**Working with AWS Config Managed Rules**

### Introduction

Now that the configuration recorder has started, you can start to enable Config Rules. In this lab step, you will use an AWS managed rule to quickly start checking compliance. There are many managed rules provided by AWS. You should be familiar with the managed rules that are available to you since they cover many common use cases. They also don't require custom development and maintenance on your part, which can't be said for custom rules. You will work with a managed rule that checks for specific tags being set on EC2 security group resources.

### Instructions

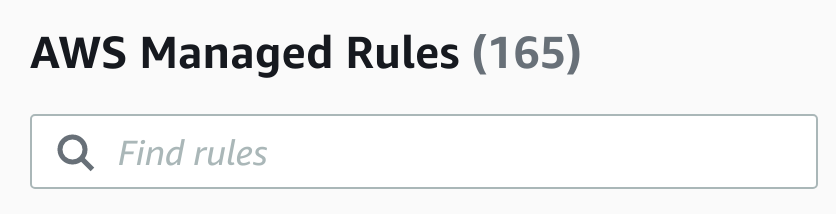
1. Click **Rules** in the AWS Config navigation panel on the left(not the one under **Aggregators**).

2. On the right-hand side, click **Add rule**:

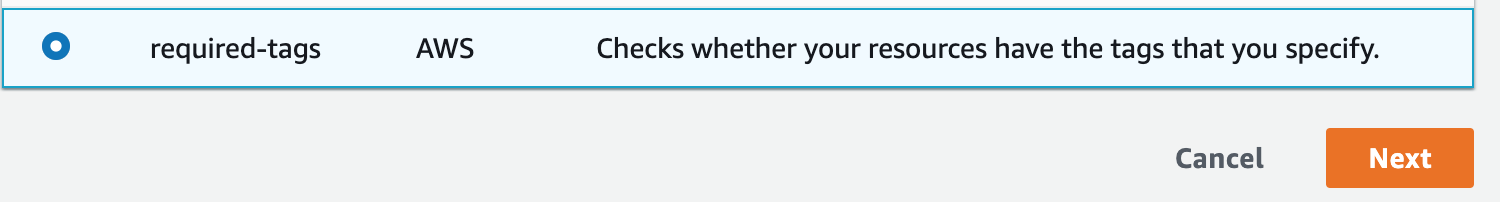


You are presented with a list of AWS managed rules. Take a moment to see the types of rules available in the list.

3. In the **Find rules** text-box, enter required-tags:



4. Select the **required-tags** rule, and click on **Next**:



The **required-tags**rule can check that resources have specific tags that you require. For this lab, imagine you are building out a blue-green deployment environment. Blue-green deployments maintain two copies of the deployment environment, a blue environment, and a green environment. As part of governing your environments, you require all resources to have a Deployment tag that identifies if it is part of the blue environment or the green environment.

5. In the **Configure rule**form, keep the default values for **Name**,**Description**, and **Scope of changes**fields.

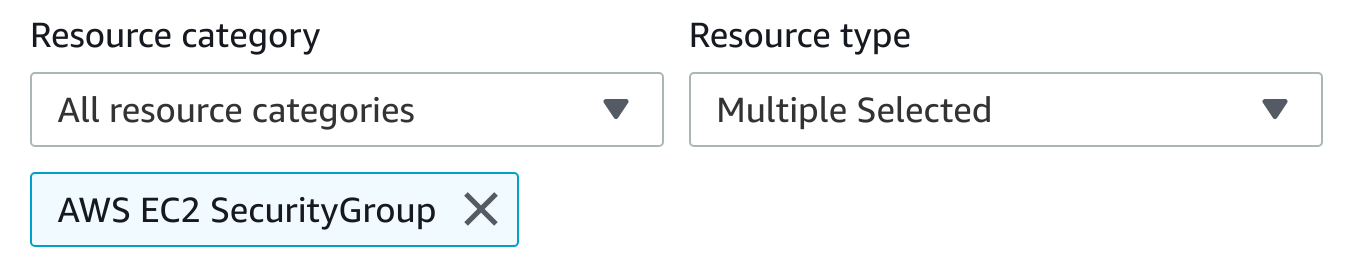
Notice that the **Trigger type** is set to **When configuration changes**. This means the rule will evaluate any time the configuration recorder records a new configuration. The **Resources** **Scope of changes** allows you to select a subset of all the resources being recorded by AWS Config.

6. Move on the **Resources** list and delete all the selected resources to clear the list.

For the sake of limiting the scope of this lab, you will only focus on EC2 Security Groups.

7. To quickly clear all the pre-selected resource types, change the **Resource category** drop-down to **AWS resources** and then back to **All resource categories**.

8. In the **Resource type** box, enter ec2 and select **SecurityGroup** from the drop-down menu:



9. In the **Parameters**section at the bottom of the form, enter:

* **tag1Key**: Deployment
* **tag1Value**: Blue, Green



The key is required, while the value(s) is optional. When the value is specified, the tag must have one of the specified values. Multiple values are separated by commas. If no value is specified, the rule only checks if the tag is set with no specific criteria for the tag value.

10. Click **Next** and then **Add rule** to create the rule and have AWS Config automatically start evaluating the rule on the resources.

It can take a minute for the evaluation to complete.

### Summary

In this lab step, you set up an AWS Config managed rule. The rule checks resource compliance when using a specific tag and allowable values. This type of rule can be useful for many scenarios including the deployment governance scenario utilized in this lab.

VALIDATION CHECKS

**1Checks**

Check again

**The Configuration Rule Has been Created**

Check that the configuration rule has been created

AWS Config