National College of Ireland

Configuration Manual

MSc Research Project
Cloud Computing

Pranav Patil
Student ID:23193867

School of Computing
National College of Ireland

Supervisor: Shreyas Setlur Arun

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Pranav Patil
Student ID:	23193867
Programme:	Cloud Computing
Year:	2024
Module:	MSc Research Project
Supervisor:	Shreyas Setlur Arun
Submission Due Date:	12/12/2024
Project Title:	Designing and Implementing a Comprehensive Cloud Security Monitoring Tool with CloudWatch Logs and CloudWatch Console
Word Count:	1259
Page Count:	11

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Pranav Patil
Date:	23rd January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Pranav Patil
Student ID:23193867

1 Introduction

In today's cloud-centric landscape, ensuring the security and integrity of your AWS resources is paramount. Amazon CloudWatch offers a robust solution for monitoring, logging, and alerting, enabling comprehensive visibility into your cloud infrastructure. This manual guides you through designing and implementing a comprehensive cloud security monitoring tool using AWS CloudWatch Logs and the CloudWatch Console. By following these steps, you'll establish a secure, scalable, and efficient monitoring system tailored to your organization's needs.

2 Prerequisites

Before embarking on this implementation, ensure you have the following:

- An active AWS account with administrative privileges.
- Basic understanding of AWS services, especially IAM, EC2, and CloudWatch.
- AWS CLI installed and configured on your local machine.
- SSH client for accessing EC2 instances.

3 Step 1: IAM Role Creation and Policy Attachment

Proper IAM roles and policies are foundational for secure access management within AWS. This step involves creating an IAM role with the necessary permissions to allow CloudWatch to interact with various AWS services.

3.1 Creating the IAM Role

1. **Navigate to IAM Console:**
    - Log in to the AWS Management Console.
    - Go to Services ¿ **IAM**.
2. **Create a New Role:**
    - Click on **Roles** in the sidebar.

- Select **Create role**.

3. **Select Trusted Entity:**
   - Choose **AWS service**.
   - Under **Use case**, select **EC2**.
   - Click **Next: Permissions**.

3.2 Attaching IAM Policies

4. **Attach Managed Policies:**
   - In the policies list, search and select:
     - `CloudWatchReadOnlyAccess`
     - `S3ReadOnlyAccess`
     - `EC2ReadOnlyAccess`

5. **Review and Create:**
   - Click **Next: Tags** (optional to add tags).
   - Click **Next: Review**.
   - Name the role `cloudmonitorrole2024`.
   - Add a description, e.g., "Role for Cloud Monitoring with read-only access."
   - Click **Create role**.

3.3 Creating and Attaching a Custom Policy

6. **Create a Custom Policy:**
   - In the IAM console, navigate to **Policies**.
   - Click **Create policy**.
   - Select the **JSON** tab.

7. **Define the Policy:**

   Custom IAM Policy for CloudWatch Configuration

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                "ssm:GetParameter",
                "ssm:DeleteParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/CloudWatchConfig/*"
```

