Compliance and Non Compliance in AWS

AWS Config helps you track the compliance status of our AWS resources by evaluating them against **AWS Config Rules** that define desired configurations or security policies.

1. Compliance in AWS

✅ **Compliance** means that an AWS resource (such as an EC2 instance, S3 bucket, or IAM policy) follows the rules and best practices defined in AWS Config.

- Example:
  - You create a rule stating that all EC2 Instance **must enabled detailed monitoring**.
  - If an EC2 Instance has enabled detailed monitoring, it is considered **compliant**.

2. Non-Compliance in AWS

❌ **Non-Compliance** means that an AWS resource does not meet the required security, governance, or operational policies defined in AWS Config Rules.

- Example:
  - A rule is set to ensure that all EC2 instances **must be within a specific VPC**.
  - If an EC2 instance is found outside the required VPC, AWS Config marks it as **non-compliant**.

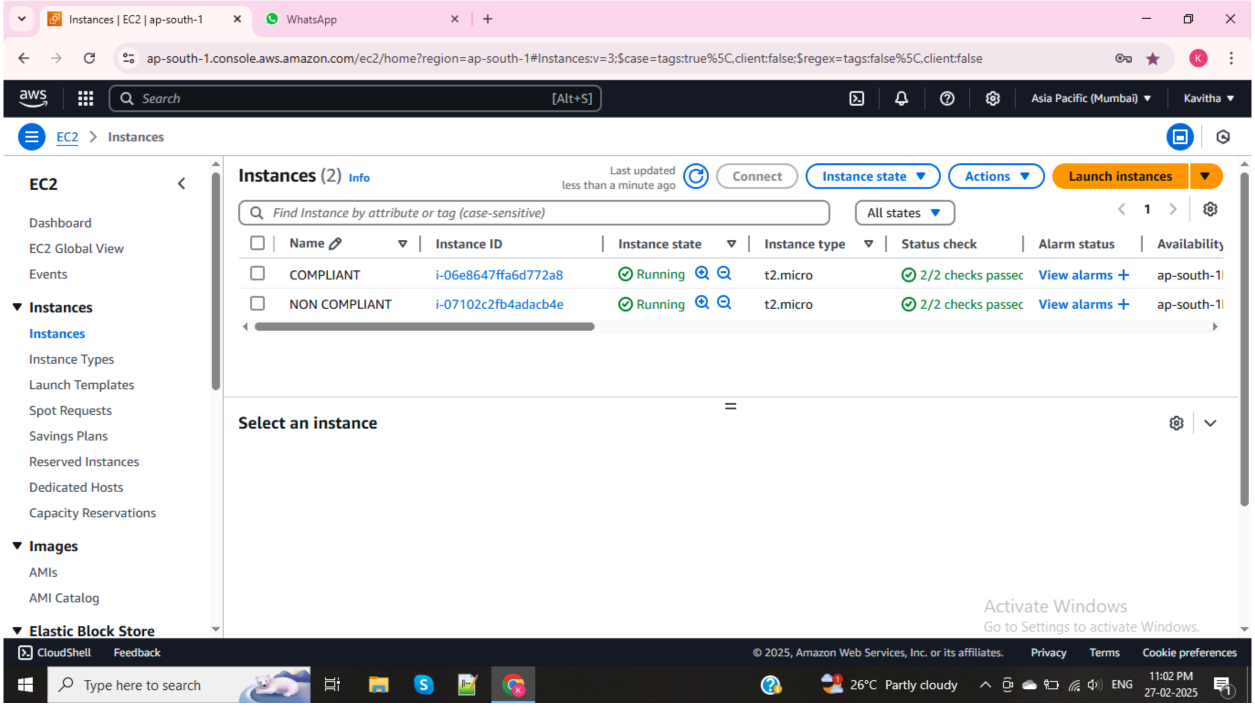
How AWS Config Evaluates Compliance

1. AWS Config **continuously** monitors resources.
2. It compares resource configurations against predefined **AWS Config Rules**.
3. If a resource matches the rule → **Compliant** ✅
   If it does not match → **Non-Compliant** ❌

TASK : Creating a rule stating that all EC2 Instances **must enable detailed monitoring**.

