



AWS
re:Start
LAB

Monitoring Infrastructure



WEEK 11





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

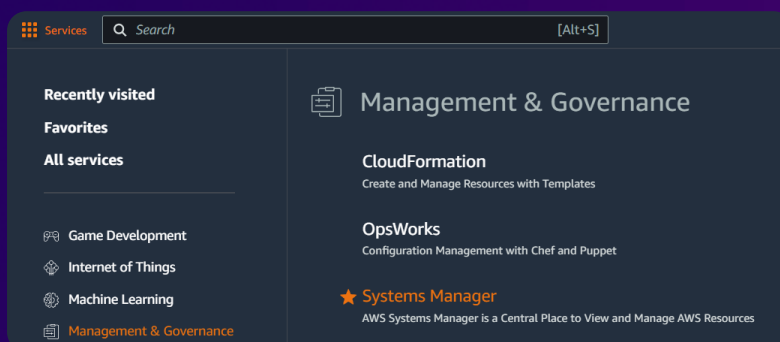


Task 1

Installing the CloudWatch agent

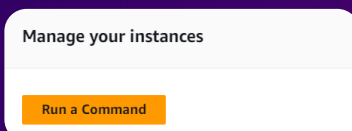
Step 1: Access Systems Manager

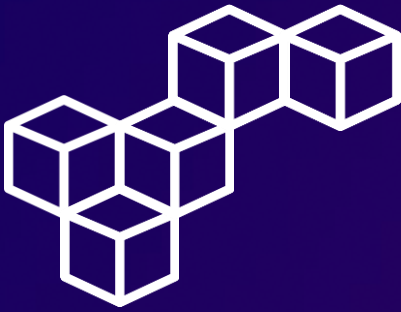
In the AWS Management Console, select Systems Manager.



Step 2: Run a Command

Navigate to the **Run Command** section, select [Run a Command](#).





Task 1

Installing the CloudWatch agent

Step 3: Command document

In the **Command document** section, select [AWS-ConfigureAWSPackage](#).

Command document
Select the type of command that you want to run.

< 1 2 3 4 ... >

	Name	Owner	Platform types
<input checked="" type="radio"/>	AWS-ConfigureAWSPackage	Amazon	Windows, Linux, MacOS

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**.

Command parameters

Action
(Required) Specify whether to install or uninstall the package.

Install ▼

Name
(Required) The package to install/uninstall.

AmazonCloudWatchAgent

Version
(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. The system will only attempt to uninstall the version that is currently installed. If no version of the package is installed, the system returns an error.

latest

Target selection

Target selection
Choose a method for selecting targets.

☒ Choose instances manually
Manually select the instances you want to register as targets.

i-08a02d19233b3ce8a

 ✕



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**.

Command status					
Overall status	Detailed status	# targets	# completed	# error	# delivery timed out
✔ Success	✔ Success	1	1	0	0

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**.

Targets and outputs

View output

Search command invocations

< 1 >

	Instance ID	Instance name	Status	Detailed Status	Start time	Finish time
<div></div>	i-08a02d19233b3ce8a	ip-10-0-0-26.us-west-2.compute.internal	<div>✔ Success</div>	<div>✔ Success</div>	Sat, 01 Jun 2024 18:03:01 GMT	Sat, 01 Jun 2024 18:03:01 GMT

▼ Output

The command output displays a maximum of 48,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.

```
arn:aws:ssm:::package/AmazonCloudWatchAgent
1.300039.0b612 is already installed
```

[Copy](#)[Download](#)

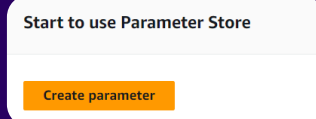


Task 1

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.

Parameter details

Name
Monitor-Web-Server

Description — *Optional*
Collect web logs and system metrics

Value

```
{
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
          {
            "log_group_name": "HttpAccessLog",
            "file_path": "/var/log/httpd/access_log",
            "log_stream_name": "[instance_id]",
            "timestamp_format": "%b %d %H:%M:%S"
          },
          {
            "log_group_name": "HttpErrorLog",
```

