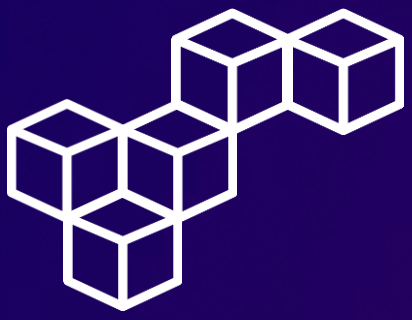
AWS re:Start LAB

Monitoring Infrastructure

WEEK 11

aws re/start



Overview

The ability to monitor your applications and infrastructure is critical for delivering reliable, consistent IT services.

Amazon CloudWatch collects and analyzes metrics and log data from your AWS resources and applications. It provides real-time insights into performance and operational health for services like EC2, RDS, and Lambda. With CloudWatch, you can set alarms, visualize logs, and monitor metrics to ensure smooth operations.

CloudWatch also supports proactive monitoring and automated responses to changes, enhancing application reliability. Create custom dashboards, set alarms, and automate actions like scaling instances. CloudWatch Logs and Events help debug and track application behavior, essential for maintaining your AWS environment's efficiency and reliability.

Topics covered

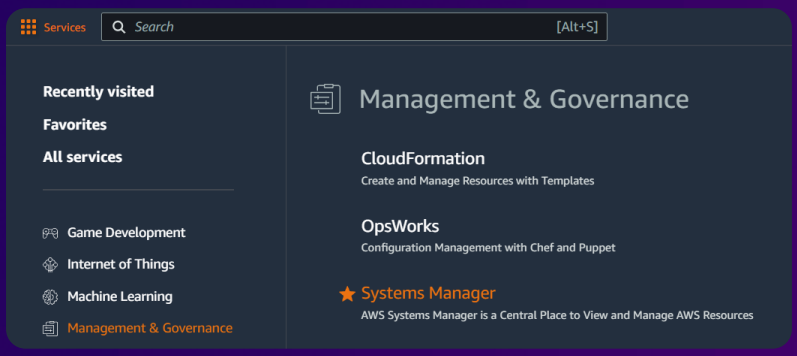
- Use the AWS Systems Manager Run Command to install the CloudWatch agent on Amazon Elastic Compute Cloud (Amazon EC2) instances
- Monitor application logs using CloudWatch agent and CloudWatch Logs
- Monitor system metrics using CloudWatch agent and CloudWatch Metrics
- Create real time notifications using CloudWatch Events
- Track infrastructure compliance using AWS Config

Task 1

Installing the CloudWatch agent

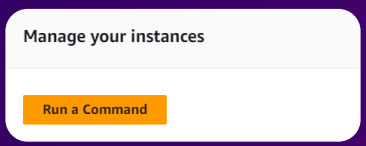
Step 1: Access Systems Manager

In the AWS Management Console, select Systems Manager.



Step 2: Run a Command

Navigate to the **Run Command** section, select Run a Command.



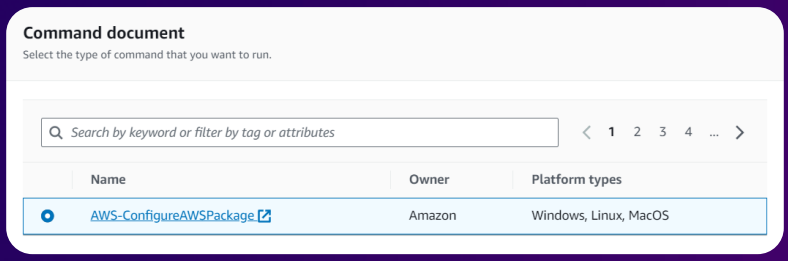
aws re/start

Task 1

Installing the CloudWatch agent

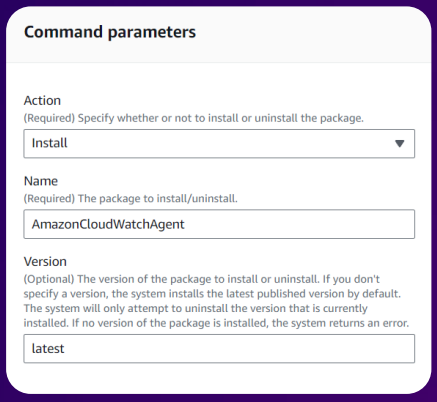
Step 3: Command document

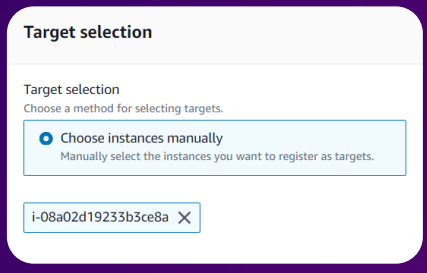
In the **Command document** section, select AWS-ConfigureAWSPackage.



Step 4: Command parameters and Target

In the **Command parameters** and **Target selection** sections, configure the following settings. This configuration installs the CloudWatch agent on the **Web Server**.





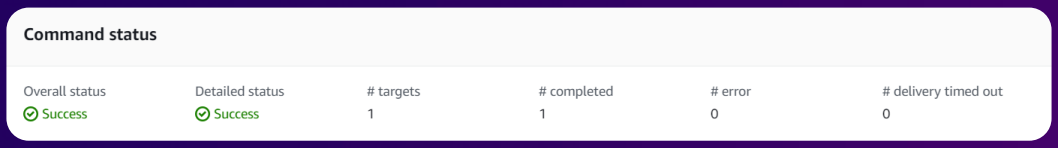
aws re/start

Task 1

Installing the CloudWatch agent

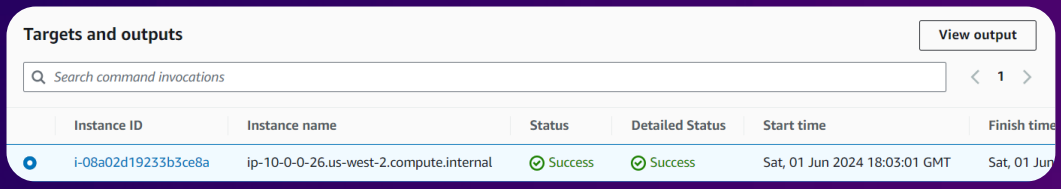
Step 5: Review Command status

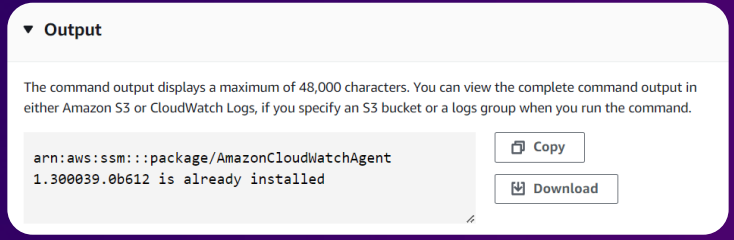
In the **Command status** section, wait for the Overall status to change to Success.



Step 6: View output

You can view the output from the job to confirm that it ran successfully. In the **Targets and outputs** section, select View output. You should see the message Successfully installed arn:aws:ssm:::package/AmazonCloudWatchAgent.





