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

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:

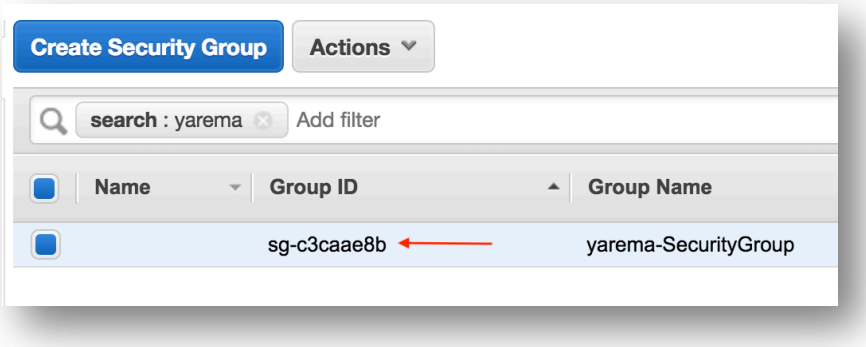
- **Security group name:** <LastName>-SecurityGroup (Replace <LastName> with your actual last name.)

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

- **VPC:** Training_VPC

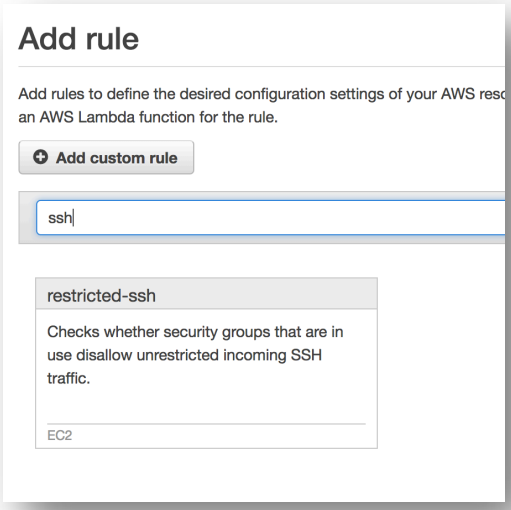
6. Click **Create.**

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.

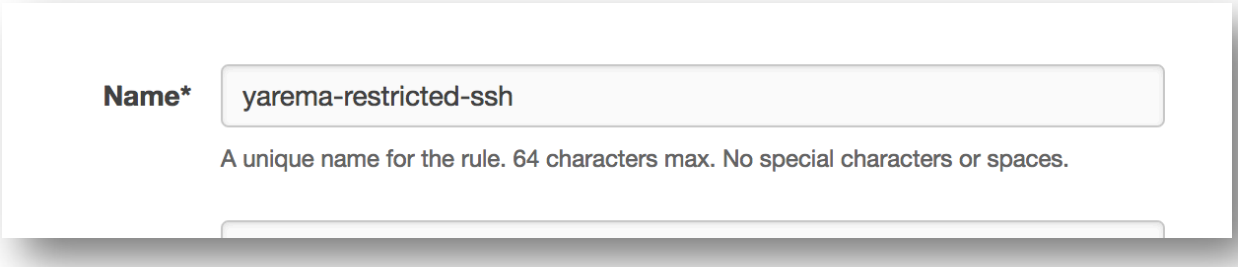


TASK 2: CREATE AN AWS CONFIG RULE.