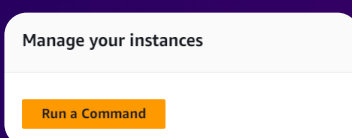


Task 1

Installing the CloudWatch agent

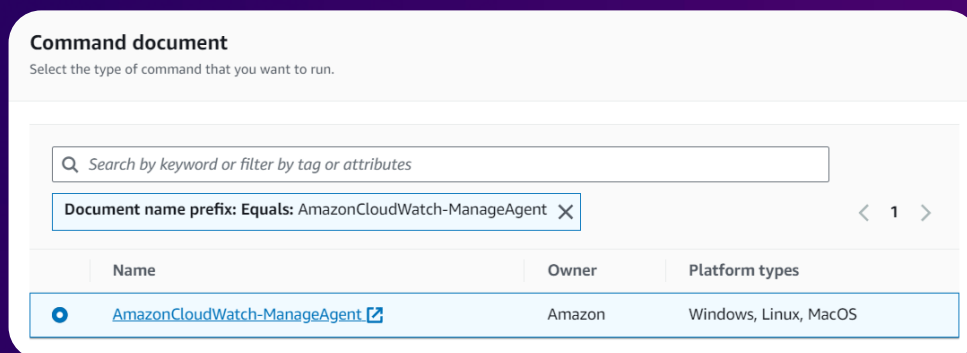
Step 9: Run Command

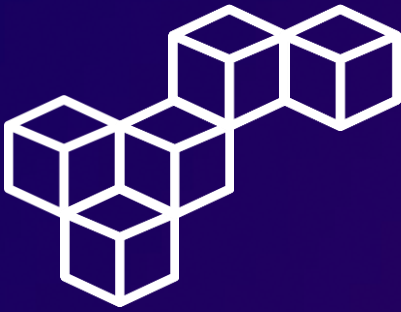
Navigate to the **Run Command** section, select [Run a Command](#).



Step 10: Command document

In the **Command document** section, select [AmazonCloudWatch-ManagedAgent](#). 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.

Command parameters

Action

The action CloudWatch Agent should take.

configure

Mode

Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

ec2

Optional Configuration Source

Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all configs for amazon-cloudwatch-agent.

ssm

Optional Configuration Location

Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

Monitor-Web-Server

Optional Restart

Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent restart.

yes

Target selection

Target selection

Choose a method for selecting targets.

Choose instances manually

Manually select the instances you want to register as targets.

i-08a02d19233b3ce8a

X

Step 12: Review Command status

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

Command status					
Overall status	Detailed status	# targets	# completed	# error	# delivery timed out
Success	Success	1	1	0	0

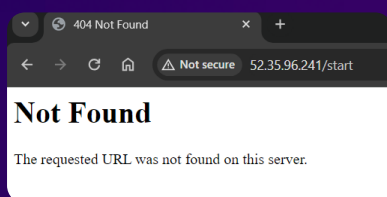


Task 2

Monitoring application logs using CloudWatch Logs

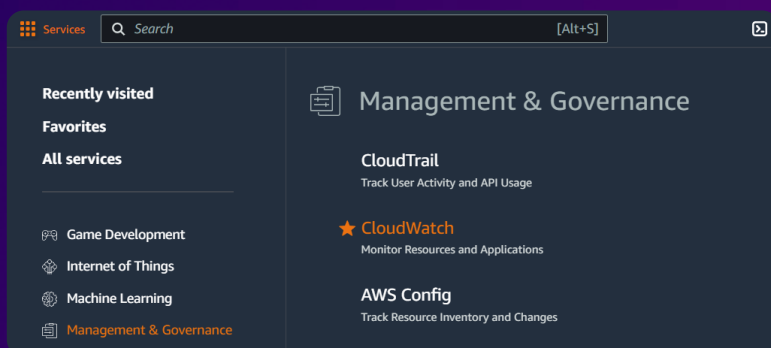
Step 1: Generate log data

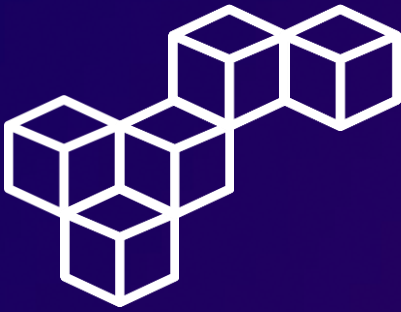
Access the WebServerIP and append /start to browser URL. You receive an error message because the page is not found. This is okay! It generates data in the access logs that are being sent to CloudWatch Logs.



Step 2: Access the CloudWatch Console

In the AWS Management Console, select CloudWatch.





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**.

Log groups (2)

Actions

View in Logs Insights

Start tailing

Create log group

By default, we only load up to 10000 log groups.

Filter log groups or try prefix search

☐ Exact match

< 1 >

<input type="checkbox"/>	Log group	Log class	Anomaly detection	Metric filters
<input type="checkbox"/>	HttpAccessLog	Standard	Configure	-
<input type="checkbox"/>	HttpErrorLog	Standard	Configure	-

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.

Log streams (1)

Delete

Create log stream

Search all log streams

Filter log streams or try prefix search

☐ Exact match ☐ Show expired

Info

< 1 >

<input type="checkbox"/>	Log stream	Last event time
<input type="checkbox"/>	i-08a02d19233b3ce8a	2024-06-01 18:19:36 (UTC)



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.

