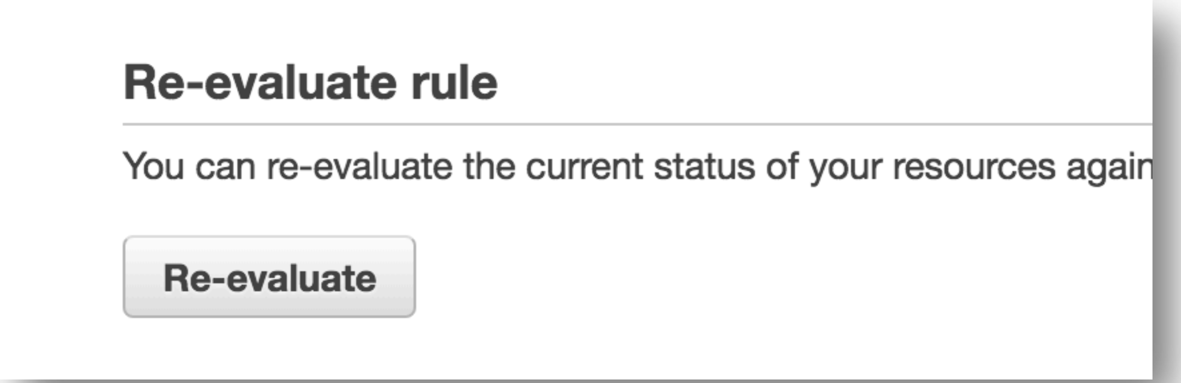
5. Select the type to be **SSH.** Ensure that the Protocol is set to **TCP** and the port range is **22**. For source, select **Anywhere**. Then click **Save.**
6. With your security group selected, click on the **Inbound** tab and you will see your inbound rules.



Security Group: sg-c3caae8b

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
SSH	TCP	22	::/0	

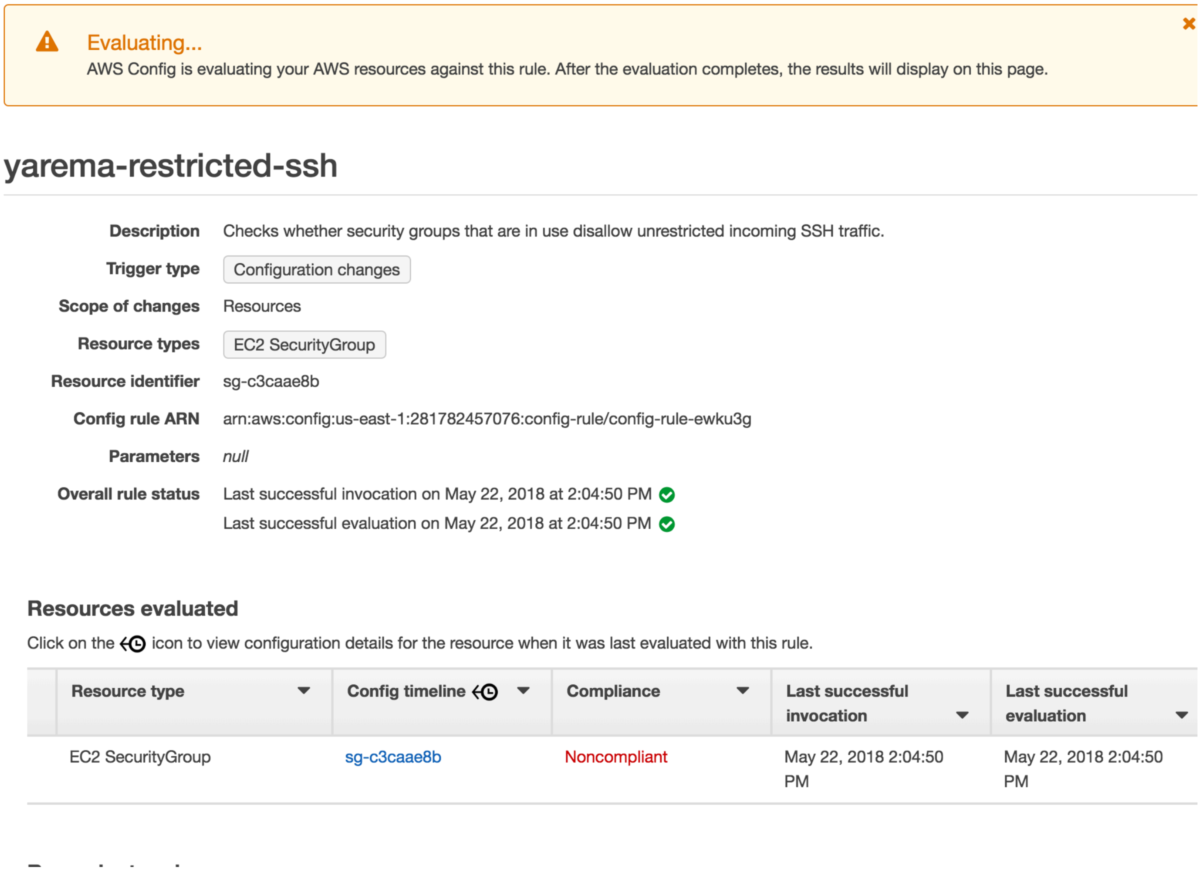
7. In the **AWS management Console,** on the **Services** menu, click **Config**.
8. In the left navigation pane, click **Rules.** Then select your Confg rule that was created in Step 2.
9. In the **Re-evaluate Rule** section, click the **Re-evaluate** button.