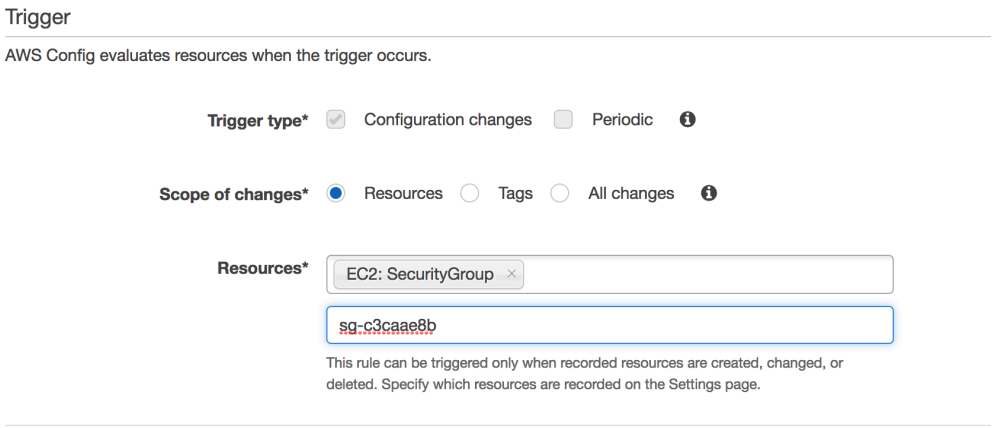
1. In the **AWS management Console,** on the **Services** menu, click **Config**.
2. In the left navigation pane, click **Rules**. Then click on the **Add Rule** button.
3. Search "ssh" in the filter bar, then select **restricted-ssh** template