Log events

Filter events - press enter to search

Clear

1m

30m

1h

12h

Custom

UTC timezone

Display

Timestamp

Message

No older events at this moment. [Retry](#)

▶

2024-06-01T18:19:31.152Z

190.117.66.167 - - [01/Jun/2024:18:19:30 +0000] "GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap...

▶

2024-06-01T18:19:36.132Z

190.117.66.167 - - [01/Jun/2024:18:19:31 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://52.35.96.241/start" "Mozilla/5.0 (W...

▶

2024-06-01T18:19:37.418Z

190.117.66.167 - - [01/Jun/2024:18:19:37 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleH...

▶

2024-06-01T18:19:41.681Z

190.117.66.167 - - [01/Jun/2024:18:19:37 +0000] "GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "http://52.35.96.241/" "Mozilla/5...

▶

2024-06-01T18:19:46.132Z

190.117.66.167 - - [01/Jun/2024:18:19:41 +0000] "GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap...

No newer events at this moment. [Auto retry paused.](#) [Resume](#)

Step 6: Create metric filter

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

Log groups (1/2)

Filter log groups or try prefix search

Log group

Log cla

⊞

HttpAccessLog

Standar

⊞

HttpErrorLog

Standar

Actions

View in Logs Insights

Start tailing

Create log group

Delete log group(s)

Edit retention setting(s)

Create metric filter

Create contributor insights rules

Create data protection policy

Anomaly detection

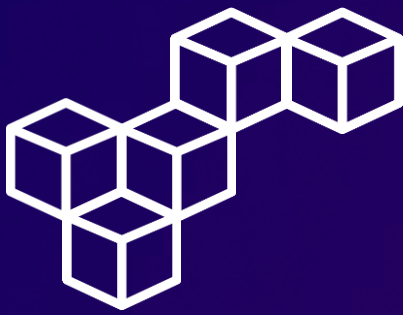
Subscription filters

Metric filters

-

-

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.

Create filter pattern
You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

Filter pattern
Specify the terms or pattern to match in your log events to create metrics.

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.

Test pattern

Select log data to test

Log event messages
Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

```
190.117.66.167 - - [01/Jun/2024:18:19:30 +0000] "GET /start HTTP/1.1"
404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0
Safari/537.36"
```

Results
Found 3 matches out of 5 event(s) in the sample log.
Show test results

Event number	\$id	\$ip	\$request	\$size
1	-	190.117.66.167	GET /start HTTP/1.1	196 "-" "Mozi
2	-	190.117.66.167	GET /favicon.ico HTTP/1.1	196 "http://5
5	-	190.117.66.167	GET /start HTTP/1.1	196 "-" "Mozi



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.

Create filter name
Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter name

Filter pattern

Metric details

Metric namespace
Namespaces let you group similar metrics. [Learn more](#)
 ☒ Create new

Metric name
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)

Metric value
Metric value is the value published to the metric name when a Filter Pattern match occurs.

Step 10: Create alarm

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

Metric filters (1/1)

Edit Delete [Create alarm](#)

Create metric filter

[404Errors](#) ☒

Filter pattern
[ip, id, user, timestamp, request, status_code=404, size]

Metric
[LogMetrics](#) / [404Errors](#)

Metric value
1



Task 2

Monitoring application logs using CloudWatch Logs

Step 11: Metric

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

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

No unit

1

0.5

0

16:00

17:00

18:00

404Errors

Namespace

LogMetrics

Metric name

404Errors

Statistic

Q Sum

Period

1 minute

Step 12: Conditions

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

Conditions

Threshold type

☒ Static

Use a value as a threshold

☐ Anomaly detection

Use a band as a threshold

Whenever 404Errors is...

Define the alarm condition.

☐ Greater

> threshold

☒ Greater/Equal

>= threshold

☐ Lower/Equal

<= threshold

☐ Lower

< threshold

than...

Define the threshold value.

5



Task 2

Monitoring application logs using CloudWatch Logs

Step 13: Notification

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

Notification

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

Create a new topic...

The topic name must be unique.