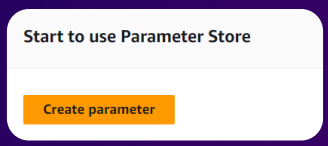
aws re/start

Task 1

Installing the CloudWatch agent

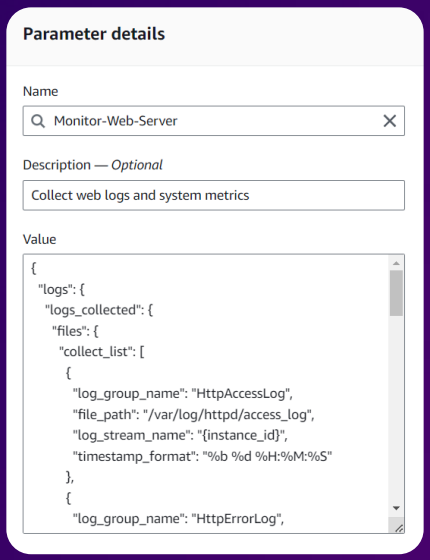
Step 7: Create parameter

Navigate to the **Parameter Store** section, and select Create parameter.



Step 8: Parameter details

In the **Parameter details** section, configure the following settings. This configuration defines two web server log files to be collected and sent to CloudWatch Logs, and CPU, disk, and memory metrics to sent to CloudWatch Metrics.



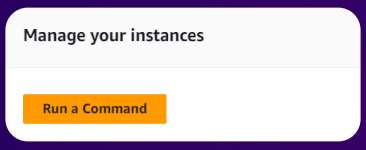
aws re/start

Task 1

Installing the CloudWatch agent

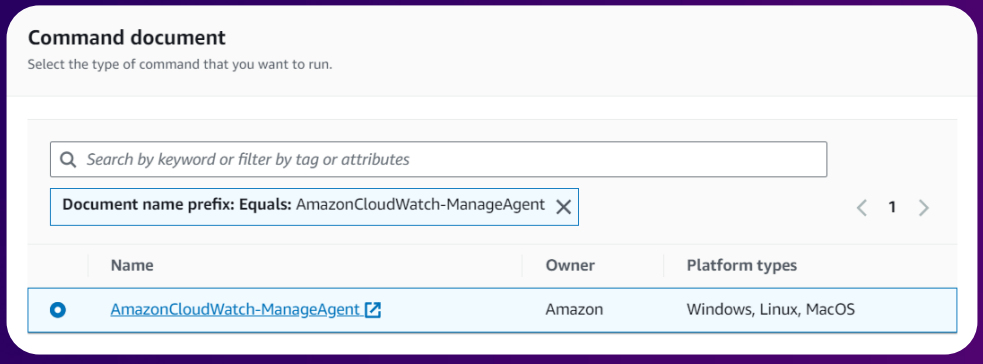
Step 9: Run Command

Navigate to the **Run Command** section, select Run a Command.



Step 10: Command document

In the **Command document** section, select AmazonCloudWatch-ManageAgent. Before running the command, you can view the definition of the command. The script references the AWS Systems Manager Parameter Store because it retrieves the CloudWatch agent configuration that you defined earlier.

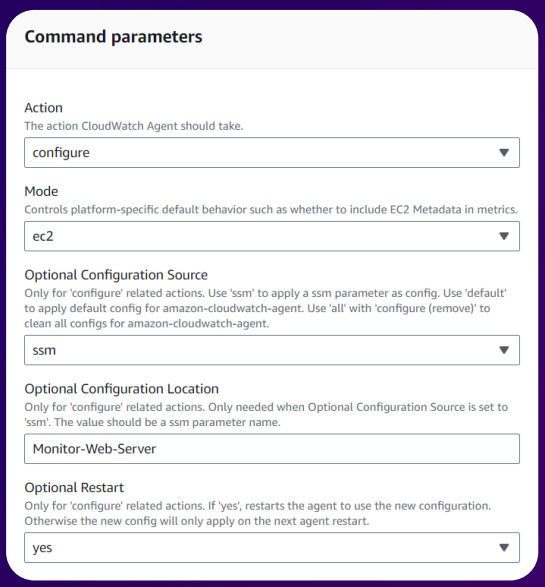


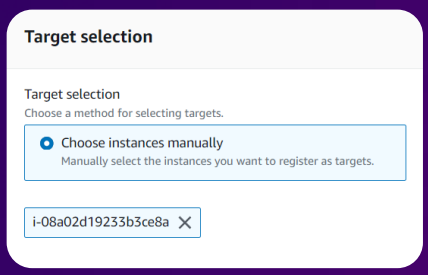
Task 1

Installing the CloudWatch agent

Step 11: Command parameters and Target

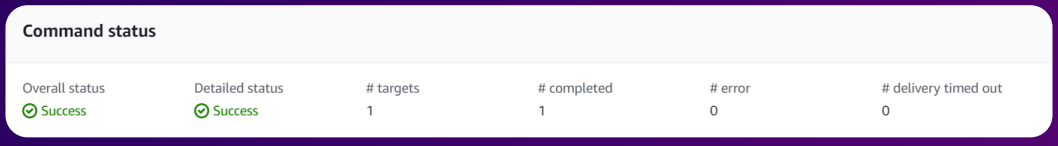
In the **Command parameters** and **Target selection** sections, configure the following settings. This configures the agent to use the configuration you previously stored in the Parameter Store.





Step 12: Review Command status

In the **Command status** section, wait for the Overall status to change to Success.



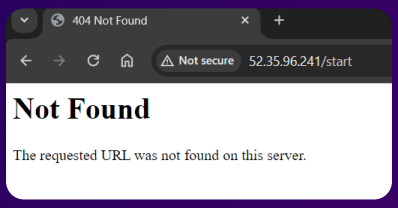
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

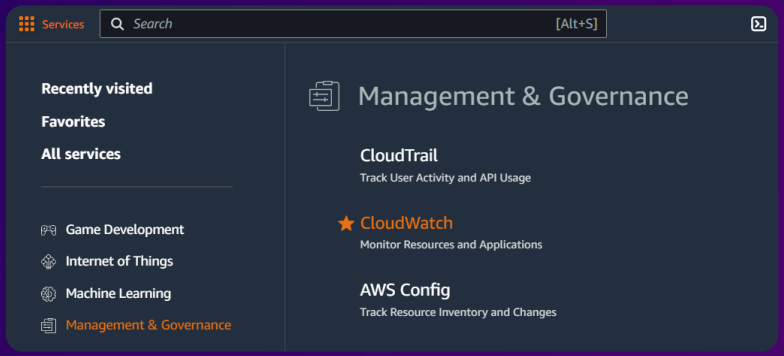
Step 1: Generate log data

Access the WebServerIP and append /start to browser URL. You receive an error message because the page is not found. This is okay! It generates data in the access logs that are being sent to CloudWatch Logs.



Step 2: Access the CloudWatch Console

In the AWS Management Console, select CloudWatch.



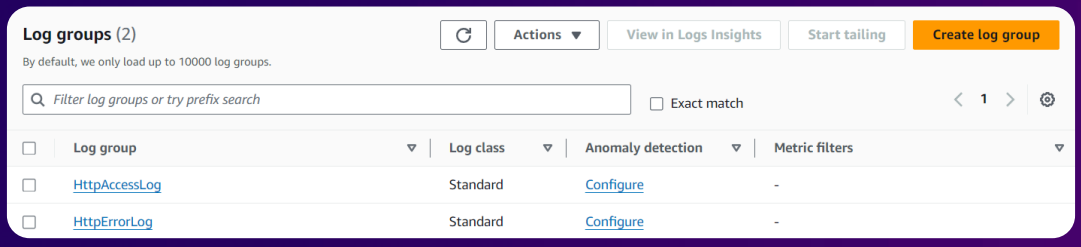
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

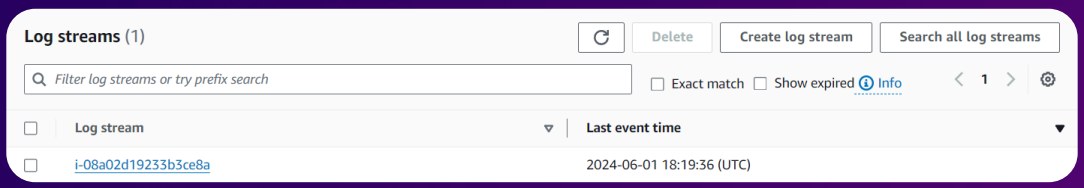
Step 3: Review Log groups

Navigate to the **Log groups** section, you should see two logs listed: **HttpAccessLog** and **HttpErrorLog**.