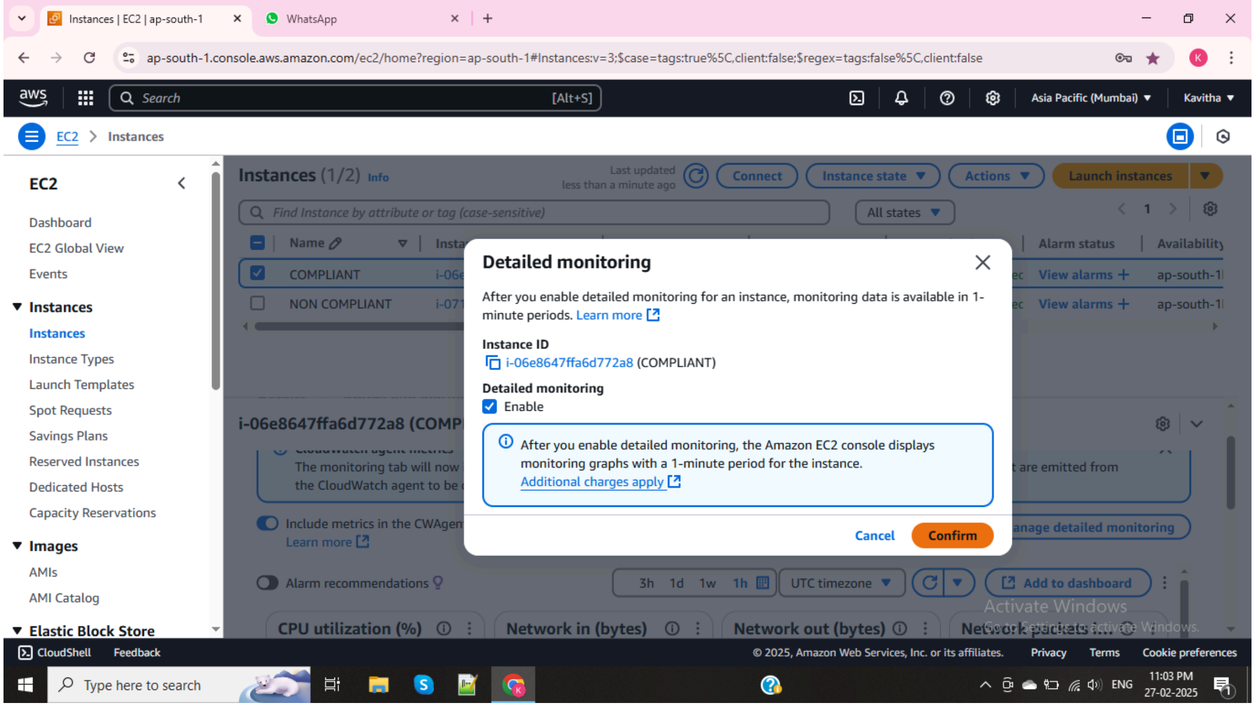
Go to **EC2 Instance** in the AWS Management Console. Creating two EC2 Instances named as **Compliance and Non compliance.**

EC2 Instance created successfully



□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
□	COMPLIANT	i-06e8647ffa6d772a8	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1
□	NON COMPLIANT	i-07102c2fb4adacb4e	Running	t2.micro	2/2 checks passec	View alarms +	ap-south-1

For Compliance Instance **enabled the Detailed Monitoring**



Detailed monitoring

After you enable detailed monitoring for an instance, monitoring data is available in 1-minute periods. Learn more