```
            }
        ]
    }
```

8. **Review and Create:**
    - Click **Next: Tags**.
    - Click **Next: Review**.
    - Name the policy `AllowSSMPutParameterForCloudWatchConfig`.
    - Add a description.
    - Click **Create policy**.
9. **Attach the Custom Policy to the Role:**
    - Navigate back to **Roles**.
    - Select `cloudmonitorrole2024`.
    - Click **Add permissions ¿ Attach policies**.
    - Search and select `AllowSSMPutParameterForCloudWatchConfig`.
    - Click **Attach policies**.

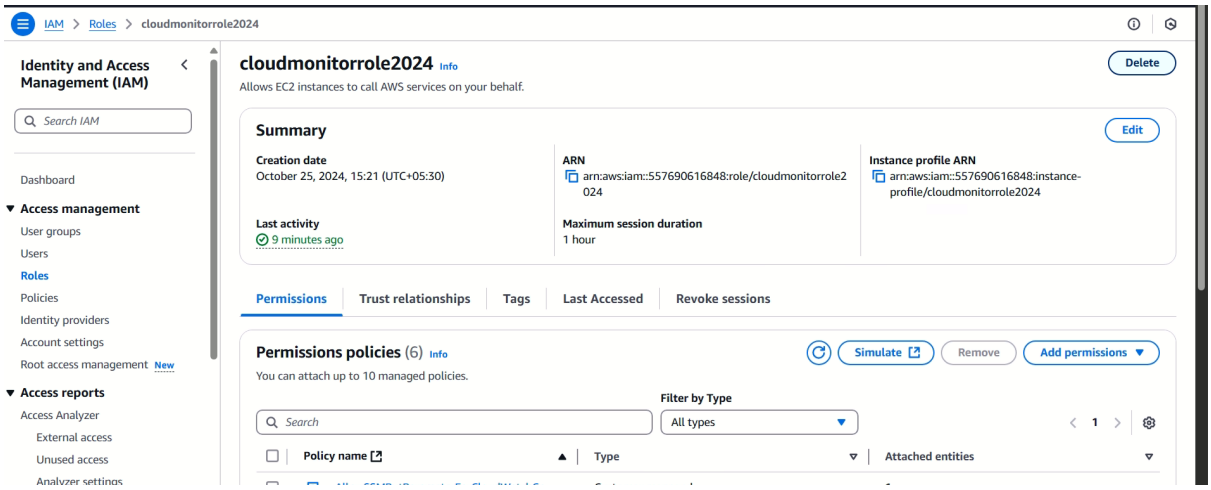

Figure 1: Figure 1: IAM Role Creation

4 Step 2: CloudWatch Log Groups Setup

Organizing logs into distinct log groups facilitates efficient monitoring and management. This step involves creating log groups for various AWS resources and configuring retention policies.

4.1 Creating Log Groups

1. **Access CloudWatch Console:**
   - Navigate to Services ¿ **CloudWatch**.
2. **Create Log Groups:**
   - In the sidebar, select **Logs ¿ Log groups**.
   - Click **Create log group**.
   - Create the following log groups:
     - `monitorloggroupec22024` for EC2 instance logs.
     - `monitorloggroups32024` for S3 bucket logs.
     - `monitorloggrouplambda2024` for Lambda function logs.

4.2 Configuring Retention Periods

3. **Set Retention Policy:**
   - For each log group, select it from the list.
   - Click **Actions ¿ Edit retention**.
   - Choose the desired retention period (e.g., 14 days for EC2 logs).
   - Click **Save**.

Figure 2: Figure 2: CloudWatch Log Groups

5 Step 3: EC2 Instance Launch and Configuration

Launching and configuring an EC2 instance serves as the foundation for deploying the CloudWatch agent, which collects and sends logs and metrics to CloudWatch.

5.1 Launching the EC2 Instance

1. **Navigate to EC2 Console:**
   - Go to Services ¿ **EC2**.
2. **Launch Instance:**
   - Click **Launch Instance**.
   - Choose an Amazon Machine Image (AMI), e.g., **Amazon Linux 2**.
   - Select an instance type, such as `t2.micro`.
   - Click **Next: Configure Instance Details**.
3. **Configure Instance Details:**
   - Assign the IAM role `cloudmonitorrole2024` to the instance.
   - Ensure **Auto-assign Public IP** is enabled.
   - Click **Next: Add Storage**.
4. **Add Storage and Tags:**
   - Configure as needed.