Default_CloudWatch_Alarms_Topic

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

cristhianbecerra99@gmail.com

Step 14: Name and description

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

Name and description

Alarm name

404 Errors

Alarm description - optional [View formatting guidelines](#)

[Edit](#) [Preview](#)

Alert when too many 404s detected on an instance

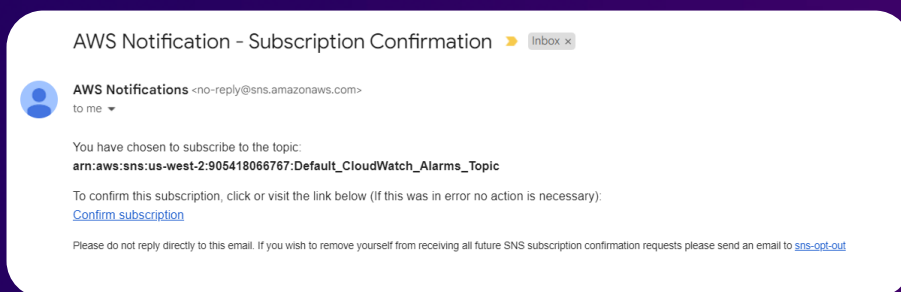


Task 2

Monitoring application logs using CloudWatch Logs

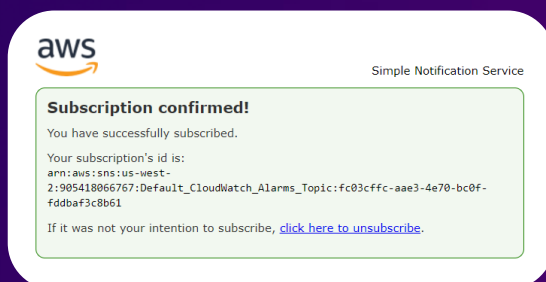
Step 15: Check your email

Go to your email and look for a confirmation message.



Step 16: Confirm subscription

Select the [Confirm subscription](#) link.





Task 2

Monitoring application logs using CloudWatch Logs

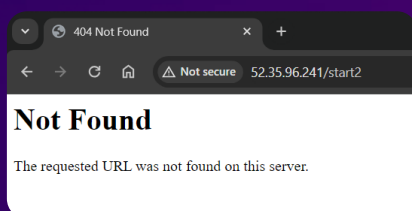
Step 17: Review Alarms

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.

Alarms (1)						
<input type="checkbox"/> Hide Auto Scaling alarms		Clear selection		Create composite alarm	Actions	Create alarm
Q Search		Alarm state: Any	Alarm type: Any	Actions status: Any	< 1 >	
<input type="checkbox"/>	Name	State	Last state update (UTC)	Conditions	Actions	
<input type="checkbox"/>	404 Errors	Insufficient data	2024-06-01 18:53:03	404Errors >= 5 for 1 datapoints within 1 minute	Actions enabled Warning	

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.





Step 19: Review In alarm state

Alarms (1)

☐ Hide Auto Scaling alarms

Clear selection

↺

Create composite alarm

Actions ▾

Create alarm

Alarm state: Any ▾

Alarm type: Any ▾

Actions status: Any ▾

<

1

>

⚙

<input type="checkbox"/>	Name ▾	State ▾	Last state update (UTC) ▾	Conditions	Actions ▾
<input type="checkbox"/>	404 Errors	⚠ In alarm	2024-06-01 18:58:10	404Errors >= 5 for 1 datapoints within 1 minute	<div> <div>🟢 Actions enabled</div> <div>🔴 Warning</div> </div>



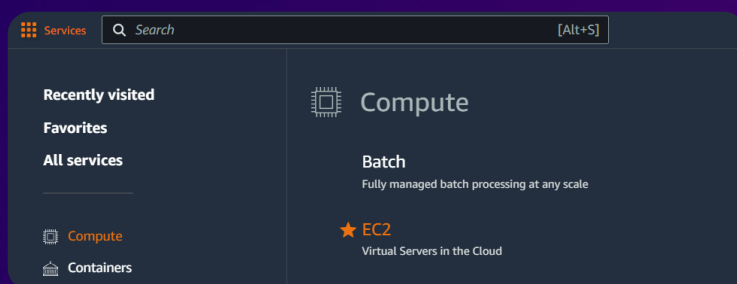


Task 3

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.

Instances (1) Info

Find Instance by attribute or tag (case-sensitive)

All states

Refresh

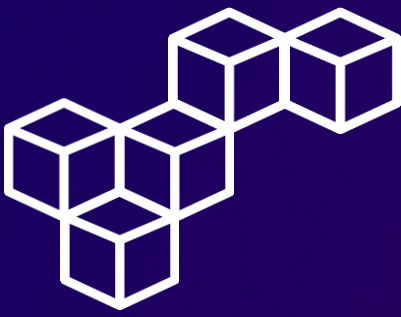
Connect

Instance state

Actions

Launch instances

<input type="checkbox"/>	Name	Instance ID	Instance state	Status check	Availability Zone	Public IPv4 ...	Private IP address
<input type="checkbox"/>	Web Server	i-08a02d19233b3ce8a	Running	2/2 checks passed	us-west-2a	52.35.96.241	10.0.0.26