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



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

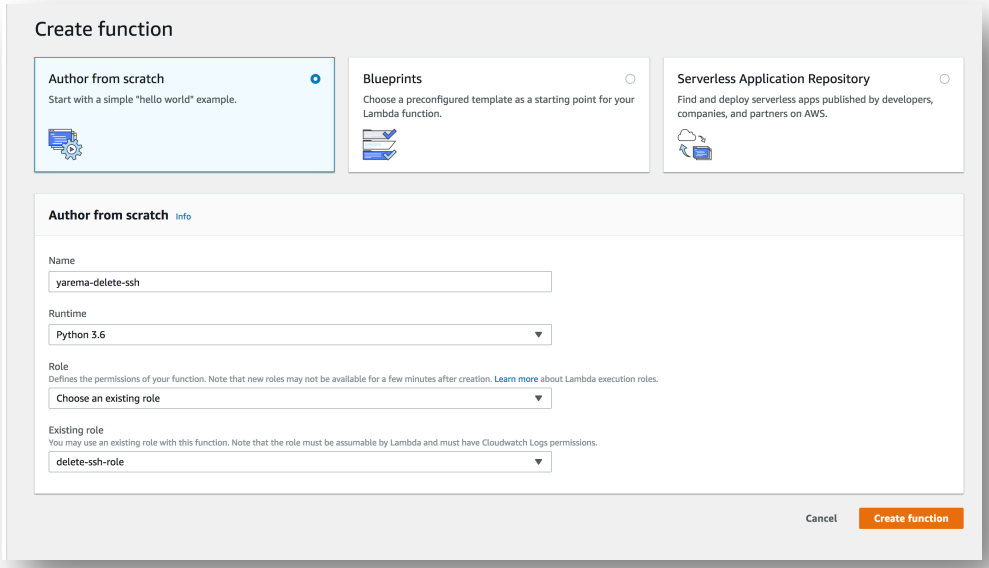


6. Review the rule and then click the **Save** button.

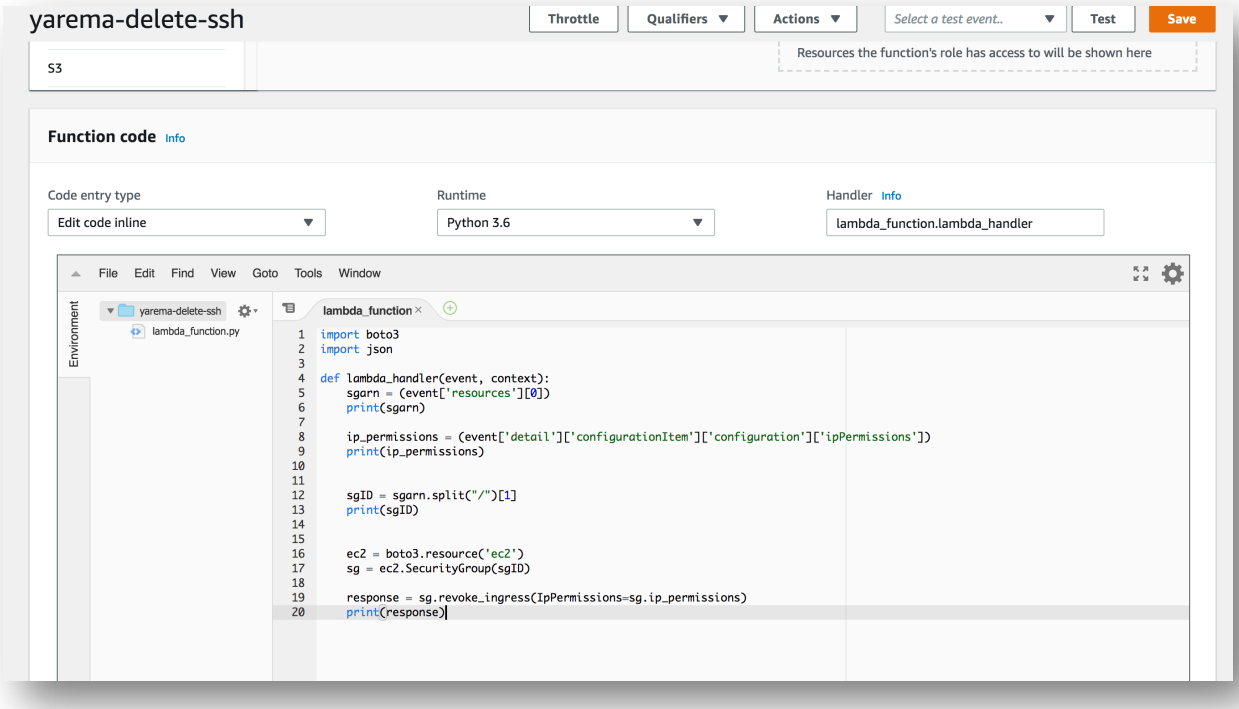
TASK 3: CREATE A LAMBDA FUNCTION

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.**

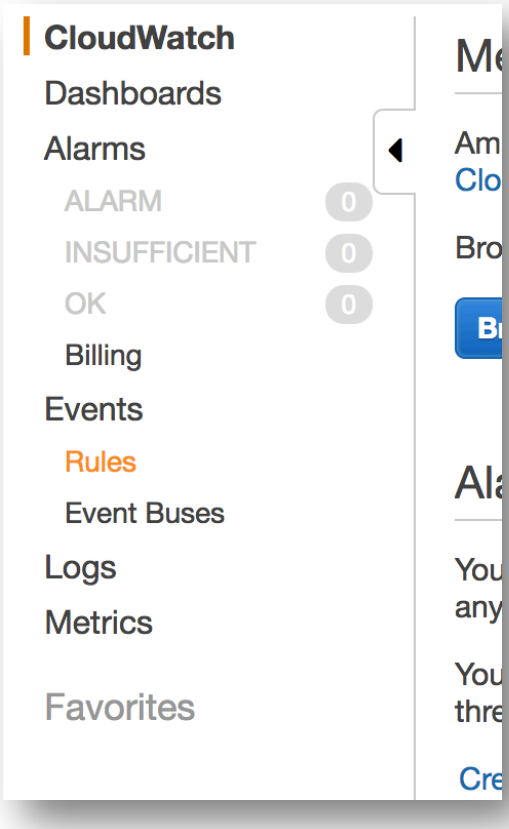


4. Copy and paste the sample Python code from url below into the inline code editor and then click **Save.** (URL**:** https://github.com/1Strategy/lambda-update-security-group/blob/master/delete_ssh.py)

