# **Table of Contents**

[Table of Contents 1](#_Toc184393490)

[Cloud Watch 2](#_Toc184393491)

[**High-level steps** 2](#_Toc184393492)

[**Assign an IAM Role to the EC2 Instance** 2](#_Toc184393493)

[**Attach the IAM Role to the EC2 Instance** 4](#_Toc184393494)

[**Install the CloudWatch Agent on the EC2 Instance** 5](#_Toc184393495)

[**Verify Logs in CloudWatch** 7](#_Toc184393496)

[**Install httpd and check the details in CloudWatch** 8](#_Toc184393497)

[**Export logs from CloudWatch Logs to an S3 bucket** 8](#_Toc184393498)

[**Create S3 Bucket** 8](#_Toc184393499)

[**CloudWatch Logs Export** 10](#_Toc184393500)

[**Verify Logs in S3** 12](#_Toc184393501)

# Cloud Watch

Amazon CloudWatch is a service that monitors applications, responds to performance changes, optimizes resource use, and provides insights into operational health. By collecting data across AWS resources, CloudWatch gives visibility into system-wide performance and allows users to set alarms, automatically react to changes, and gain a unified view of operational health.

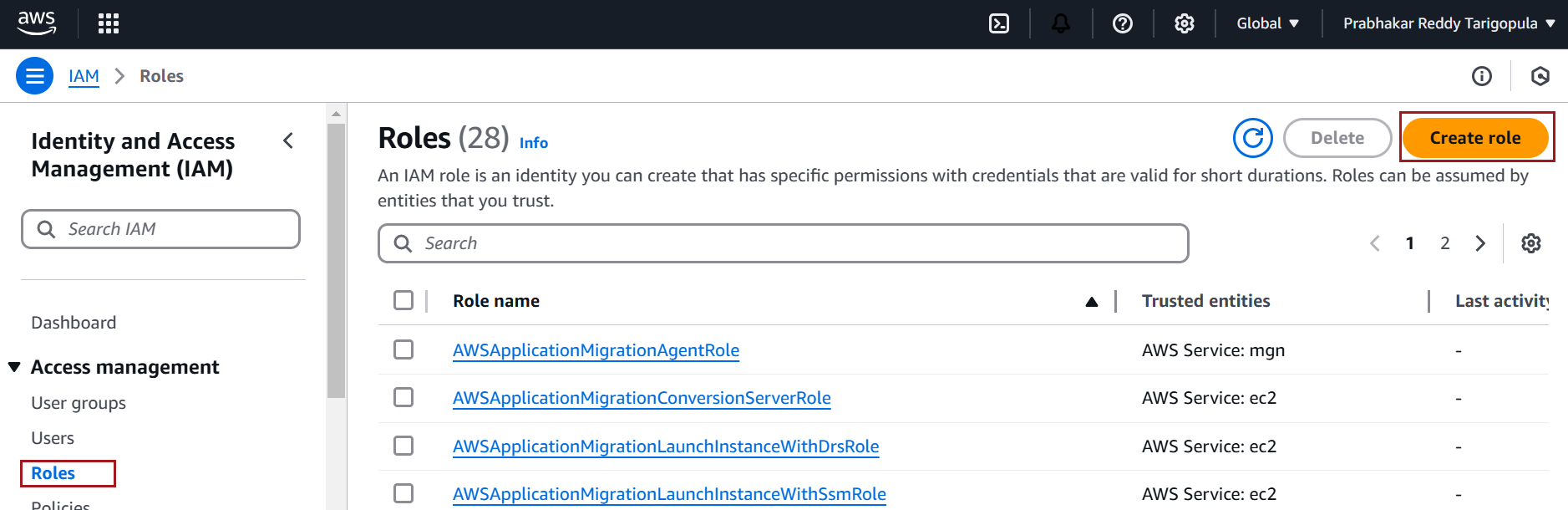
To install the CloudWatch agent on an EC2 instance and configure it to send all logs to Amazon CloudWatch, follow these steps

### **High-level steps**

1. Assign an IAM Role to the EC2 Instance
2. Install the CloudWatch Agent on the EC2 Instance
3. Configure the CloudWatch Agent
4. Verify Logs in CloudWatch