Step 4: Review Log streams

Choose **HttpAccessLog**. In the **Logs streams** section, choose the Log stream in the table. It has the same ID as the EC2 instance that the log is attached to.



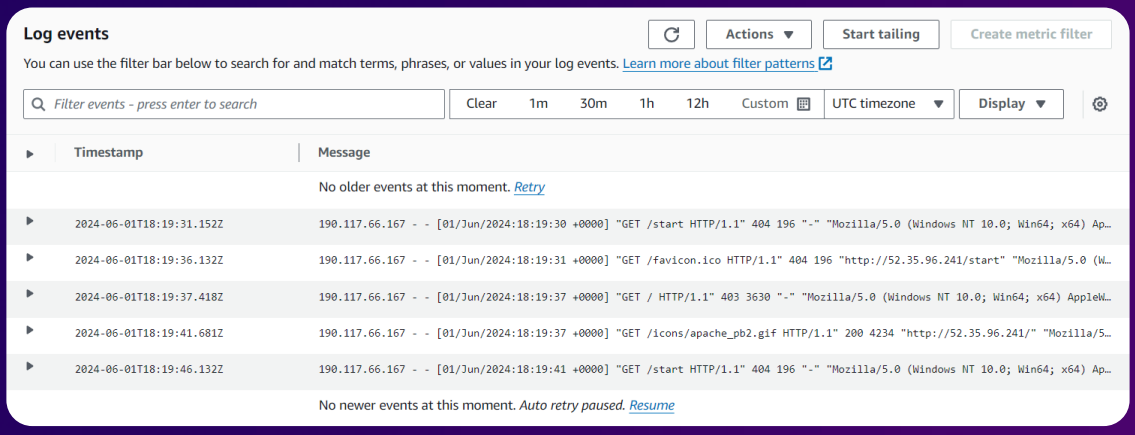
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

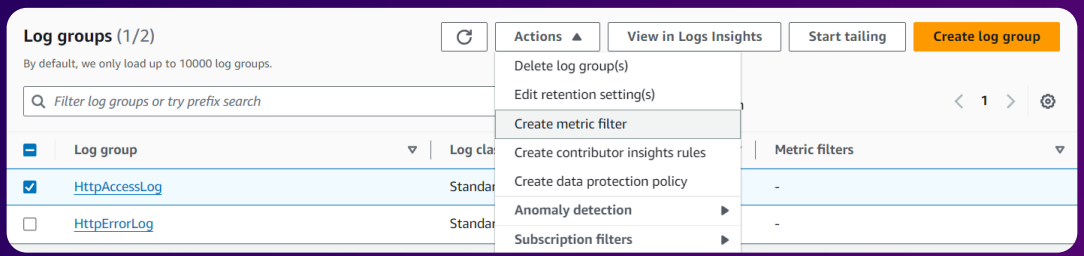
Step 5: Review Log events

Log data is displayed, consisting of GET requests that were sent to the web server. You should see a line with your /start request with a code of 404, which means that the page was not found.



Step 6: Create metric filter

In the **Log groups** section, select **HttpAccessLog**, and from the Actions dropdown menu, select Create metric filter.



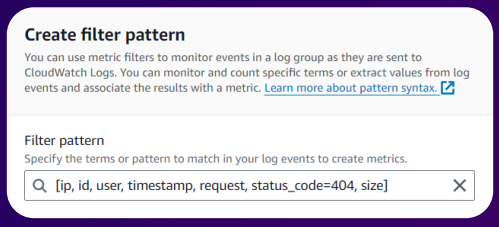
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

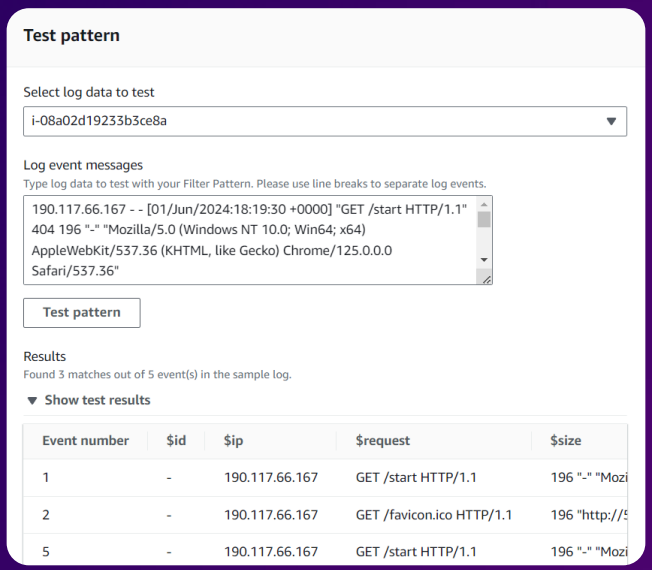
Step 7: Create filter pattern

In the **Create filter pattern** section, enter the following Filter pattern.



Step 8: Test pattern

In the **Test pattern** section, configure the following settings, and choose Test pattern. In the **Results** section, You should see at least one result with a $status_code of 404. This status code indicates that a page was requested that was not found.



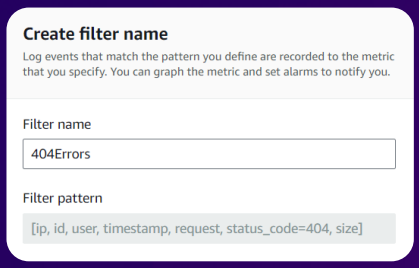
aws re/start

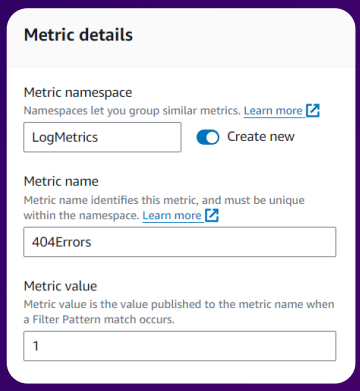
Task 2

Monitoring application logs using CloudWatch Logs

Step 9: Metric details

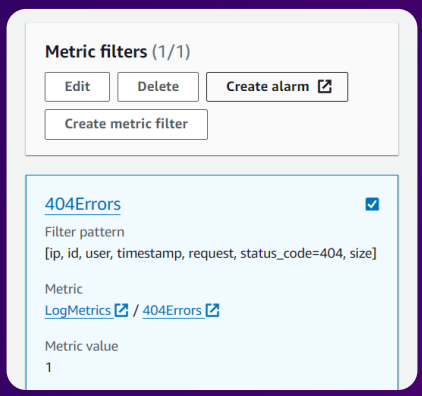
In the **Create filter name** and **Metric details** sections, configure the following settings.





Step 10: Create alarm

In the **Metric filters** section, select the **404Errors** metric filter, and choose Create alarm.