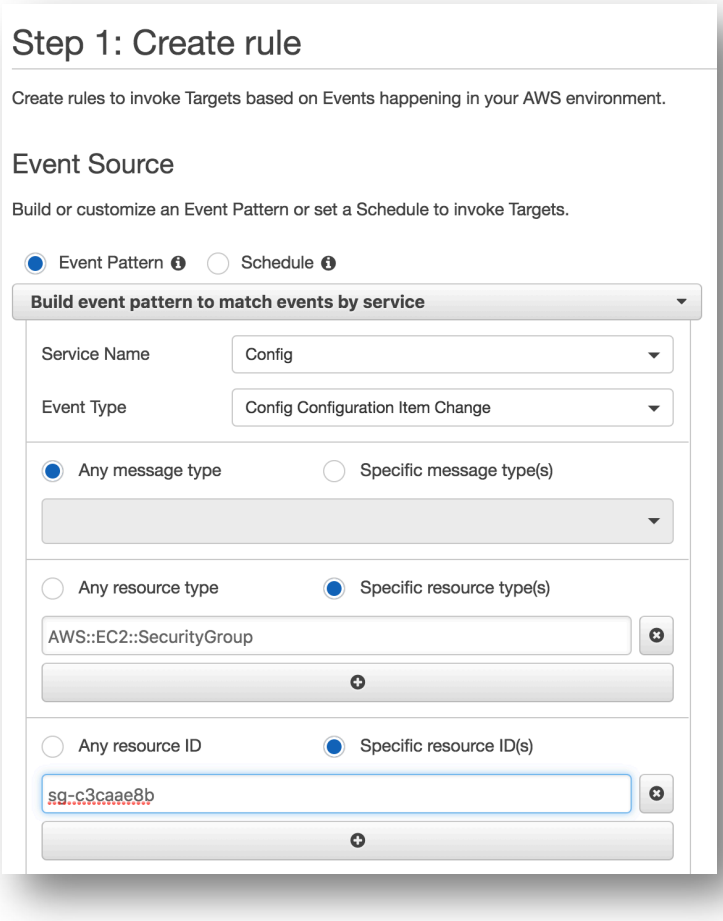


TASK 4: CREATE A CLOUDWATCH EVENT

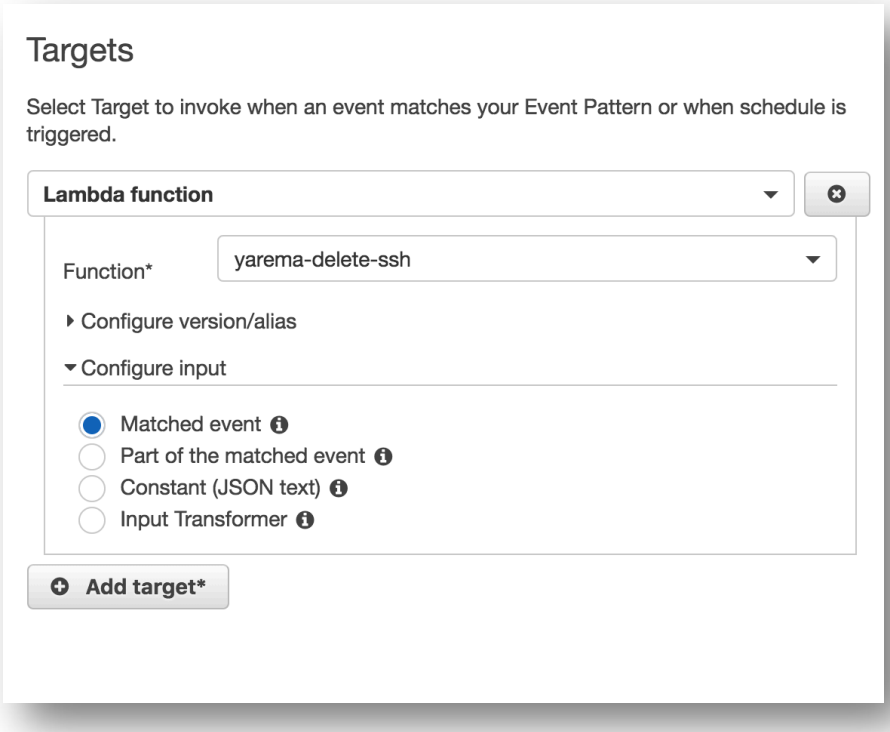
1. In the **AWS management Console,** on the **Services** menu, click **CloudWatch**.
2. In the left navigation pane, click **Rules**. Then click on the **Create Rule** button.