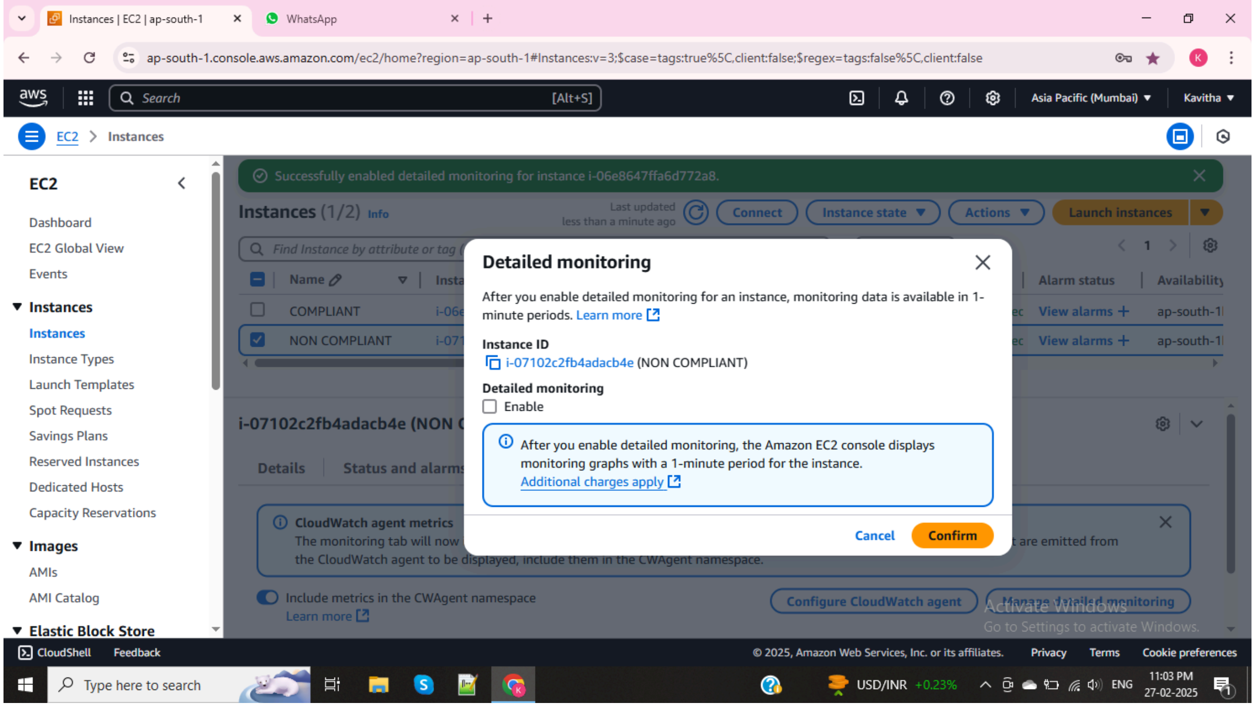
Instance ID
i-06e8647ffa6d772a8 (COMPLIANT)

Detailed monitoring
☑ Enable

After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance.
Additional charges apply

Cancel Confirm

For Non Compliance instance **Detailed monitoring was not enabled**



Successfully enabled detailed monitoring for instance i-06e8647ffa6d772a8.

The monitoring tab will now ... the CloudWatch agent to be displayed, include them in the CWAgent namespace. ... are emitted from

Detailed monitoring

After you enable detailed monitoring for an instance, monitoring data is available in 1-minute periods. Learn more

Instance ID
i-07102c2fb4adacb4e (NON COMPLIANT)