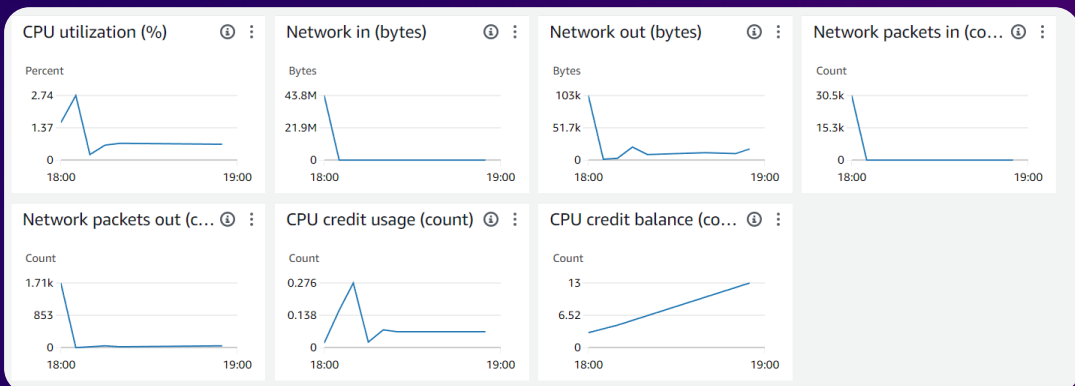


Task 3

Monitoring instance metrics using CloudWatch

Step 3: Monitoring

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

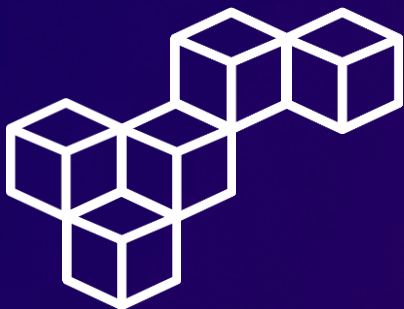


Step 4: device, fstype, host, path metrics

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.

The screenshot shows the CloudWatch Metrics console with the following table of metrics:

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.

The screenshot shows the AWS CloudWatch Metrics console. The breadcrumb navigation is Oregon > All > CWAgent > host. The search bar contains the text "Search for any metric, dimension, resource id or account id". Below the search bar, there is a table with the following data:

<input type="checkbox"/>	host 2/2	Metric name	Alarms
<input type="checkbox"/>	ip-10-0-0-26.us-west-2.compute.internal	mem_used_percent ⓘ	No alarms
<input type="checkbox"/>	ip-10-0-0-26.us-west-2.compute.internal	swap_used_percent ⓘ	No alarms

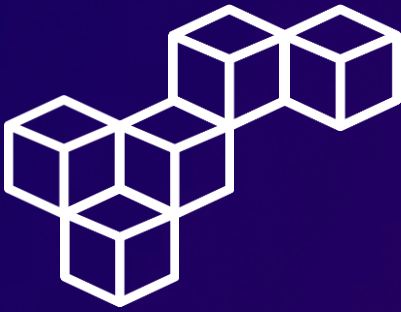
Step 6: Review all Metrics

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.

The screenshot shows the AWS CloudWatch Metrics console with the "All" namespace selected. The search bar contains the text "Search for any metric, dimension, resource id or account id". Below the search bar, there is a table with the following data:

Custom namespaces	
CWAgent 17	LogMetrics 1

AWS namespaces			
EBS 10 • View automatic dashboard	EC2 20 • View automatic dashboard	Events 8 • View automatic dashboard	Logs 18 • View automatic dashboard
SNS 4 • View automatic dashboard	SSM Run Command 3 • View automatic dashboard	Usage 86 • View automatic dashboard	



Task 4

Creating real time notifications

Step 1: Create rule

Navigate to the **Rules** section, and choose [Create rule](#).

Rules (3)				
<div><div>Find rules</div><div>Any status</div></div>				
<div><div>< 1 ></div><div></div></div>				
<input type="checkbox"/>	Name	Status	Type	Description
<input type="checkbox"/>	voc-rds-cw-rule	Enabled	Standard	rds all events
<input type="checkbox"/>	voc-ec2-cw-rule	Enabled	Standard	ec2 state change events
<input type="checkbox"/>	voc-codebuild-cw-rule	Enabled	Standard	codebuild build state change events

Step 2: Rule detail

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

Rule detail

Name

Instance_Stopped_Terminated



Task 4

Creating real time notifications

Step 3: Event pattern

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

The screenshot shows the 'Event pattern' configuration page in the AWS EventBridge console. The 'Event source' is set to 'AWS services'. The 'AWS service' is set to 'EC2'. The 'Event type' is set to 'EC2 Instance State-change Notification'. Under 'Event Type Specification 1', the 'Specific state(s)' option is selected, and the states 'stopped' and 'terminated' are listed. The 'Event pattern' section shows a JSON pattern:

```
1 {
2   "source": ["aws.ec2"],
3   "detail-type": ["EC2 Instance State-change Notification"],
4   "detail": {
5     "state": ["stopped", "terminated"]
6   }
7 }
```

 Buttons for 'Copy', 'Test pattern', and 'Edit pattern' are visible at the bottom right of the pattern section.