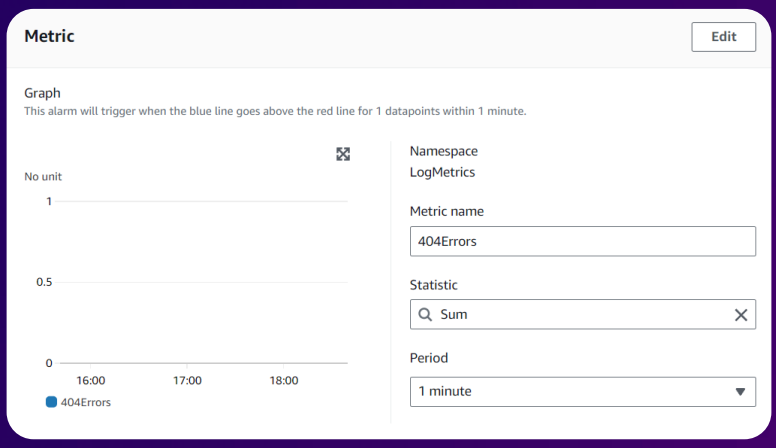
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

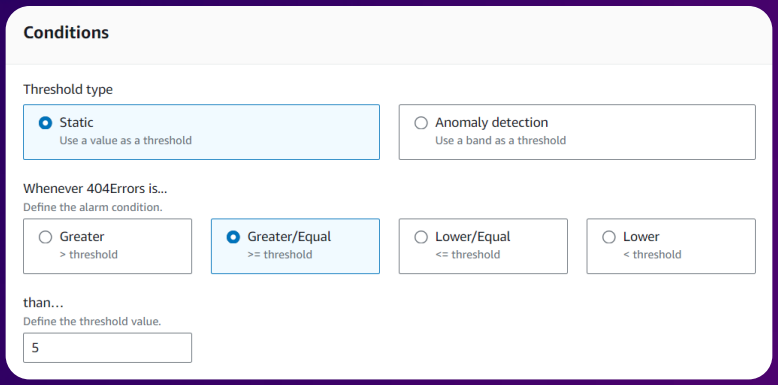
Step 11: Metric

In the **Metric** section, configure the following settings.



Step 12: Conditions

In the **Conditions** section, configure the following settings.



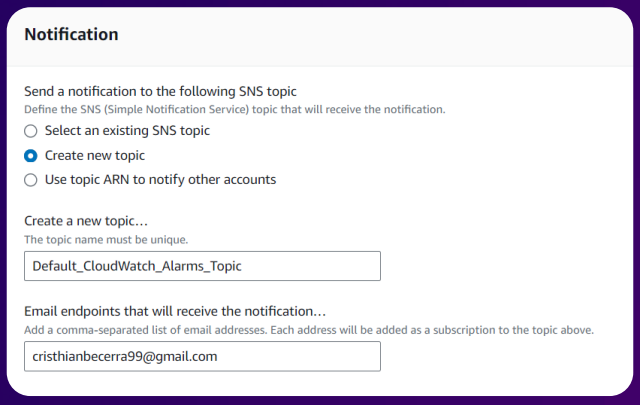
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

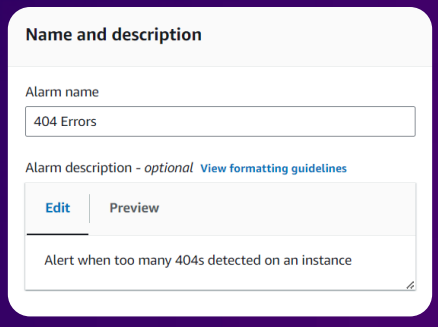
Step 13: Notification

In the **Notification** section, configure the following settings.



Step 14: Name and description

In the **Name and description** section, configure the following settings.



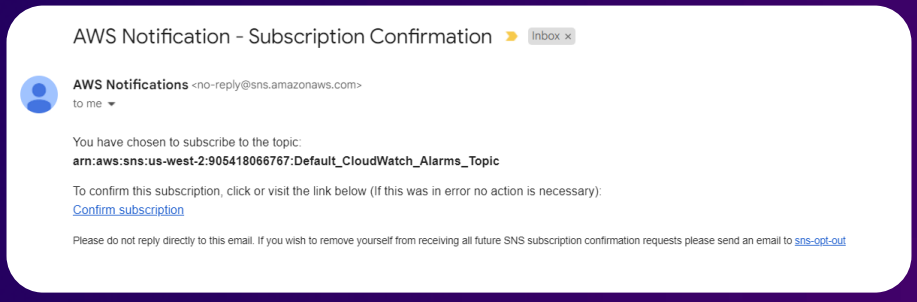
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

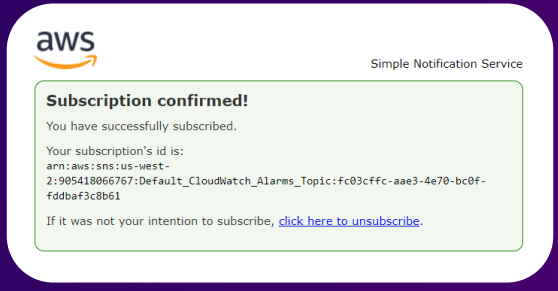
Step 15: Check your email

Go to your email and look for a confirmation message.



Step 16: Confirm subscription

Select the Confirm subscription link.



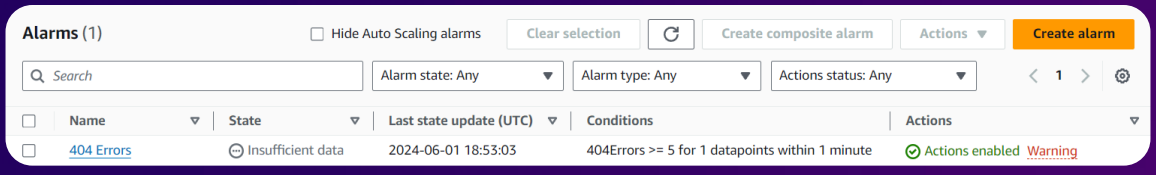
aws re/start

Task 2

Monitoring application logs using CloudWatch Logs

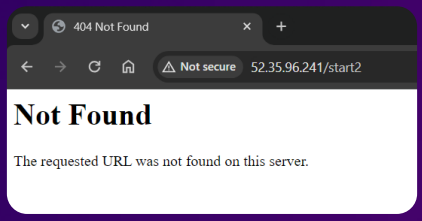
Step 17: Review Alarms

Your alarm might appear in orange, indicating that there is Insufficient data to trigger the alarm. This alarm appears because no data has been received in the past minute.



Step 18: Generate log data

Access the web server to generate log data. Attempt to go to pages that do not exist by adding a page name after the IP address. Repeat this step at least five times.



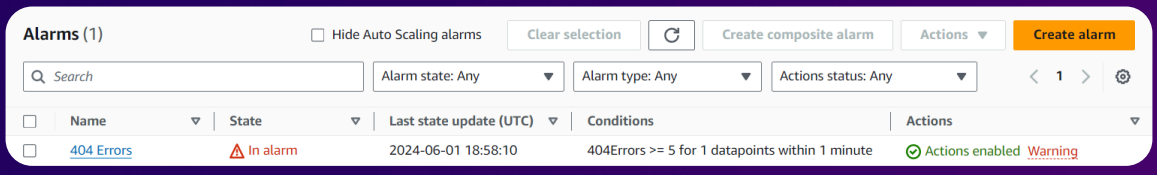
aws re/start

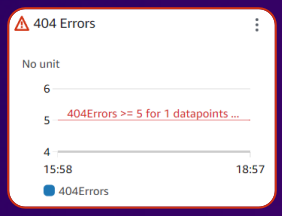
Task 2

Monitoring application logs using CloudWatch Logs

Step 19: Review In alarm state

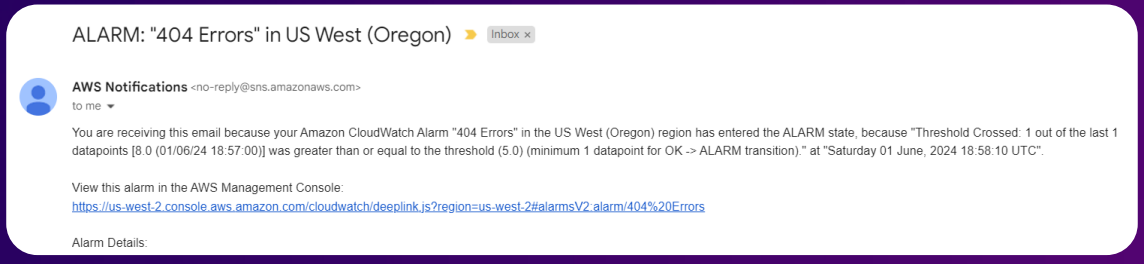
Wait for the alarm to trigger. The graph shown on the CloudWatch page should turn red to indicate that it is in the In Alarm state.