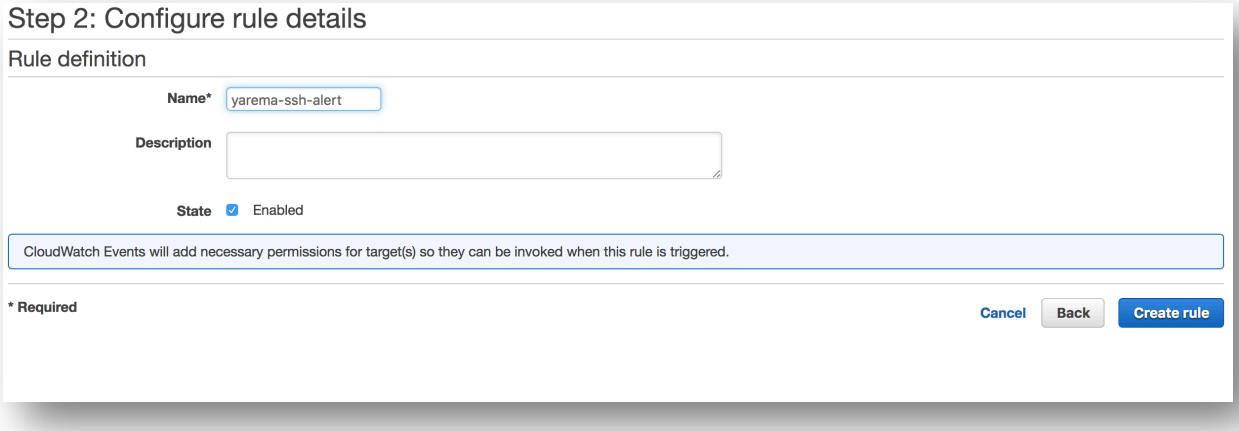
3. Configure the rule with the following changes:
    a. Select **Event Pattern**.
    b. For Service Name, select **Config**.
    c. Select the Event Type to be **Config Configuration Item Change**.
    d. Select **Specific resource type(s)** instead of "All resource type", and then input the **AWS::EC2::SecurityGroup** 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.



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.