Detailed monitoring
☐ Enable

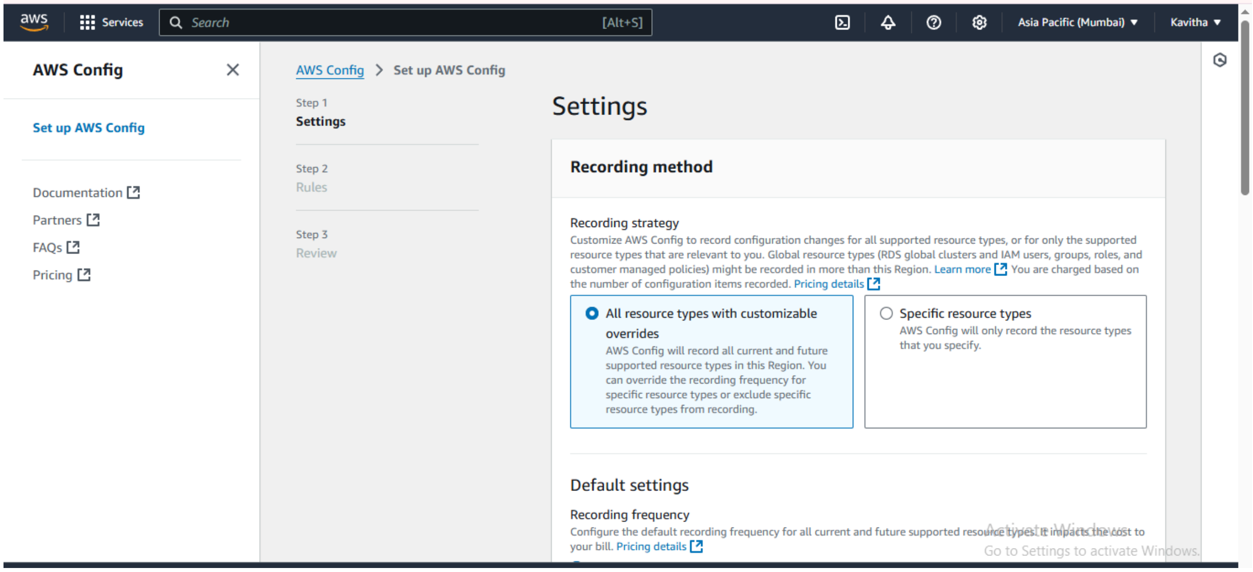
After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance.
Additional charges apply

Cancel Confirm

Now, Go to **AWS CONFIG**

1. Set up AWS Config:

- **If this is your first time setting up AWS Config, you'll be prompted to set it up.**
- **Click on Get started to begin the setup process.**



Settings

Recording method

Recording strategy

Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Global resource types (RDS global clusters and IAM users, groups, roles, and customer managed policies) might be recorded in more than this Region. Learn more You are charged based on the number of configuration items recorded. Pricing details

● All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

○ Specific resource types
AWS Config will only record the resource types that you specify.

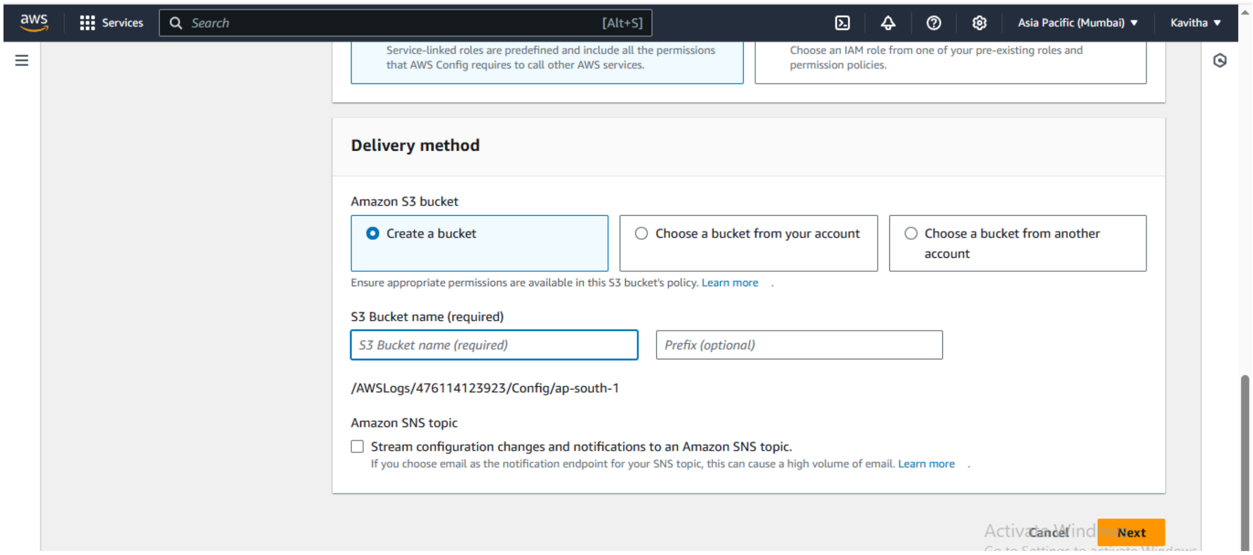
Default settings

Recording frequency

Configure the default recording frequency for all current and future supported resource types. It impacts the cost to your bill. Pricing details

2. Choose Resource Types:

- AWS Config lets you track configuration changes for different resource types. Select the **Resources** you want to monitor. You can select specific resources like EC2 instances, S3 buckets, VPCs, etc.



Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.

Choose an IAM role from one of your pre-existing roles and permission policies.

Delivery method

Amazon S3 bucket

● Create a bucket ○ Choose a bucket from your account ○ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. Learn more .

S3 Bucket name (required)

S3 Bucket name (required) | Prefix (optional)

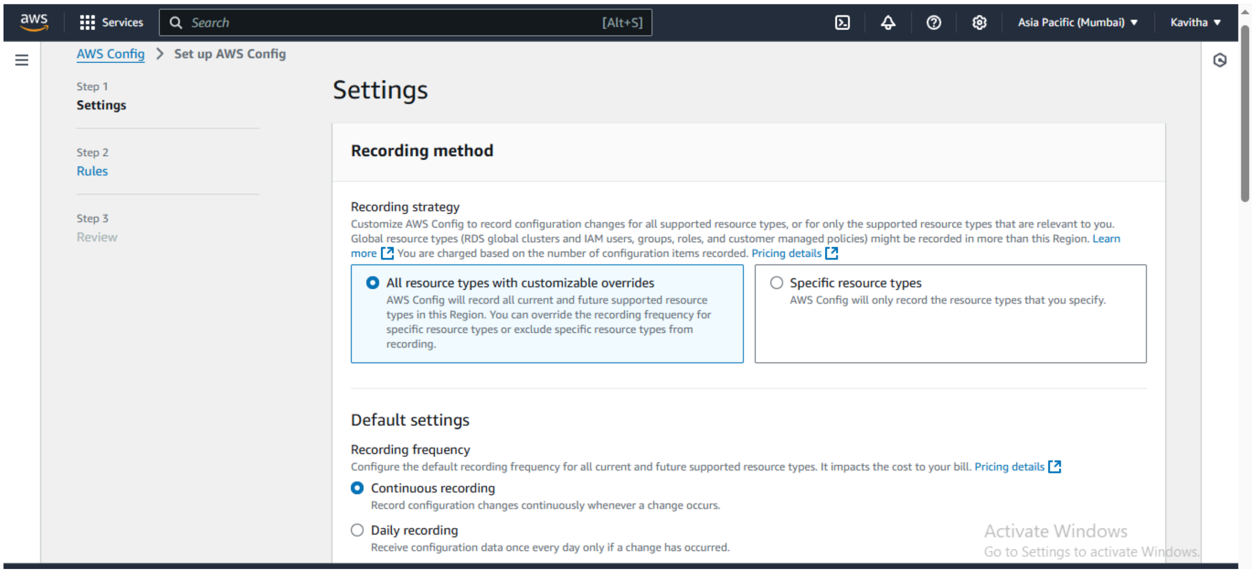
/AWSLogs/476114123923/Config/ap-south-1

Amazon SNS topic

□ Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more .

3. Set Recording Settings:

- You will be asked to choose whether to record configuration changes for all resources or just specific types.
- To track all resources, select **Record all resources**.
- If you want to track specific resources, select **Record selected resources** and choose which types to monitor.



Settings

Recording method

Recording strategy

Customize AWS Config to record configuration changes for all supported resource types, or for only the supported resource types that are relevant to you. Global resource types (RDS global clusters and IAM users, groups, roles, and customer managed policies) might be recorded in more than this Region. Learn more You are charged based on the number of configuration items recorded. Pricing details

● All resource types with customizable overrides
AWS Config will record all current and future supported resource types in this Region. You can override the recording frequency for specific resource types or exclude specific resource types from recording.

○ Specific resource types
AWS Config will only record the resource types that you specify.