Step 20: Check your email

Check your email. You should have received an email with the subject ALARM: "404 Errors".



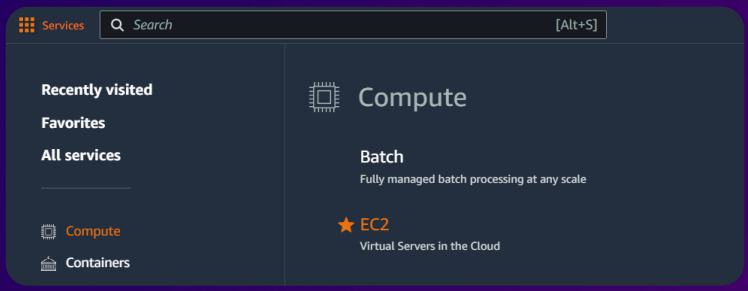
aws re/start

Task 3

Monitoring instance metrics using CloudWatch

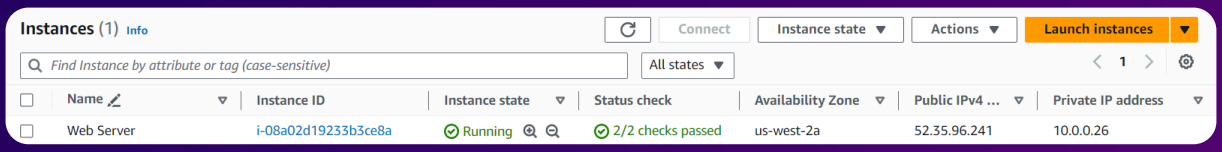
Step 1: Access the EC2 Management Console

In the AWS Management Console, select EC2.



Step 2: Review Instances

Navigate to the **Instances** section, and select the **Web Server** instance.



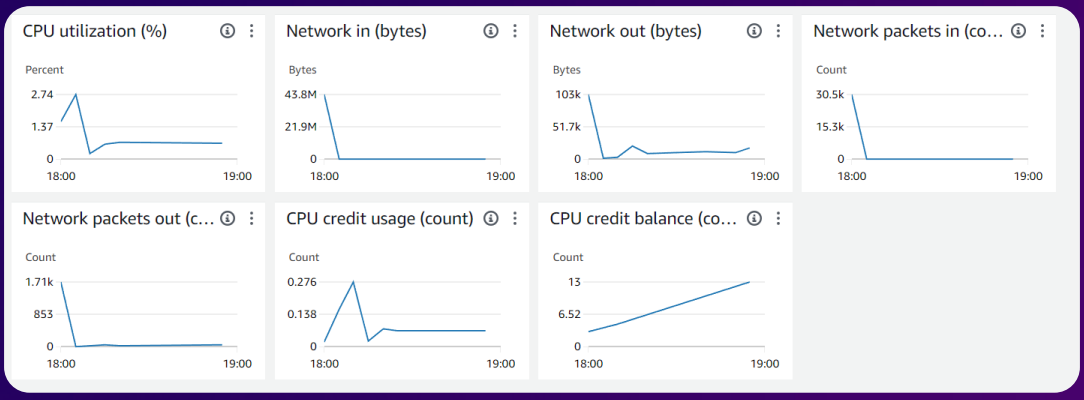
aws re/start

Task 3

Monitoring instance metrics using CloudWatch

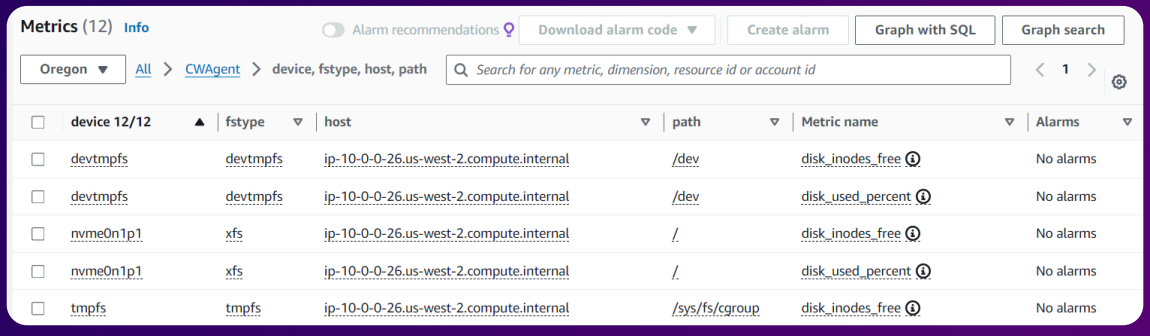
Step 3: Monitoring

Choose the **Monitoring** tab for the **Web Server** instance. Examine the metrics presented.



Step 4: device, fstype, host, path metrics

In the CloudWatch Console, navigate to the **Metrics** section, choose **CWAgent**, and then choose device, fstype, host, path. You see the disk space metrics that the CloudWatch agent is capturing.



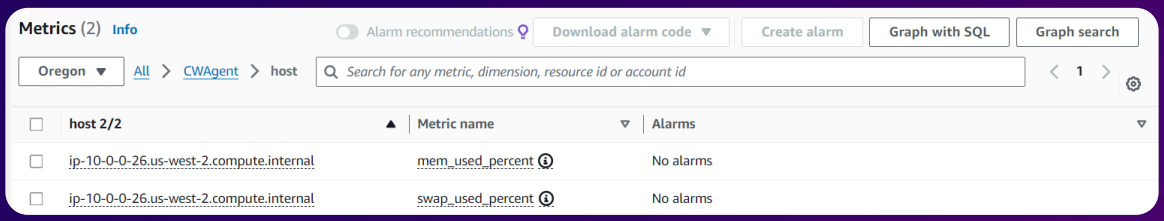
device 12/12	fstype	host	path	Metric name	Alarms
devtmpfs	devtmpfs	ip-10-0-0-26.us-west-2.compute.internal	/dev	disk_inodes_free	No alarms
devtmpfs	devtmpfs	ip-10-0-0-26.us-west-2.compute.internal	/dev	disk_used_percent	No alarms
nvme0n1p1	xfs	ip-10-0-0-26.us-west-2.compute.internal	/	disk_inodes_free	No alarms
nvme0n1p1	xfs	ip-10-0-0-26.us-west-2.compute.internal	/	disk_used_percent	No alarms
tmpfs	tmpfs	ip-10-0-0-26.us-west-2.compute.internal	/sys/fs/cgroup	disk_inodes_free	No alarms