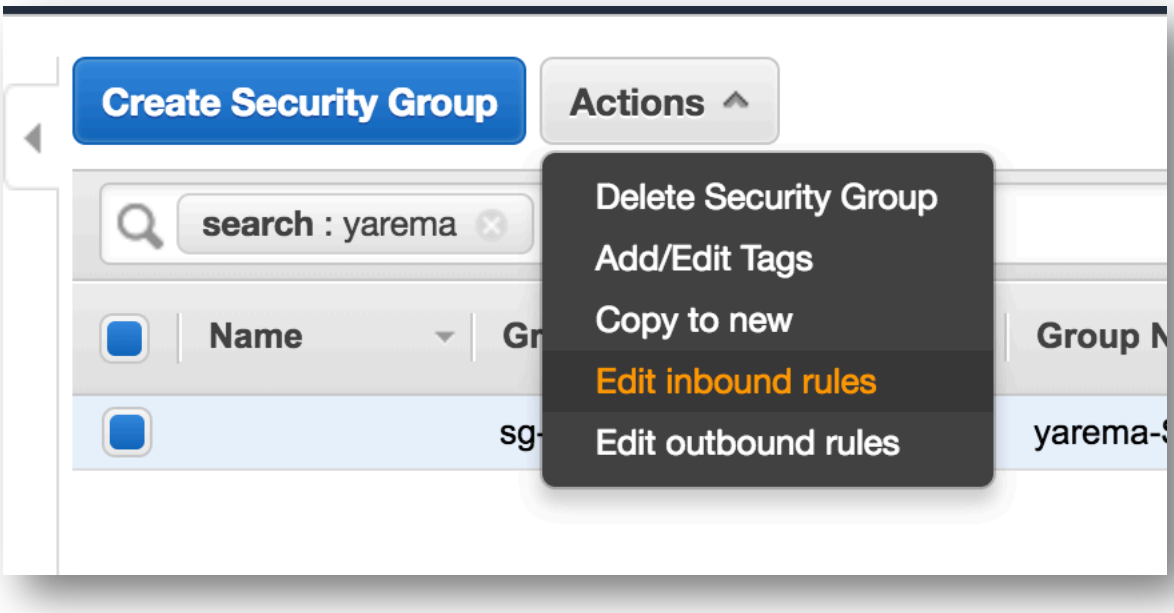


6. Specify a name for the CloudWatch event rule. <LastName>-ssh-alert. And then select **Create rule** button.

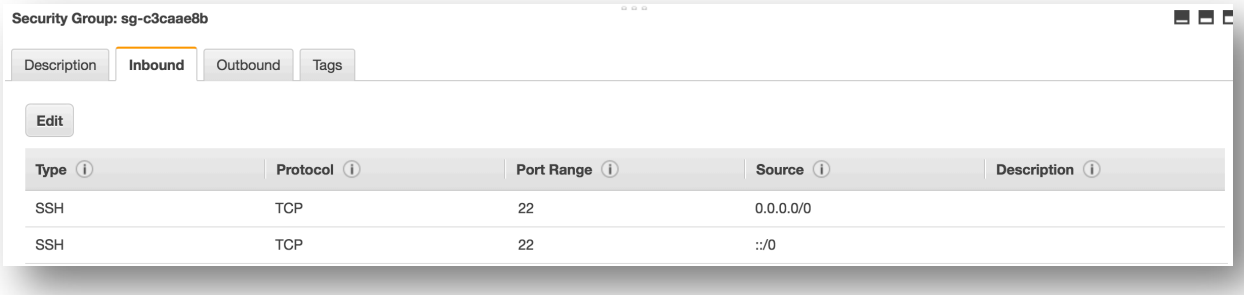


TASK 5: TEST RULE

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**.