Step 4: Target 1

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

The screenshot shows the 'Target 1' configuration page in the AWS EventBridge console. The 'Select a target' dropdown is set to 'SNS topic'. The 'Topic' dropdown is set to 'Default_CloudWatch_Alarms_Topic'. A refresh button is visible next to the topic dropdown.



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](#).

Topics (1)			
<input type="text" value="Search"/>		Edit	Delete
		Publish message	Create topic
< 1 > ⚙			
Name	Type	ARN	
Default_CloudWatch_Alarms_Topic	Standard	arn:aws:sns:us-west-2:905418066767:Default_C...	

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

Subscriptions (1)

Edit

Delete

Request confirmation

Confirm subscription

Create subscription

Search

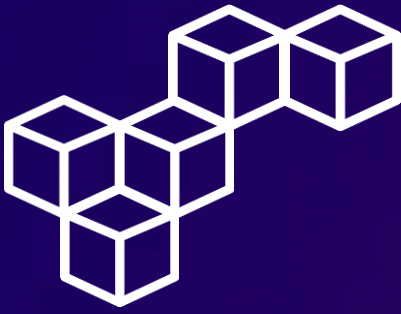
<

1

>

⚙

	ID	Endpoint	Status	Protocol
<input type="radio"/>	fc03cffc-aae3-4e70-bc0f-fddbaf3c8b61	cristhianbecerra99@gmail.com	<div><div></div>Confirmed</div>	EMAIL



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.

Instances (1) Info							Connect	Instance state ▼	Actions ▼	Launch instances ▼
Find Instance by attribute or tag (case-sensitive)							All states ▼	< 1 > ⚙		
<input type="checkbox"/>	Name ↗	Instance ID	Instance state ▼	Status check	Availability Zone ▼	Public IPv4 ... ▼	Private IP address ▼			
<input type="checkbox"/>	Web Server	i-08a02d19233b3ce8a	⏻ Stopped 🔍	-	us-west-2a	-	10.0.0.26			

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 Notification Message ▶ Inbox x



AWS Notifications <no-reply@sns.amazonaws.com>
to me ▼

{
 "version": "0",
 "id": "40816bcf-474e-1de9-2839-4063d754c82f",
 "detail-type": "EC2 Instance State-change Notification",
 "source": "aws.ec2",
 "account": "905418066767",
 "time": "2024-06-01T19:21:30Z",
 "region": "us-west-2",
 "resources": [{"arn": "aws:ec2:us-west-2:905418066767:instance/i-08a02d19233b3ce8a"}],
 "detail": {"instance-id": "i-08a02d19233b3ce8a", "state": "stopped"}
}

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:

https://sns.us-west-2.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-2:905418066767:Default_CloudWatch_Alarms_Topic_fc03cfc-aae3-4e70-bc0f-fddbfaf3c8b61&Endpoint=cristhianbecerra99@gmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

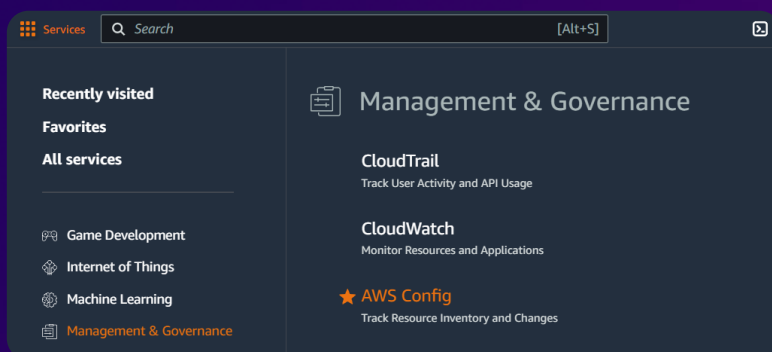


Task 5

Monitoring for infrastructure compliance

Step 1: Access the AWS Config service

In the AWS Management Console, select AWS Config.