Task 3

Monitoring instance metrics using CloudWatch

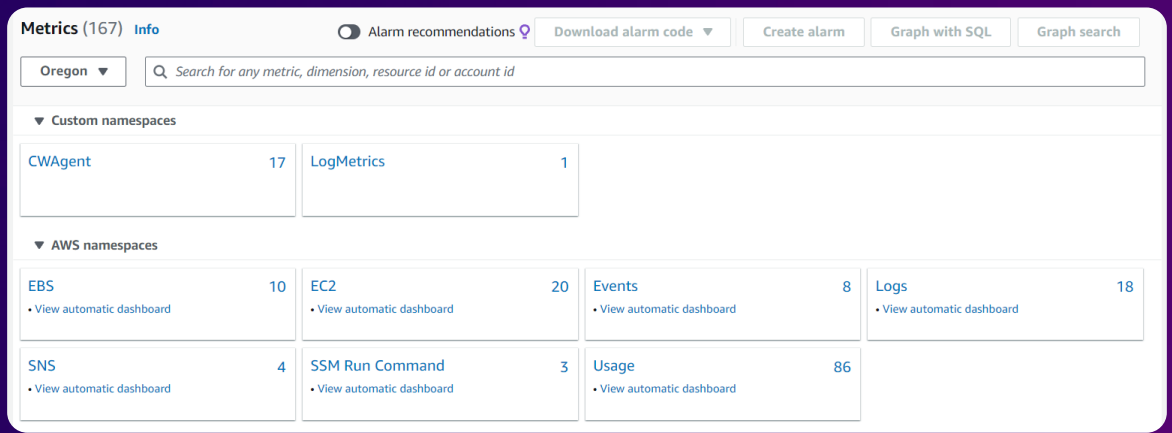
Step 5: host metrics

Choose **CWAgent**, and choose host. You see metrics relating to system memory.



Step 6: Review all Metrics

Choose **All**. Explore the other metrics that CloudWatch is capturing. These are automatically generated metrics coming from the AWS services that have been used in this AWS account.



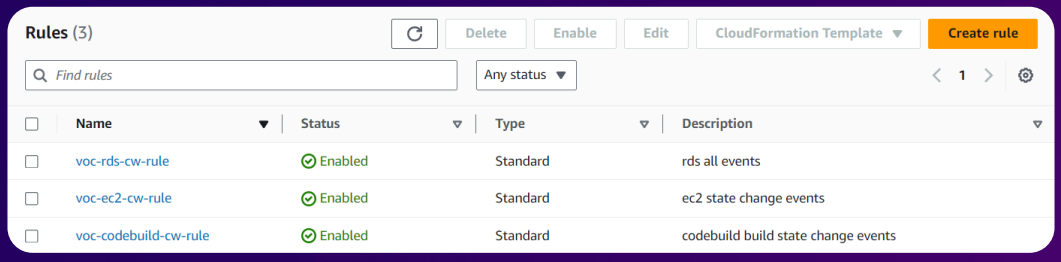
aws re/start

Task 4

Creating real time notifications

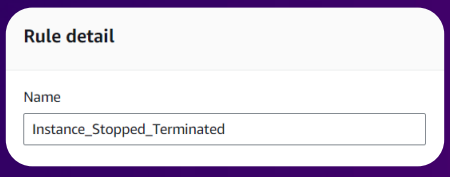
Step 1: Create rule

Navigate to the **Rules** section, and choose Create rule.



Step 2: Rule detail

In the **Rule detail** section, configure the following settings.



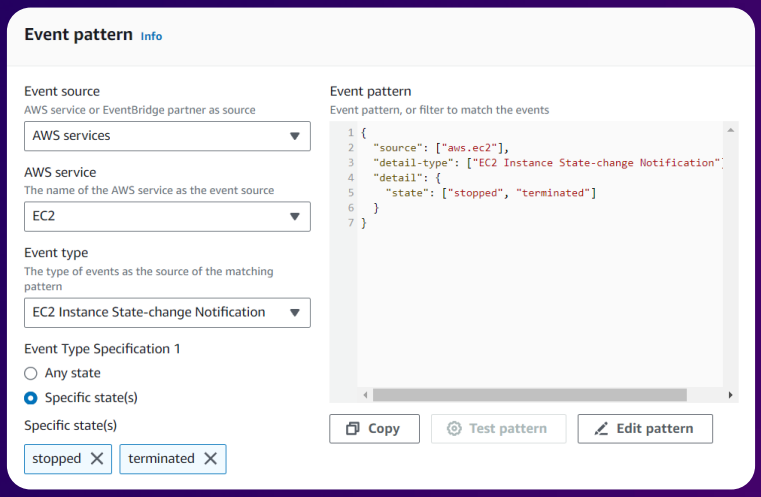
aws re/start

Task 4

Creating real time notifications

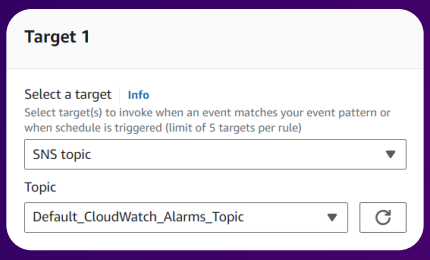
Step 3: Event pattern

In the **Event pattern** section, configure the following settings.



Step 4: Target 1

In the **Target 1** section, configure the following settings.



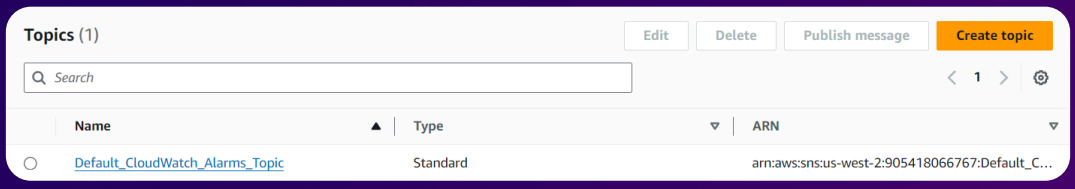
aws re/start

Task 4

Creating real time notifications

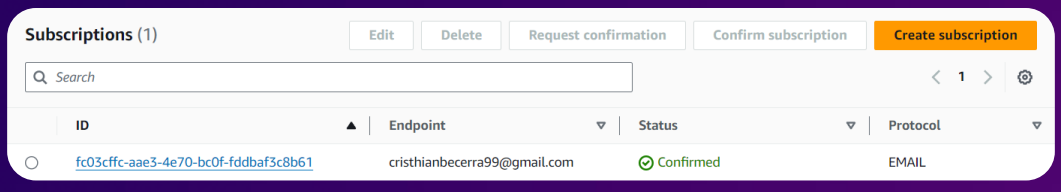
Step 5: Review Topics

In the Simple Notification Service Console, navigate to the **Topics** section, and choose Default_CloudWatch_Alarms_Topic.



Step 6: Review Subscriptions

In the **Subscriptions** section, you should see a single subscription associated with your email address. This is the Topic you configured in Task 2



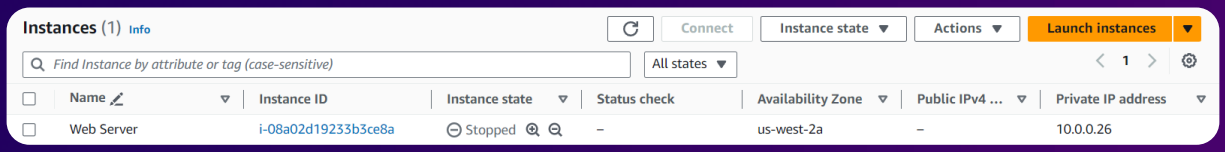
aws re/start

Task 4

Creating real time notifications

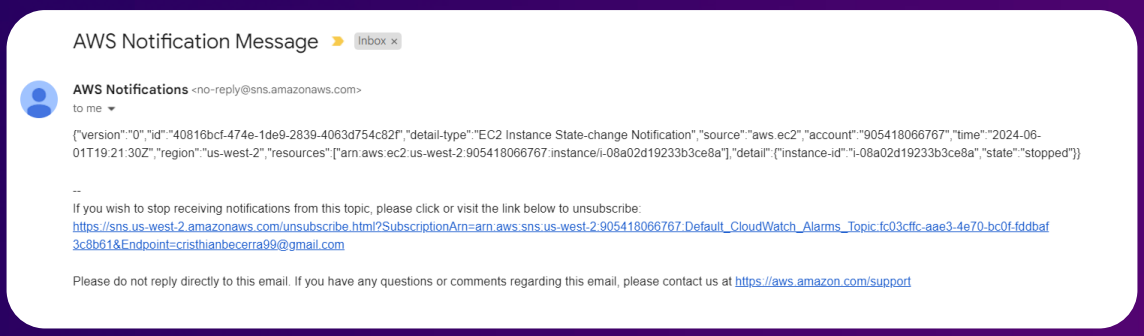
Step 7: Stop instance

In the EC2 Management Console, navigate to the **Instances** section, select the **Web Server** instance, choose Instance state > Stop instance. The **Web Server** instance enters the Stopped state.