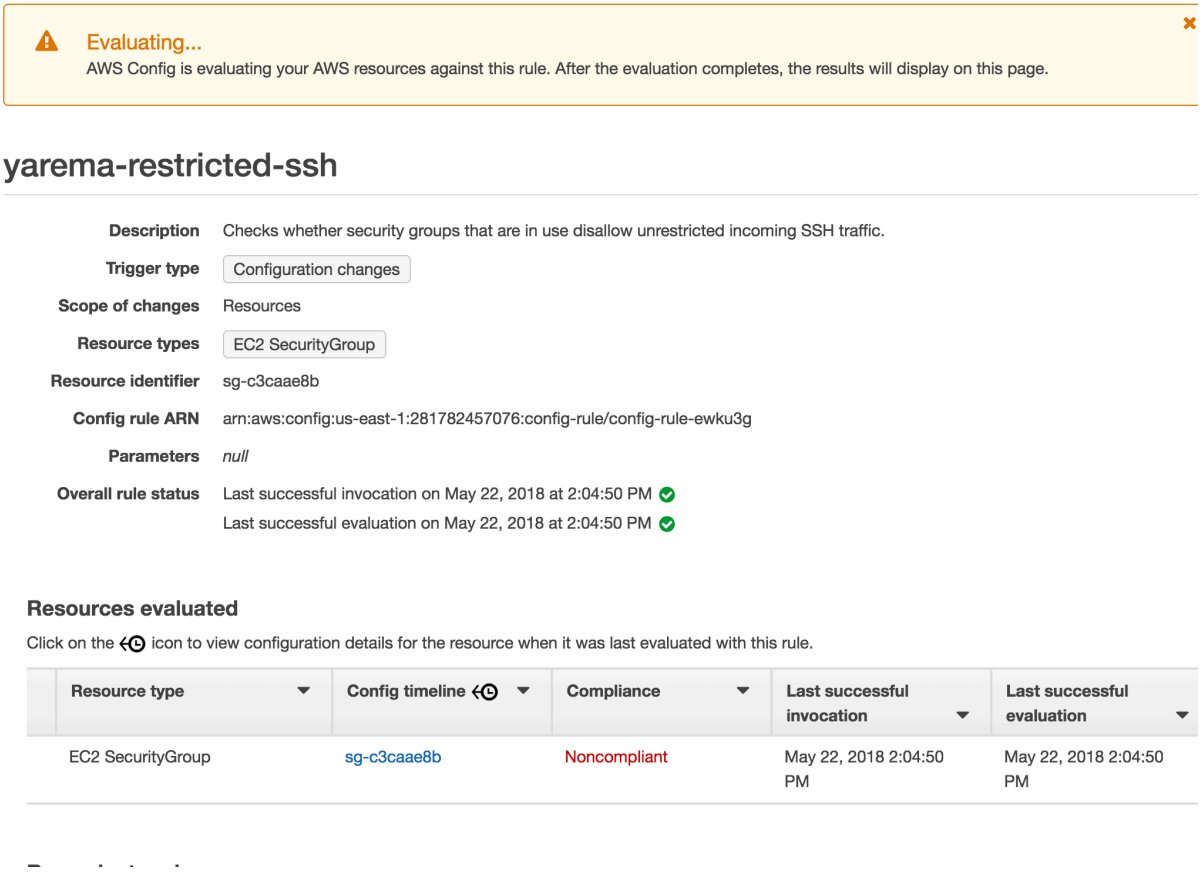


5. Select the type to be **SSH.** Ensure that the Protocol is set to **TCP** and the port range is **22**. For source, select **Anywhere**. Then click **Save.**
6. With your security group selected, click on the **Inbound** tab and you will see your inbound rules.