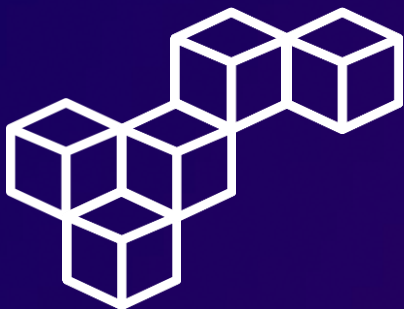
Step 2: Get started

Choose [Get started](#) > [Next](#) > [Next](#) > [Confirm](#). This configures AWS Config for initial use.

Set up AWS Config

A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.

[Get started](#)[1-click setup](#)

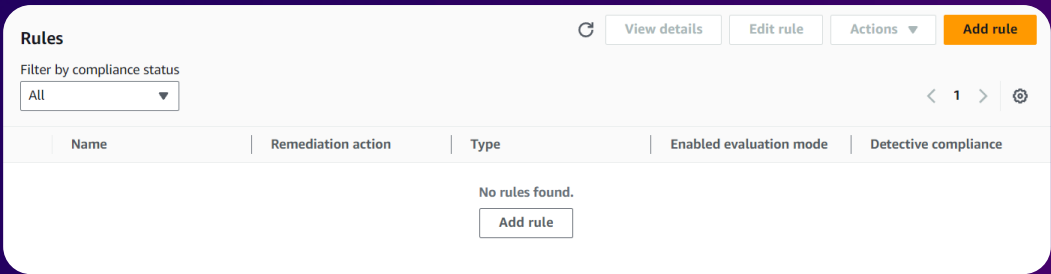


Task 5

Monitoring for infrastructure compliance

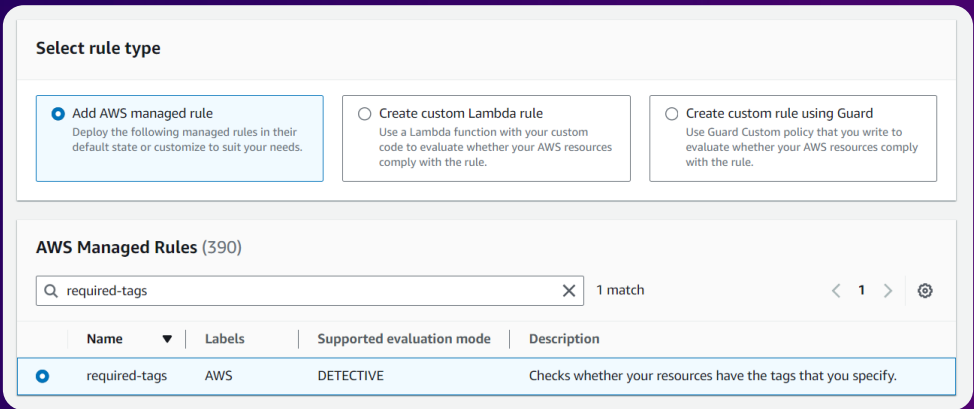
Step 3: Add rule

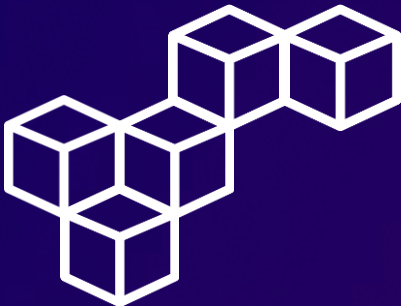
Navigate to the **Rules** section, and select [Add rule](#).



Step 4: Select rule

In the **Select rule type** section, select [Add AWS managed rule](#).
In the **AWS Managed Rules** section, select [required-tags](#).





Task 5

Monitoring for infrastructure compliance

Step 5: Parameters

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

Parameters
Rule parameters define attributes that your resources must adhere to for compliance with the rule. Example attributes include a required tag or a specified S3 bucket. **Optional** parameters that are not valid, such as missing a key or a value, will not be saved.

Key	Value
<input type="text" value="tag1Key"/>	<input type="text" value="project"/>

Step 6: Add rule

In to the **Rules** section, select [Add rule](#).

Rules

Filter by compliance status

All

< 1 >

⚙

View details

Edit rule

Actions

Add rule

Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
<input type="radio"/> required-tags	Not set	AWS managed	DETECTIVE	⚠ 14 Noncompliant resource(s)



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**.

Select rule type

☒ Add AWS managed rule
Deploy the following managed rules in their default state or customize to suit your needs.

☐ Create custom Lambda rule
Use a Lambda function with your custom code to evaluate whether your AWS resources comply with the rule.

☐ Create custom rule using Guard
Use Guard Custom policy that you write to evaluate whether your AWS resources comply with the rule.