Step 8: Check your email

You should receive an email with details about the instance that was stopped. The message is formatted in JSON. To receive a message that is easier to read, you could create an AWS Lambda function that CloudWatch Events triggers. The Lambda function could then format a more readable message and send it via Amazon SNS.



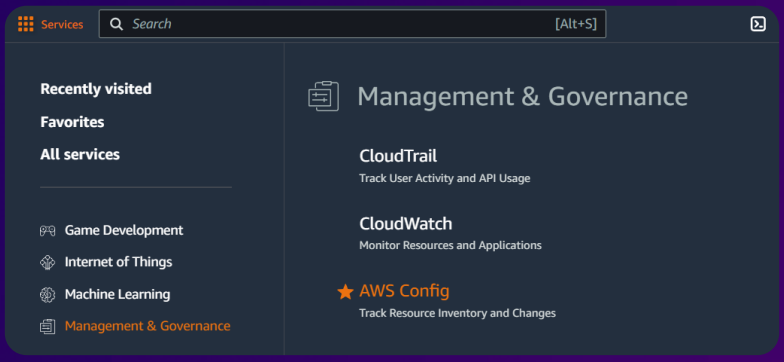
aws re/start

Task 5

Monitoring for infrastructure compliance

Step 1: Access the AWS Config service

In the AWS Management Console, select AWS Config.



Step 2: Get started

Choose Get started > Next > Next > Confirm. This configures AWS Config for initial use.

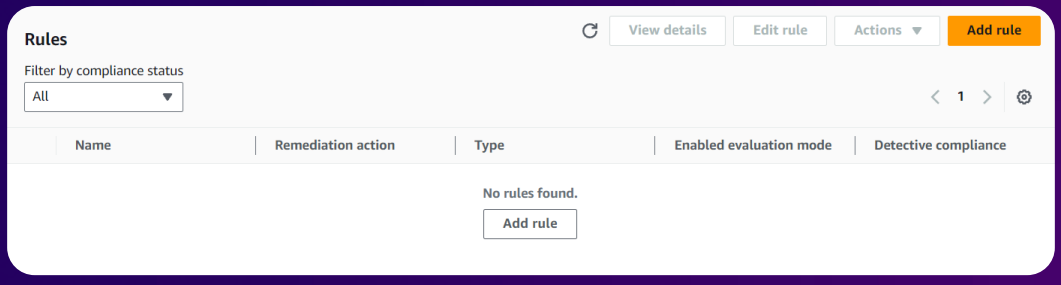
aws re/start

Task 5

Monitoring for infrastructure compliance

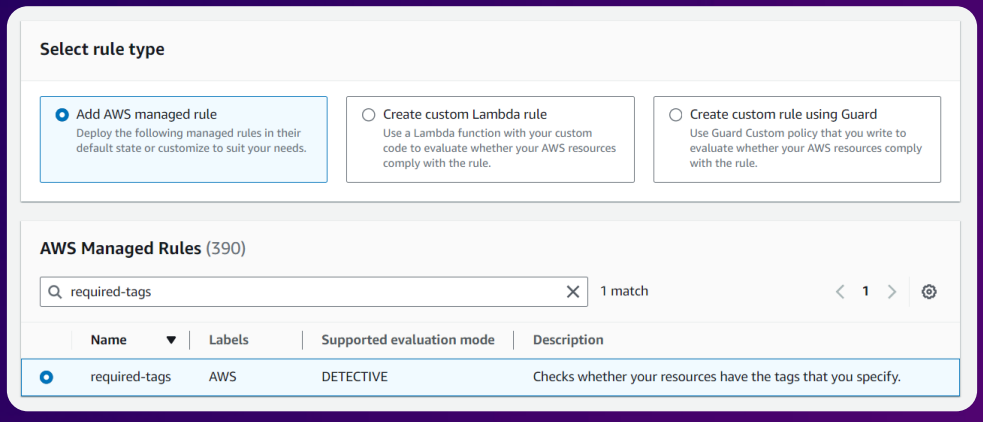
Step 3: Add rule

Navigate to the **Rules** section, and select Add rule.



Step 4: Select rule

In the **Select rule type** section, select Add AWS managed rule.
In the **AWS Managed Rules** section, select required-tags.



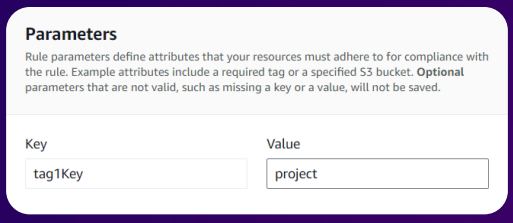
aws re/start

Task 5

Monitoring for infrastructure compliance

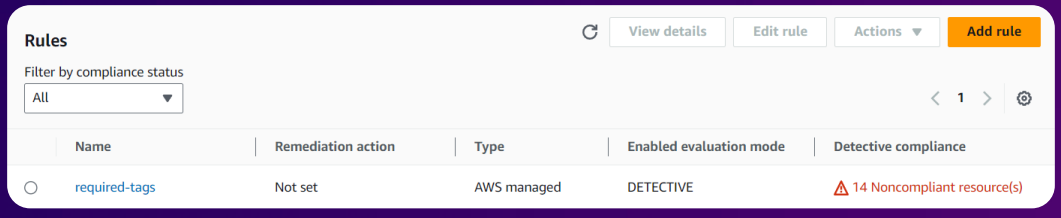
Step 5: Parameters

In the **Parameters** section, configure the following setings.



Step 6: Add rule

In to the **Rules** section, select Add rule.