Default settings

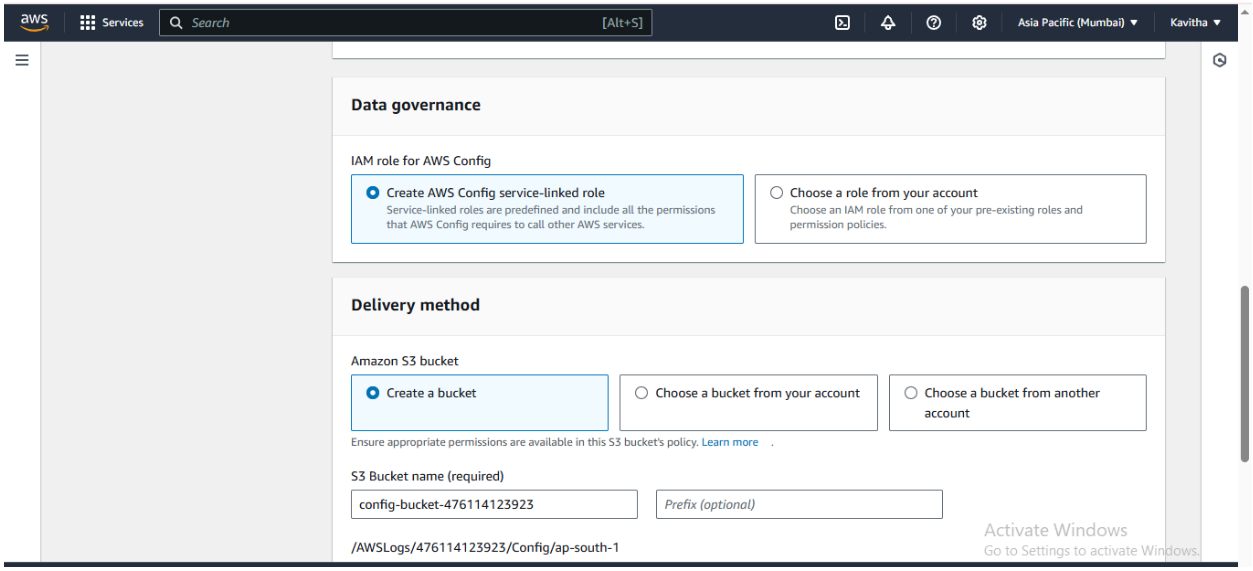
Recording frequency

Configure the default recording frequency for all current and future supported resource types. It impacts the cost to your bill. Pricing details

● Continuous recording
Record configuration changes continuously whenever a change occurs.

○ Daily recording
Receive configuration data once every day only if a change has occurred.

4. After configuring the settings, review everything > click **Confirm** to complete the setup.



Data governance

IAM role for AWS Config

● Create AWS Config service-linked role
Service-linked roles are predefined and include all the permissions that AWS Config requires to call other AWS services.

○ Choose a role from your account
Choose an IAM role from one of your pre-existing roles and permission policies.

Delivery method

Amazon S3 bucket

● Create a bucket

○ Choose a bucket from your account

○ Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. Learn more .

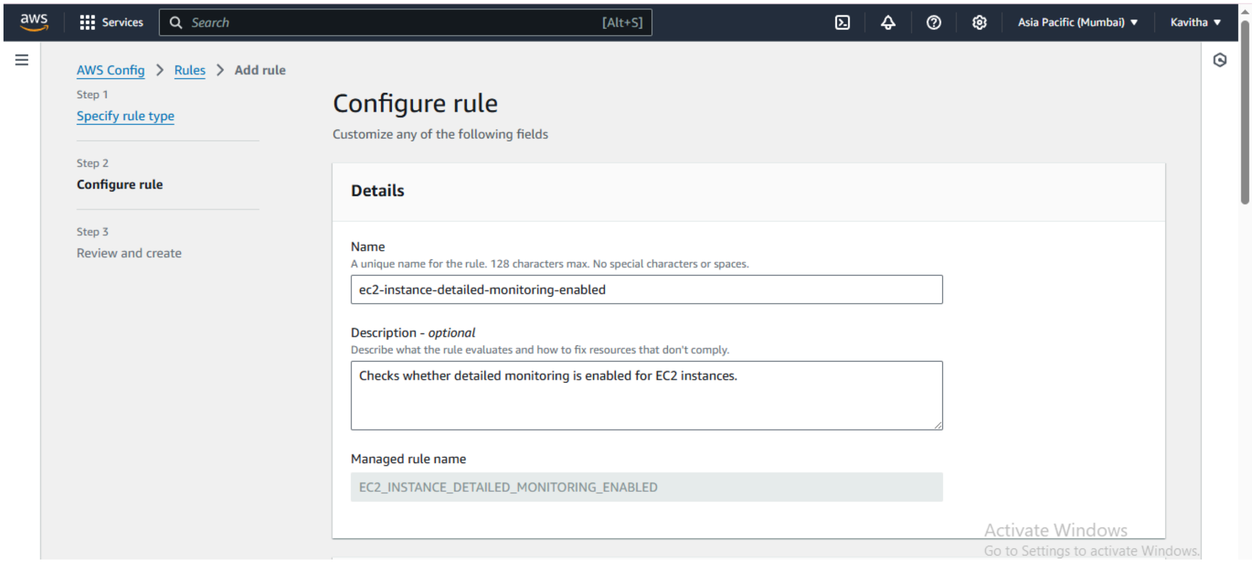
S3 Bucket name (required)