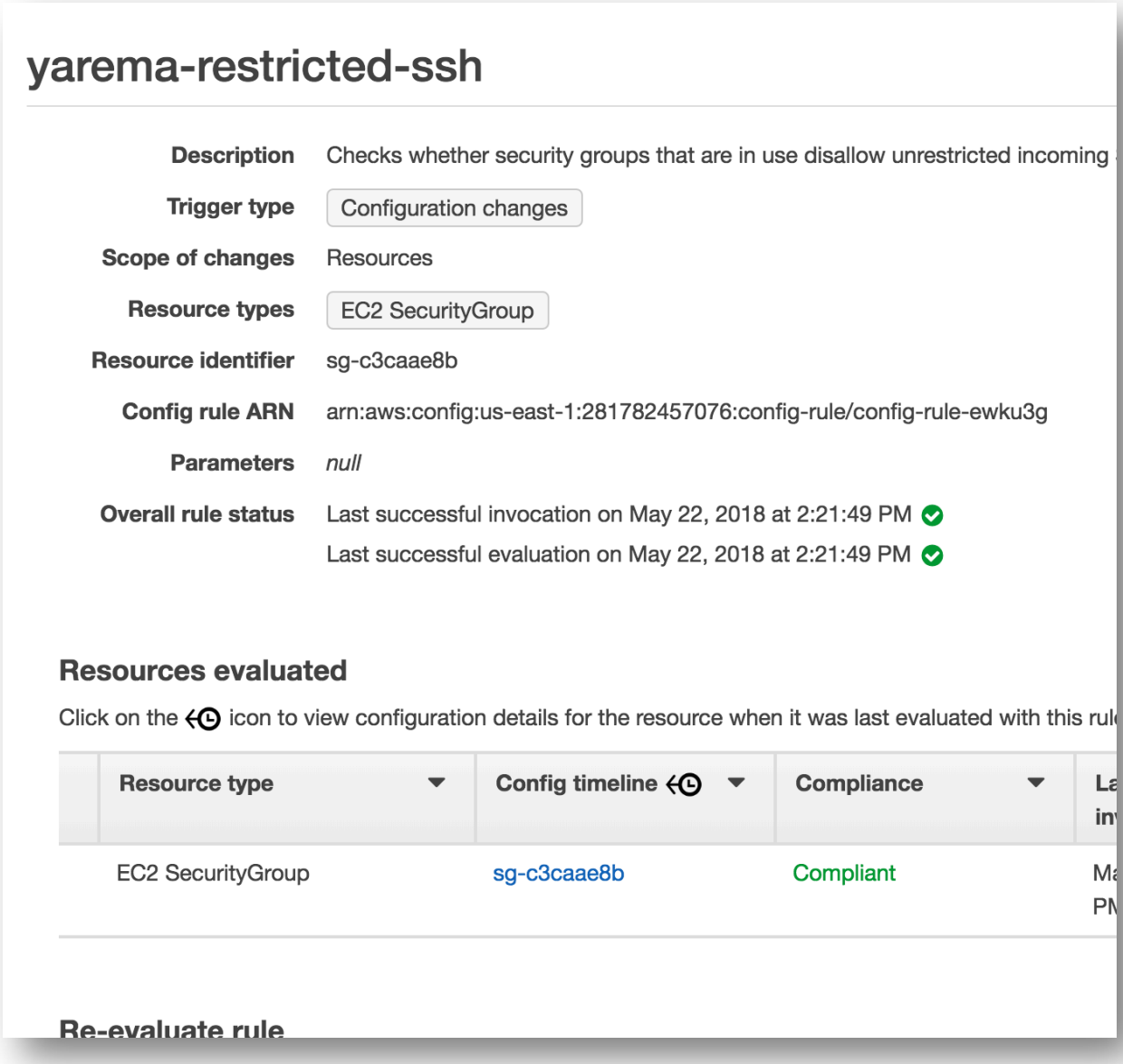


7. In the **AWS management Console,** on the **Services** menu, click **Config**.
8. In the left navigation pane, click **Rules**. Then select your Confg rule that was created in Step 2.
9. In the **Re-evaluate Rule** section, click the **Re-evaluate** button.

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

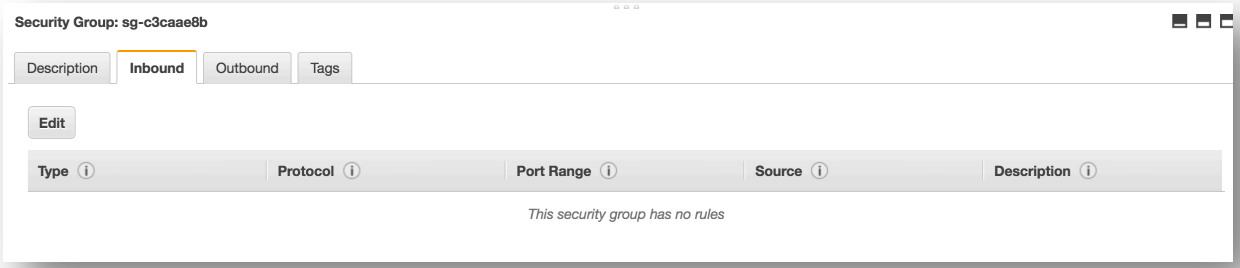


11. Refresh the page again and you will notice that the "Evaluating" notice disappears. Surprisingly, the security group is compliant! But why? Let's proceed to the next step to figure out why Config rule says it is in compliant when we created unrestricted ssh access in step 6.



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”.



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