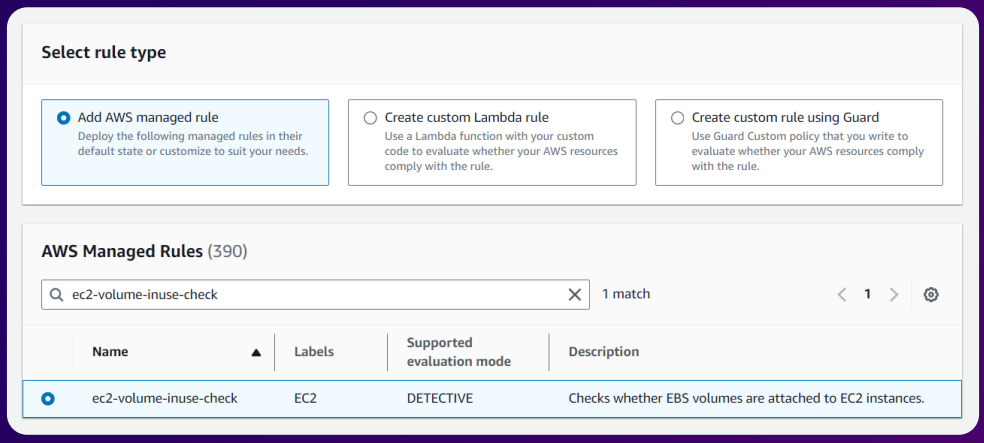
aws re/start

Task 5

Monitoring for infrastructure compliance

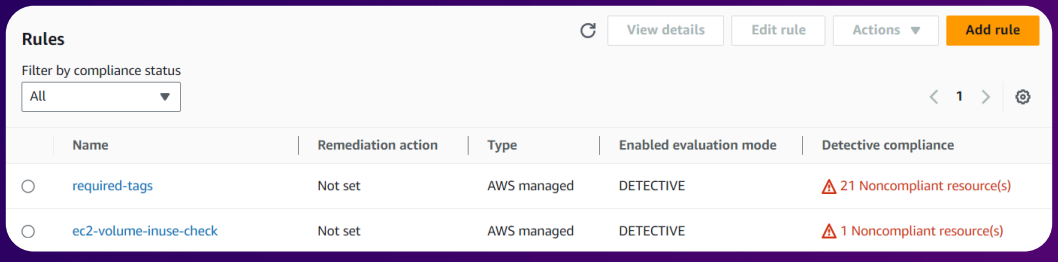
Step 7: Select rule

In the **Select rule type** section, select Add AWS managed rule. In the **AWS Managed Rules** section, select ec2-volume-inuse-check.



Step 8: Review rules

In the **Rules** section, when both rules have completed evaluation, choose each of the rules to view the result of the audits.



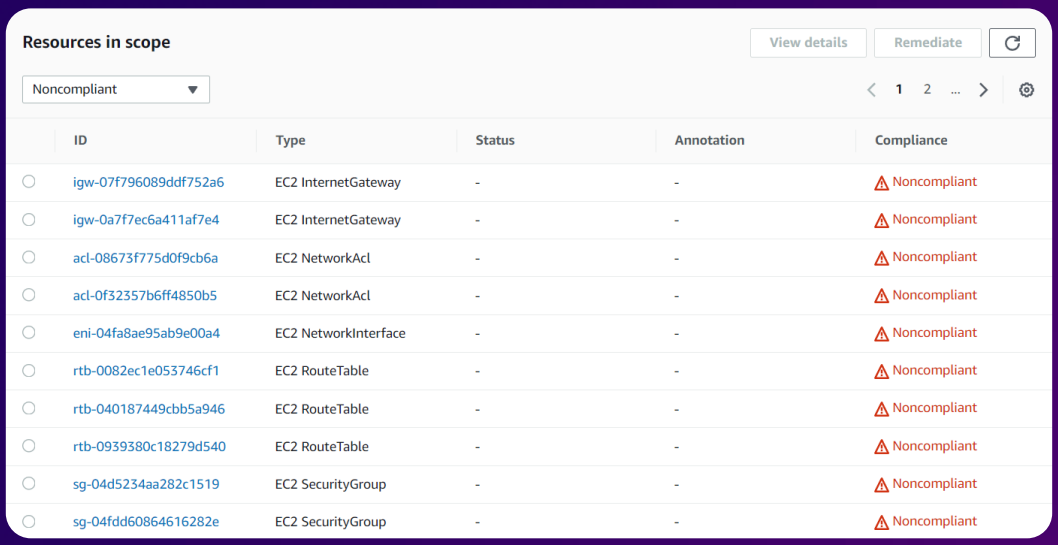
aws re/start

Task 5

Monitoring for infrastructure compliance

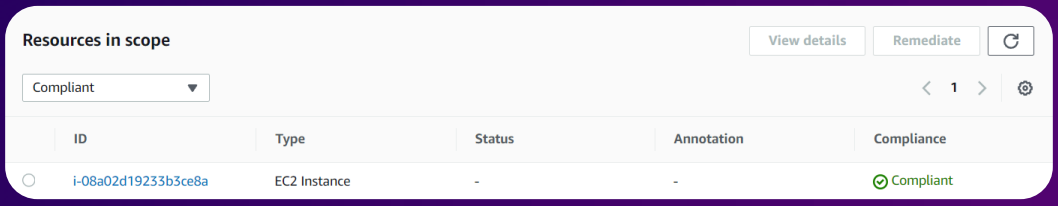
Step 9: required-tags

In the **Resources in scope** section, select **Compliant**.



Step 10: required-tags (Compliant)

Review the results: A compliant EC2 instance (because the Web Server has a project tag) and many non-compliant resources that do not have a project tag.



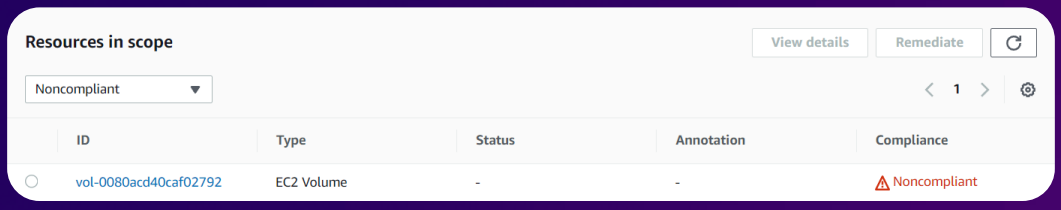
aws re/start

Task 5

Monitoring for infrastructure compliance

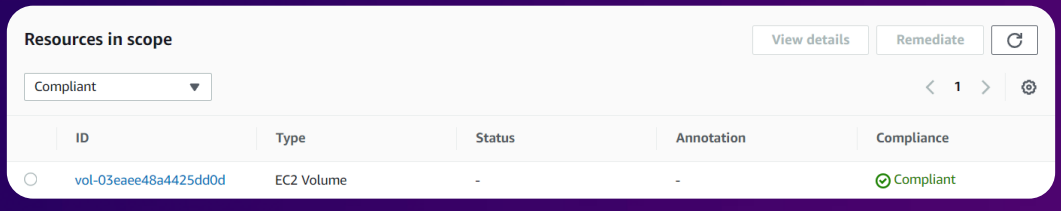
Step 11: ec2-volume-inuse-check

In the **Resources in scope** section, select **Compliant**.

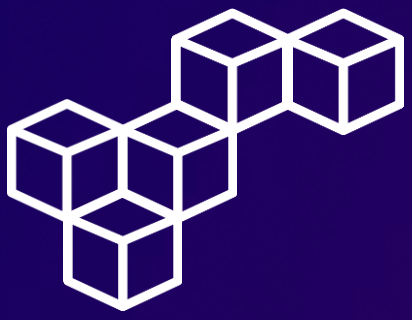


Step 12: ec2-volume-inuse-check (Compliant)

Review the results: One compliant volume (attached to an instance) and one non-compliant volume (not attached to an instance).



aws re/start



Conclusions

CloudWatch Agents
CloudWatch Agents collect detailed system-level metrics and logs from your instances, enabling comprehensive monitoring and custom metric creation.

CloudWatch Logs
CloudWatch Logs centralize log data from various sources, providing storage, analysis, and real-time monitoring capabilities to improve troubleshooting and operational insights.

CloudWatch Metrics
CloudWatch Metrics track the performance and health of AWS resources, offering key insights and enabling the creation of alarms for automated responses to metric changes.

CloudWatch Events
CloudWatch Events facilitate automated responses to state changes in AWS resources, allowing real-time event-driven actions to maintain system health and efficiency.

AWS Config Rules
AWS Config Rules ensure compliance and governance by automatically evaluating resource configurations against predefined policies and best practices.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru