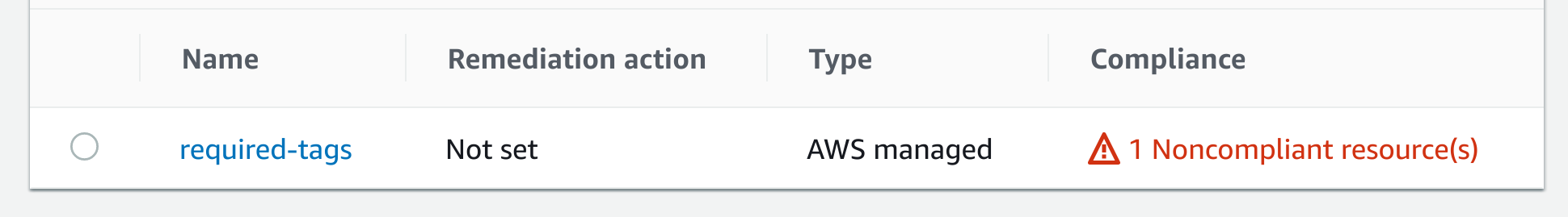
**Analyzing and Remedying a Noncompliant Resource**

### Introduction

The Cloud Academy lab environment created an EC2 security group during the startup routine. Recall that the configuration recorder is recording only security group configurations. The security group is not compliant with the managed rule you previously set up. In this Lab Step, you will learn to analyze noncompliant resources using AWS Config and use its integration with CloudTrail to review associated API calls. After analyzing, you will adjust the security group configuration and verify it is compliant.

### Instructions

1. On the AWS Config **Rules** page, observe that it found **1 Noncompliant resource(s)**after rule evaluation:

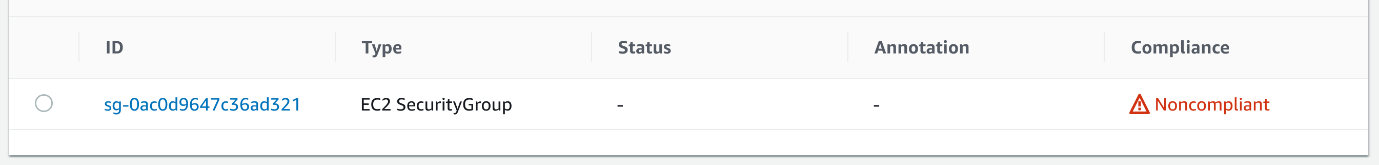


Note: To refresh the **Rules** page, refresh the page using your web browser. The managed rule can take about a minute to finish evaluating.

2. Click on **required-tags**in the **Name** column.

This will open the rule details view for the **required-tags** rule. In the top section, you will see all of the settings you configured when adding the rule.

3. Scroll down to the **Resources in scope**section:

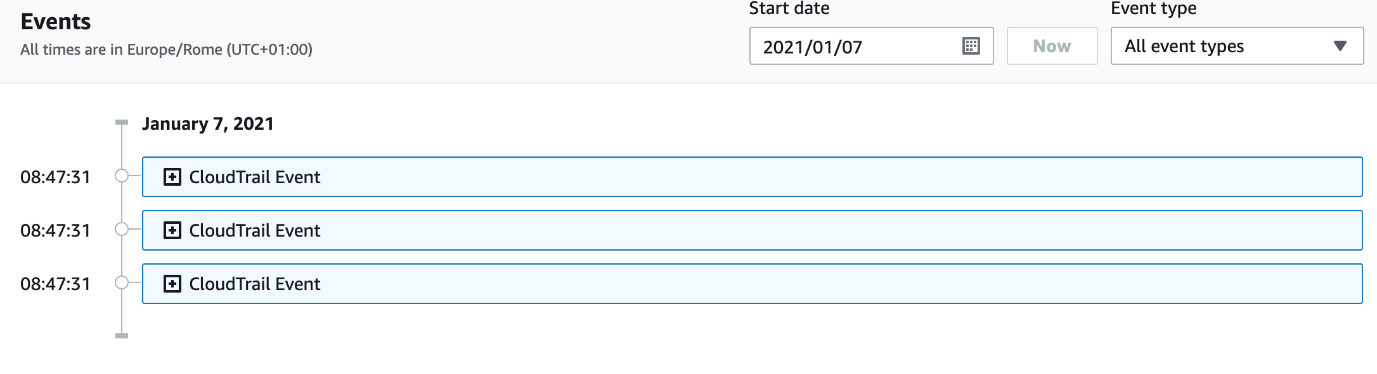


Here you will find a summary of all the resources evaluated against your rules. You will see it evaluated an **EC2 Security Group**and it is **Noncompliant** with your rules.

4. Click on the resource, and, on the right, click on **Resource timeline**:



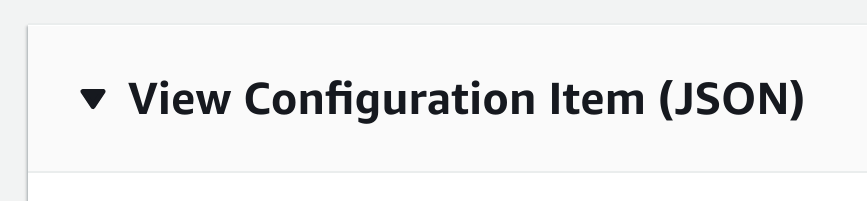
You will see a panel listing **Events**:



Note: You can periodically refresh your browser tab to refresh the timeline in case you don't see any **Events**under the configuration item in the timeline.

Note: Ensure the **Event type** drop-down is set to **All event types** to ensure all types of events are shown.

5. Go back to the resource page and expand the **View Configuration Item (JSON)**:



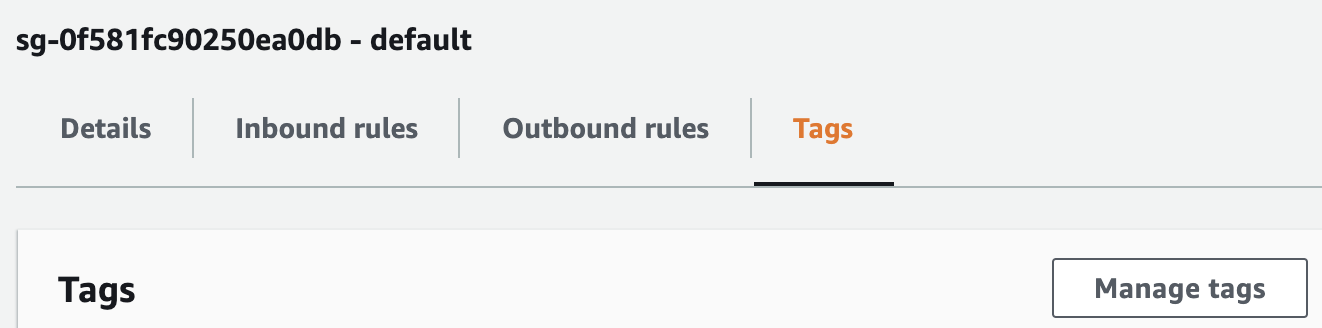
This will open the full configuration. There are many details here that are not in the summary. For example, scroll down and see that the **ipPermissions** that specify the security group ingress and egress permissions are visible.

6. Scroll to the top and click **Manage resource**:



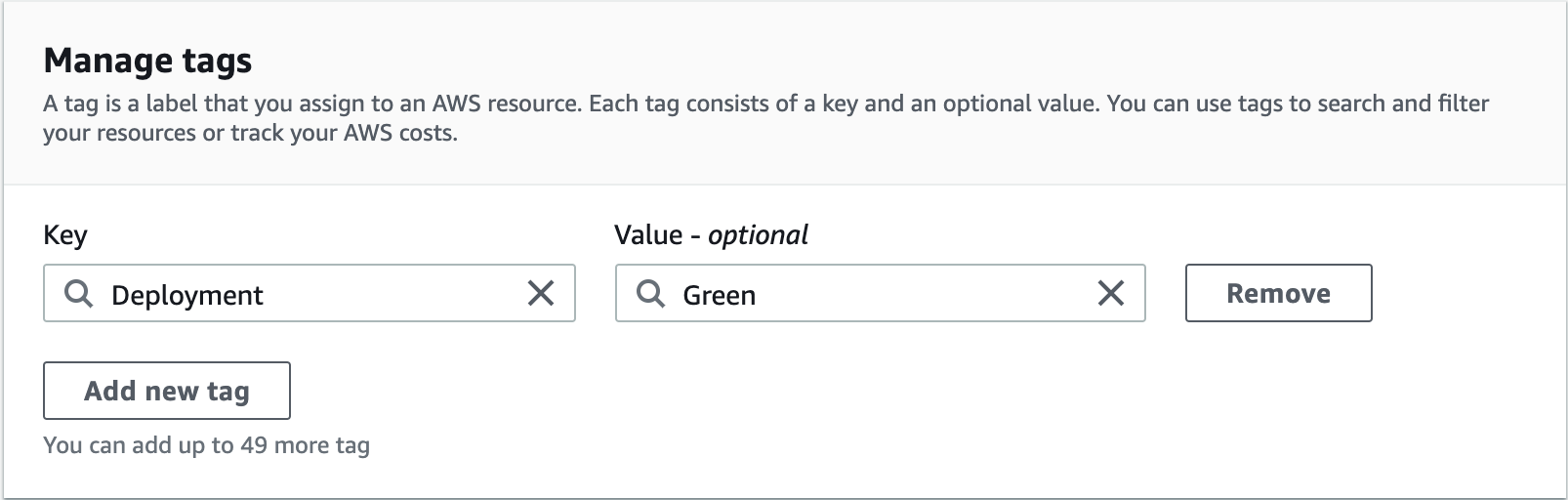
This is a quick way to go to the Management Console page for configuring the resource, which is a security group in this case.

7. On the **Tags** tab, click the **Manage tags** button:



8. In the Manage Tags dialog, click **Add new tag** and enter the following values:

* **Key**: Deployment
* **Value**: Green



This tag makes the security group compliant with the managed rule you enabled.