AWS Managed Rules (390)

ec2-volume-inuse-check

X

1 match

< 1 >

⚙

Name	Labels	Supported evaluation mode	Description
<input checked="" type="radio"/> ec2-volume-inuse-check	EC2	DETECTIVE	Checks whether EBS volumes are attached to EC2 instances.

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.

Rules

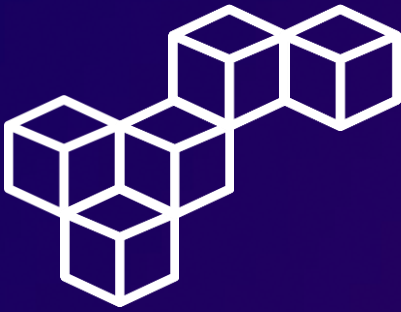
Filter by compliance status

All

< 1 >

⚙

	Name	Remediation action	Type	Enabled evaluation mode	Detective compliance
<input type="radio"/>	required-tags	Not set	AWS managed	DETECTIVE	⚠ 21 Noncompliant resource(s)
<input type="radio"/>	ec2-volume-inuse-check	Not set	AWS managed	DETECTIVE	⚠ 1 Noncompliant resource(s)



Task 5

Monitoring for infrastructure compliance

Step 9: required-tags

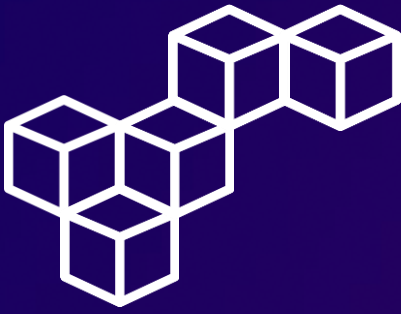
In the **Resources in scope** section, select **Compliant**.

Resources in scope						View details	Remediate	
Noncompliant						< 1 2 ... > ⚙		
	ID	Type	Status	Annotation	Compliance			
<input type="radio"/>	igw-07f796089ddf752a6	EC2 InternetGateway	-	-	⚠ Noncompliant			
<input type="radio"/>	igw-0a7f7ec6a411af7e4	EC2 InternetGateway	-	-	⚠ Noncompliant			
<input type="radio"/>	acl-08673f775d0f9cb6a	EC2 NetworkAcl	-	-	⚠ Noncompliant			
<input type="radio"/>	acl-0f32357b6ff4850b5	EC2 NetworkAcl	-	-	⚠ Noncompliant			
<input type="radio"/>	eni-04fa8ae95ab9e00a4	EC2 NetworkInterface	-	-	⚠ Noncompliant			
<input type="radio"/>	rtb-0082ec1e053746cf1	EC2 RouteTable	-	-	⚠ Noncompliant			
<input type="radio"/>	rtb-040187449cbb5a946	EC2 RouteTable	-	-	⚠ Noncompliant			
<input type="radio"/>	rtb-0939380c18279d540	EC2 RouteTable	-	-	⚠ Noncompliant			
<input type="radio"/>	sg-04d5234aa282c1519	EC2 SecurityGroup	-	-	⚠ Noncompliant			
<input type="radio"/>	sg-04fdd60864616282e	EC2 SecurityGroup	-	-	⚠ Noncompliant			

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.

Resources in scope						View details	Remediate	
Compliant						< 1 > ⚙		
	ID	Type	Status	Annotation	Compliance			
<input type="radio"/>	i-08a02d19233b3ce8a	EC2 Instance	-	-	✅ Compliant			



Task 5

Monitoring for infrastructure compliance

Step 11: ec2-volume-inuse-check

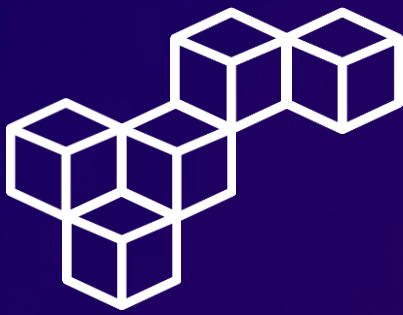
In the **Resources in scope** section, select **Compliant**.

Resources in scope					View details	Remediate	
Noncompliant					< 1 >		
ID	Type	Status	Annotation	Compliance			
vol-0080acd40cafd2792	EC2 Volume	-	-	Noncompliant			

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).

Resources in scope					View details	Remediate	
Compliant					< 1 >		
ID	Type	Status	Annotation	Compliance			
vol-03eae48a4425dd0d	EC2 Volume	-	-	Compliant			



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.



Cristhian Becerra



[cristhian-becerra-espinoza](#)



+51 951 634 354



cristhianbecerra99@gmail.com



Lima, Peru