config-bucket-476114123923 | *Prefix (optional)*

/AWSLogs/476114123923/Config/ap-south-1

AWS Rule was selected from **AWS Managed Rules.**

Checks whether **detailed monitoring is enabled for All EC2 Instance**



Configure rule

Customize any of the following fields

Details

Name

A unique name for the rule. 128 characters max. No special characters or spaces.

ec2-instance-detailed-monitoring-enabled

Description - *optional*

Describe what the rule evaluates and how to fix resources that don't comply.

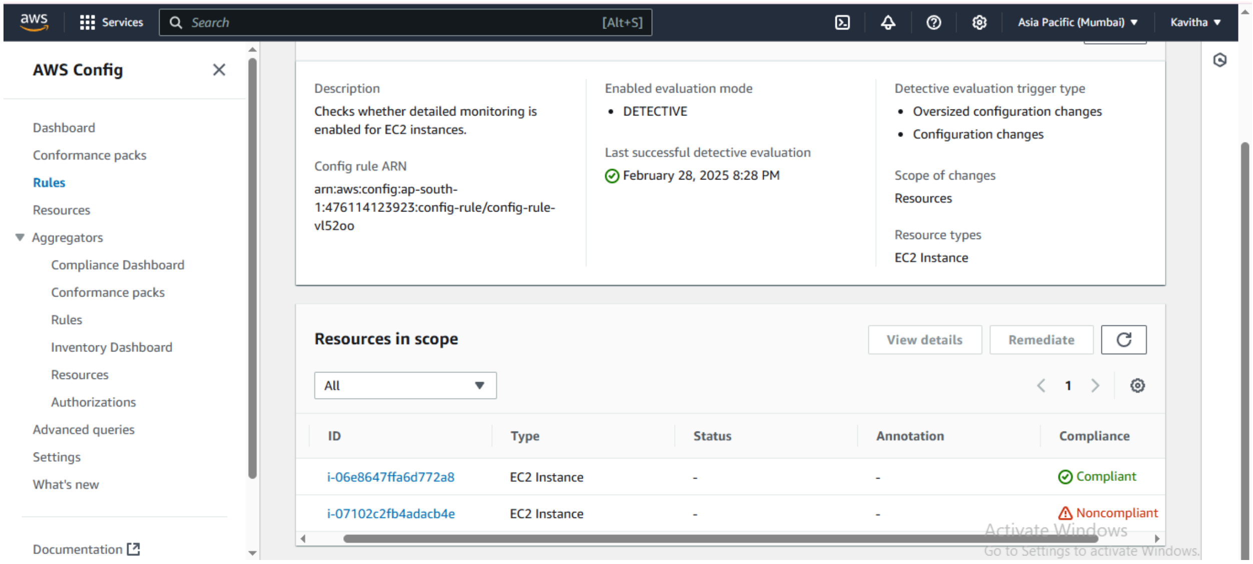
Checks whether detailed monitoring is enabled for EC2 instances.

Managed rule name

EC2_INSTANCE_DETAILED_MONITORING_ENABLED

Click Rule go to actions > click **re-valuate** for results

Its shows Compliance and Non compliance in **Resources in Scope** (choose All in drop down).