Re-evaluate rule

You can re-evaluate the current status of your resources agair

10. Refresh the page, and you will see that your security group rule is being evaluated.



Evaluating...
AWS Config is evaluating your AWS resources against this rule. After the evaluation completes, the results will display on this page.

yarema-restricted-ssh

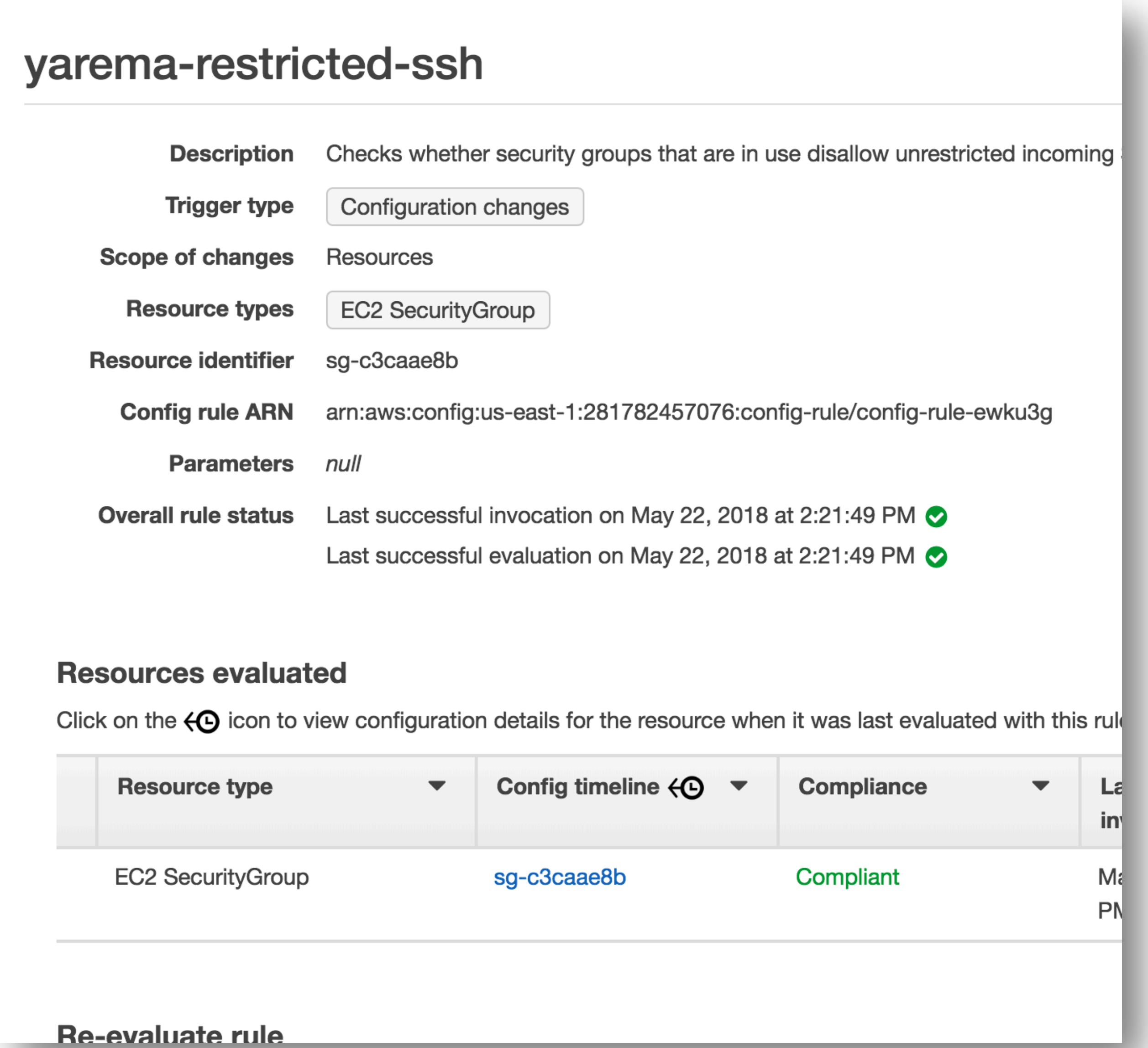
Description	Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.
Trigger type	Configuration changes
Scope of changes	Resources
Resource types	EC2 SecurityGroup
Resource identifier	sg-c3caae8b
Config rule ARN	arn:aws:config:us-east-1:281782457076:config-rule/config-rule-ewku3g
Parameters	*null*
Overall rule status	Last successful invocation on May 22, 2018 at 2:04:50 PM ✓ Last successful evaluation on May 22, 2018 at 2:04:50 PM ✓

Resources evaluated

Click on the icon to view configuration details for the resource when it was last evaluated with this rule.

Resource type	Config timeline	Compliance	Last successful invocation	Last successful evaluation
EC2 SecurityGroup	sg-c3caae8b	Noncompliant	May 22, 2018 2:04:50 PM	May 22, 2018 2:04:50 PM

11. Refresh the page again and you will notice that the "Evaluating" notice disappears. Surprisingly, the security group is compliant! But why? Let's proceed to the next step to figure out why Config rule says it is in compliant when we created unrestricted ssh access in step 6.



yarema-restricted-ssh

Description	Checks whether security groups that are in use disallow unrestricted incoming
Trigger type	Configuration changes
Scope of changes	Resources
Resource types	EC2 SecurityGroup
Resource identifier	sg-c3caae8b
Config rule ARN	arn:aws:config:us-east-1:281782457076:config-rule/config-rule-ewku3g
Parameters	*null*
Overall rule status	Last successful invocation on May 22, 2018 at 2:21:49 PM ✓ Last successful evaluation on May 22, 2018 at 2:21:49 PM ✓

Resources evaluated

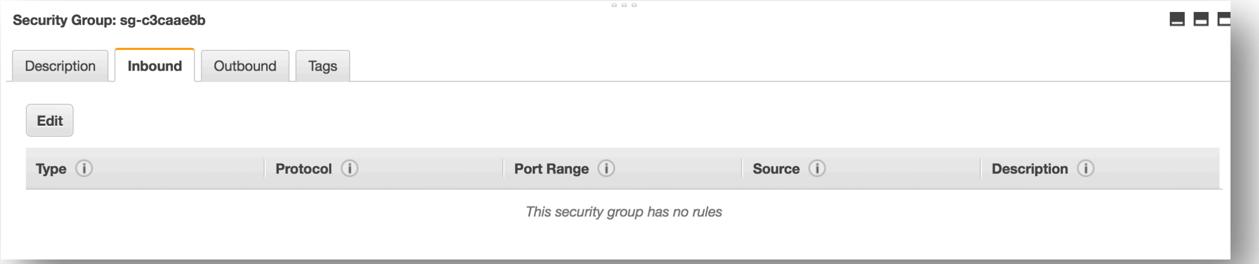
Click on the icon to view configuration details for the resource when it was last evaluated with this rul

Resource type	Config timeline	Compliance	La in
EC2 SecurityGroup	sg-c3caae8b	Compliant	Ma PM

Re-evaluate rule

12. In the **AWS management Console,** on the **Services** menu, click **EC2.**
13. In the left navigation pane, click **Security Groups**.
14. Search and Find your security group that was created in Task 1
15. Select the security group that was created in Task 1. Click **Inbound** tab.

16. Notice that security inbound rule is deleted. This was deleted automatically by the Lambda function triggered by the CloudWatch Event Rule which itself was triggered by the Config Rule noticing that the security group was "non-compliant".



Security Group: sg-c3caae8b

Type	Protocol	Port Range	Source	Description

This security group has no rules

PREPARED BY

Prepared By

PAVEL YAREMA
AWS SOLUTIONS ARCHITECT

pavel@1strategy.com

Company Information

1Strategy
3025 112th Ave SE #200

Bellevue, WA 98004

www.1strategy.com