### **Assign an IAM Role to the EC2 Instance**

Open the **IAM Management Console,** Click **Roles** → **Create Role**



Select **AWS Service** → **EC2** → **Next**

A screenshot of a computer

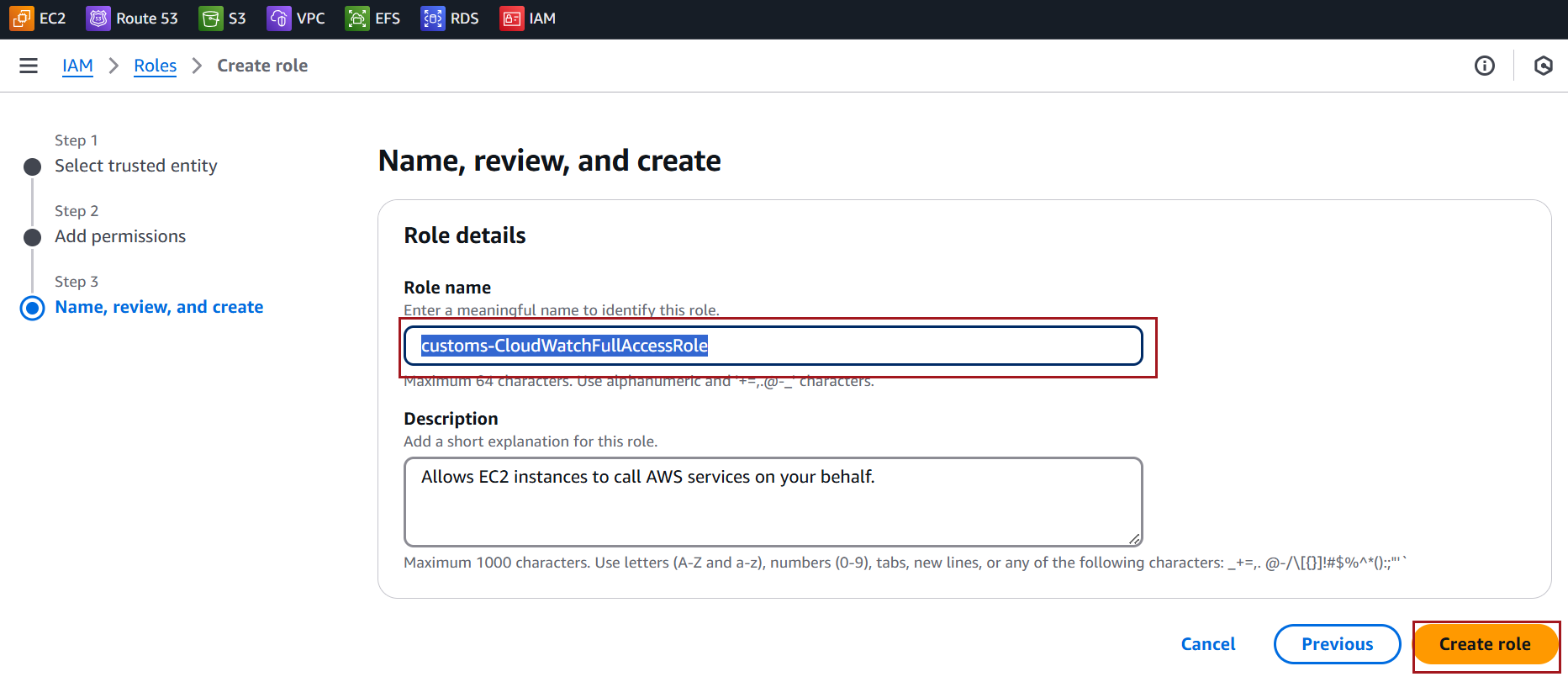
Description automatically generated

Attach the [CloudWatchAgentServerPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentServerPolicy) managed policy

A screenshot of a computer

Description automatically generated

Provide a name for the role, e.g. customs-CloudWatchFullAccessRole, and create the role.



### **Attach the IAM Role to the EC2 Instance**

Select the EC2 instance where you want to install the CloudWatch agent.

Click **Actions** → **Security** → **Modify IAM Role**.

A screenshot of a computer

Description automatically generated

Select the IAM role you just created and click **Update IAM Role**

A screenshot of a computer

Description automatically generated

### **Install the CloudWatch Agent on the EC2 Instance**

Connect to the EC2 Instance and run the command below to install couldwatch Agent

sudo yum install amazon-cloudwatch-agent -y

A screenshot of a computer

Description automatically generated

Create a Configuration File using below command

sudo vi /opt/aws/amazon-cloudwatch-agent/bin/config.json

A screenshot of a computer

Description automatically generated

Add the following configuration to capture **all logs**

{

"logs": {

"logs\_collected": {

"files": {

"collect\_list": [

{

"file\_path": "/var/log/\*",

"log\_group\_name": "ec2-all-logs",

"log\_stream\_name": "{instance\_id}-all-logs"

}

]

}

}

}

}

Start the agent using the configuration file:

sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s

A screenshot of a computer

Description automatically generated

Logs typically appear in CloudWatch within **2 to 5 minutes** of enabling the agent, depending on the configuration and volume of logs being generated

### **Verify Logs in CloudWatch**

Open the **CloudWatch Console** in the AWS Management Console

Navigate to **Logs** → **Log Groups**

A screenshot of a computer

Description automatically generated

Select a log group and view log streams for your EC2 instance

A screenshot of a computer

Description automatically generated

### **Install httpd and check the details in CloudWatch**

sudo yum install httpd -y

A screenshot of a computer

Description automatically generated

Verify the httpd log in cloudwatch

A screenshot of a computer

Description automatically generated

### **Export logs from CloudWatch Logs to an S3 bucket**

#### **Create S3 Bucket**

Navigate to the **S3** service

Click **Create bucket after entering Bucket Name** and leave other defaults

A screenshot of a computer

Description automatically generated

Go to the bucket's **Permissions** tab

A screenshot of a computer

Description automatically generated

**Go to Bucket Policy**. Click **Edit**

A screenshot of a computer

Description automatically generated

**Add the following policy:**

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "AllowCloudWatchLogs",

"Effect": "Allow",

"Principal": {

"Service": "logs.amazonaws.com"

},

"Action": [

"s3:PutObject",

"s3:GetBucketAcl",

"s3:GetObject"

],

"Resource": [

"arn:aws:s3:::my-cloudwatch-logs-bucket-pr/\*",

"arn:aws:s3:::my-cloudwatch-logs-bucket-pr"

]

}

]

}

Click on **Save Changes**

A screenshot of a computer

Description automatically generated

#### **CloudWatch Logs Export**

Navigate to **Logs** → **Log Groups**

Choose the log group you want to export

A screenshot of a computer

Description automatically generated

Click on **Actions** → **Export data to Amazon S3**

A screenshot of a computer

Description automatically generated

Choose your S3 bucket name and Click on **Export**

A screenshot of a computer

Description automatically generated

#### **Verify Logs in S3**

Open the bucket and check for logs in the specified folder or directly at the root

A screenshot of a computer

Description automatically generated

You should see files in .gz format, as CloudWatch compresses the exported logs.

A screenshot of a computer

Description automatically generated