Description

Checks whether detailed monitoring is enabled for EC2 instances.

Config rule ARN

arn:aws:config:ap-south-1:476114123923:config-rule/config-rule-vl52oo

Enabled evaluation mode

- DETECTIVE

Last successful detective evaluation

✓ February 28, 2025 8:28 PM

Detective evaluation trigger type

- Oversized configuration changes
- Configuration changes

Scope of changes

Resources

Resource types

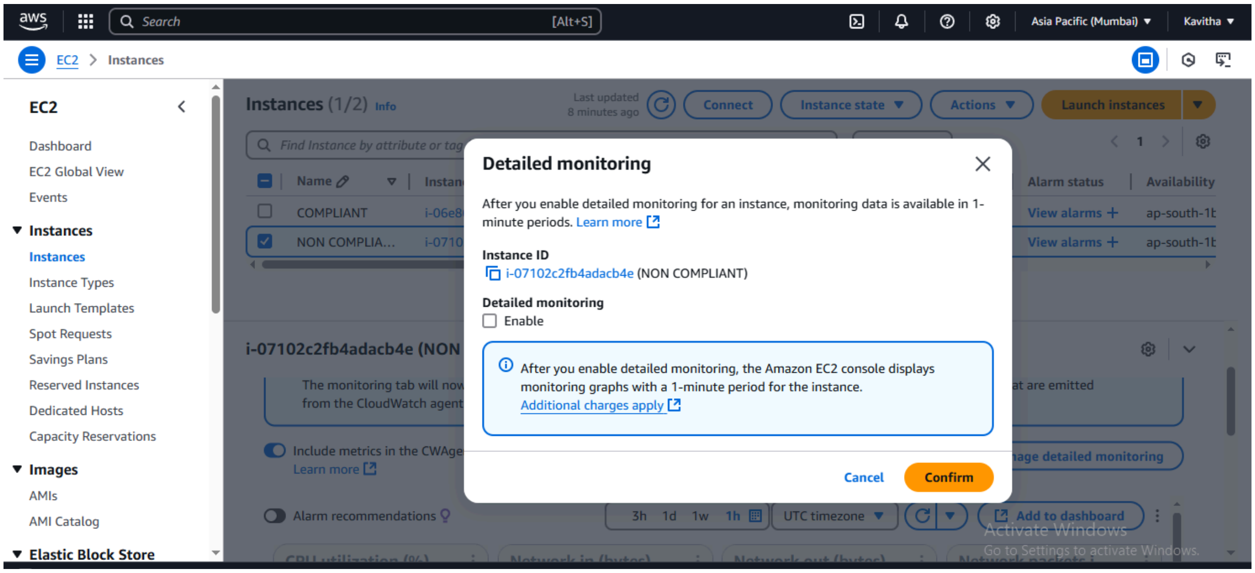
EC2 Instance

Resources in scope

All ▼

ID	Type	Status	Annotation	Compliance
i-06e8647ffa6d772a8	EC2 Instance	-	-	✓ Compliant
i-07102c2fb4adacb4e	EC2 Instance	-	-	⚠ Noncompliant

From this list **Note the Non compliance EC2 Instance ID** then go to EC2 Instance enable the detailed monitoring.



Detailed monitoring

After you enable detailed monitoring for an instance, monitoring data is available in 1-minute periods. Learn more

Instance ID
i-07102c2fb4adacb4e (NON COMPLIANT)

Detailed monitoring
☐ Enable

After you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period for the instance.
Additional charges apply

Examples of AWS Config Rules for Compliance

Rule Name	Description	Compliance Criteria
`s3-bucket-public-read-prohibited`	Ensures S3 buckets are **not publicly accessible**	Compliant if bucket is private
`ec2-instance-managed-by-ssm`	Ensures EC2 instances are managed by AWS Systems Manager	Compliant if instance is managed
`iam-user-no-inline-policies`	Ensures IAM users do not have inline policies	Compliant if no inline policies exist

Automating Non-Compliance Remediation

If a resource is **non-compliant**, AWS Config can trigger:

- **AWS Systems Manager Automation** (to fix the issue)
- **Lambda functions** (to remediate automatically)
- **SNS notifications** (to alert administrators)