9. Click **Save changes** and return to the AWS Config browser tab.

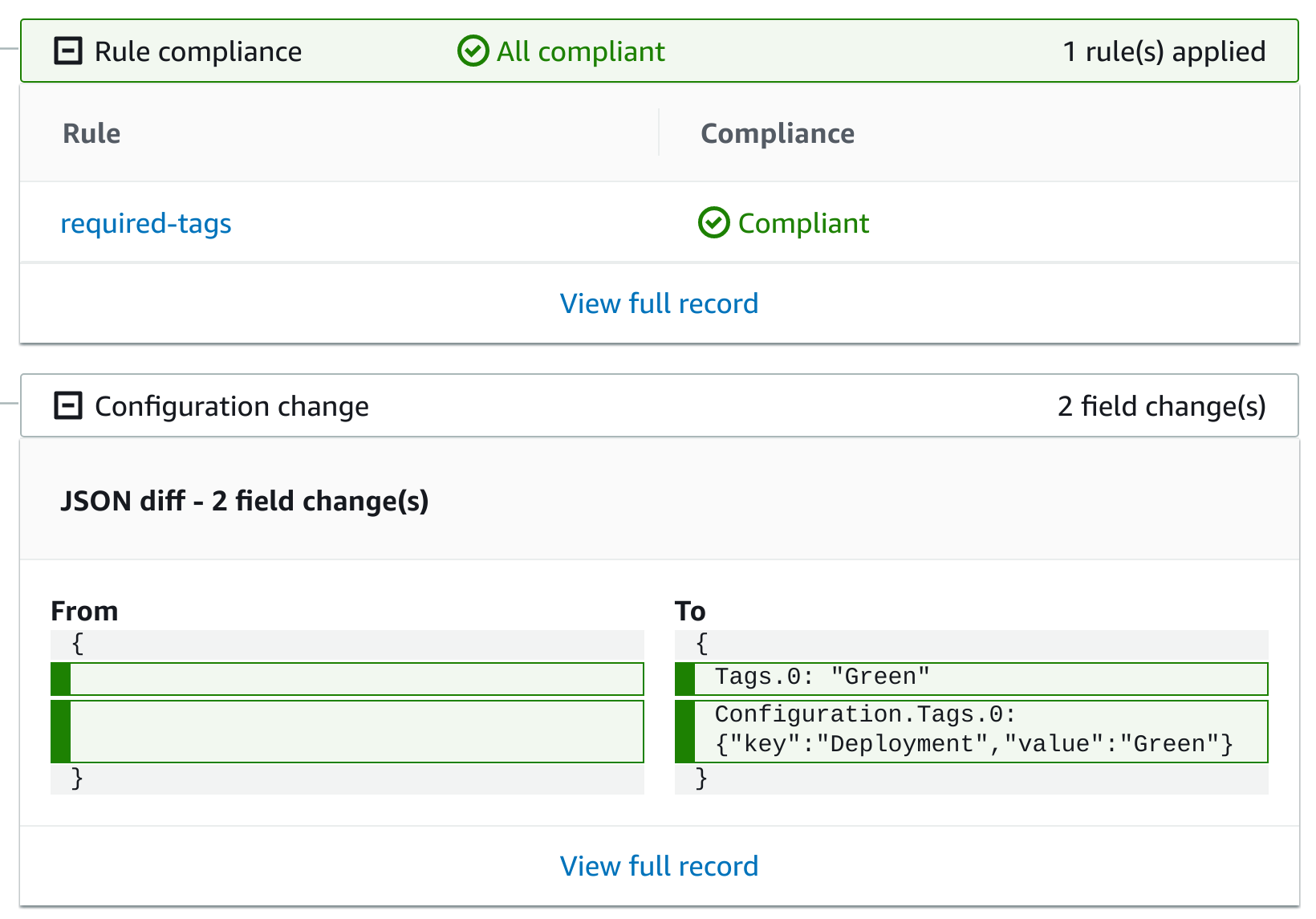
10. Click **Resource Timeline**, and refresh your browser every minute until you see a new configuration item in the timeline.

Note: It can take up to 10 minutes for the configuration change to be recorded. You may want to read ahead in the Lab and return to this step after several minutes. This delay is intrinsic to CloudTrail and cannot be accelerated.

Notice the new item has a **Change** and an **Event**. The **Configuration Details** also include the **Deployment:Green** tag now:

Notice the two latest events:

* A **Configuration change** event, showing that the deployment tag was added to the security group
* A **Rule compliance** event, showing that all resources are now compliant with this rule



11. Return to the **Rules** page by clicking **Rules** in the left-hand navigation panel.

The **Compliance**column value reads **Compliant**, verifying the rule is in compliance after the security group configuration change:



### Summary

In this Lab Step, you enabled an AWS Config managed rule. In analyzing a noncompliant resource, you saw how AWS Config integrates with CloudTrail to combine the benefits of both services. For practical experience, you also resolved a noncompliant configuration and observed how AWS Config reports changes in the timeline.