   - Add tags for identification, e.g., `Name: cloudmonitorec2server`.
   - Click **Next: Configure Security Group**.
5. **Configure Security Group:**
   - Allow SSH (port 22) from trusted IPs.
   - Allow necessary ports for CloudWatch agent.
   - Click **Review and Launch**.
6. **Review and Launch:**
   - Review settings.
   - Click **Launch**.

5.2 Creating and Storing Key Pair

7. **Create Key Pair:**
   - During the launch process, select **Create a new key pair**.
   - Name it `cloudmonitorkeypair`.
   - Click **Download Key Pair**.

- Save the `.pem` file securely.

8. **Secure Storage:**
   - Store `cloudmonitorkeypair.pem` in a secure location.
   - Set appropriate permissions (see Step 4).

5.3 Configuring CloudWatch Agent

After launching the EC2 instance, SSH into it to install and configure the CloudWatch agent.

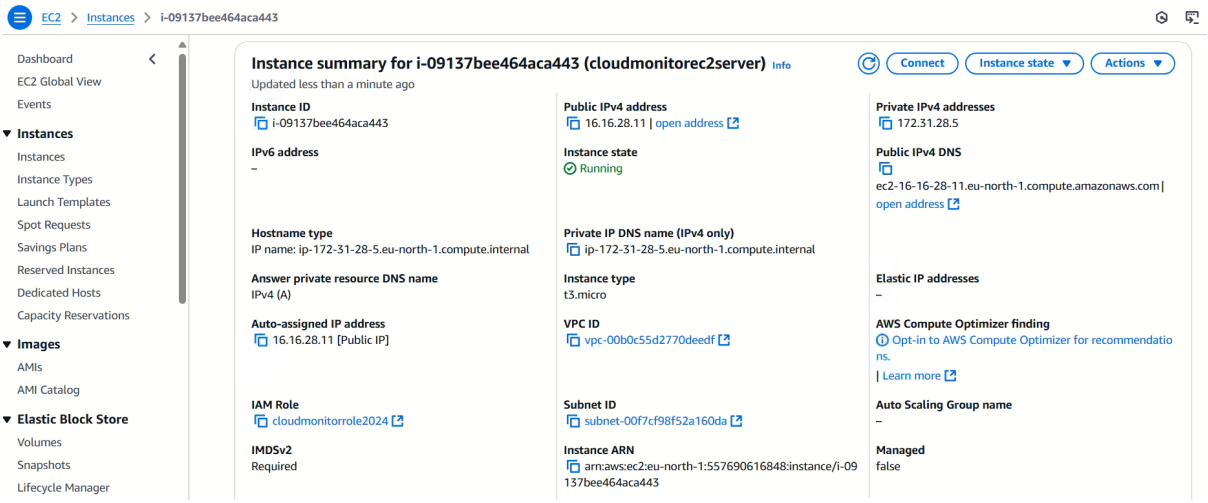

Figure 3: Figure 3: EC2 Instance Launch

6 Step 4: Secure SSH Key Setup

Securing the SSH key ensures that only authorized personnel can access the EC2 instance, mitigating potential security risks.

6.1 Restricting Key File Access

1. **Set Permissions:**
   - On your local machine, navigate to the directory containing `cloudmonitorkeypair.pem`.
   - Run the following command to restrict access:

     ```
     chmod 400 cloudmonitorkeypair.pem
     ```

2. **Verify Permissions:**
   - Ensure that the key file is readable only by the owner.
   - Use the `ls -l` command to verify:

     ```
     ls -l cloudmonitorkeypair.pem
     ```

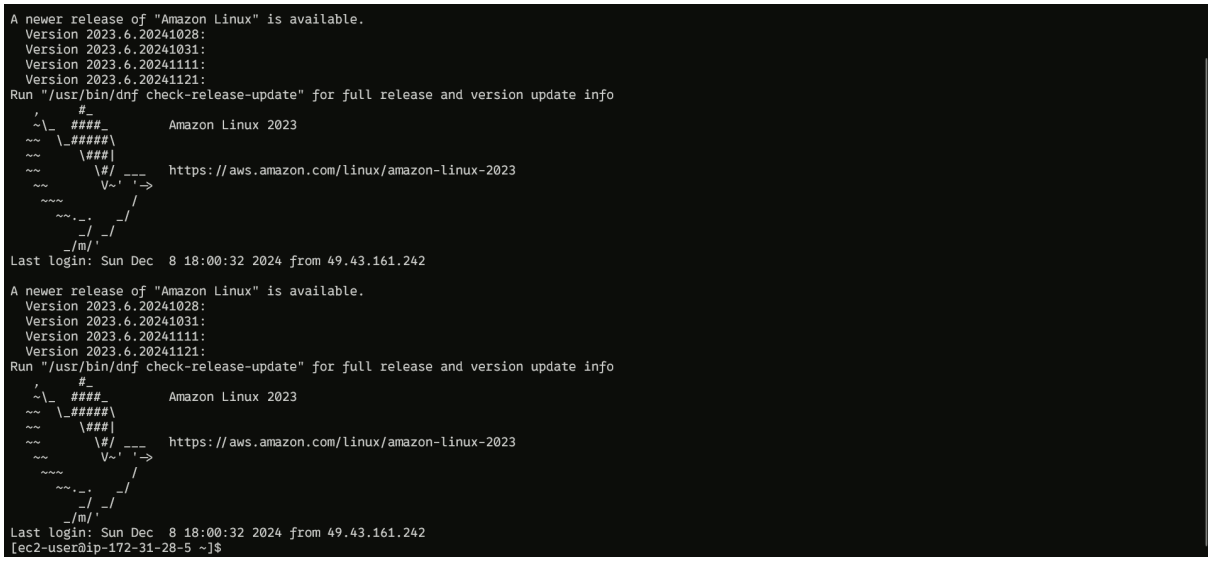

Figure 4: Figure 4: SSH Key Permissions

7 Step 5: CloudWatch Agent Installation and Configuration

Installing the CloudWatch agent on the EC2 instance enables the collection and transmission of system metrics and log data to CloudWatch.

7.1 Installing the CloudWatch Agent

1. **SSH into EC2 Instance:**

   Connect to your EC2 instance using the SSH key pair.

2. **Update Packages:**

   Ensure that all packages are up to date.

3. **Install the CloudWatch Agent:**

   Install the Amazon CloudWatch agent using the package manager.

7.2 Running Configuration Wizard

4. **Start Configuration Wizard:**

   Initiate the CloudWatch agent configuration wizard to guide you through the setup process.

5. **Follow Prompts:**

   - Specify metrics to collect (e.g., disk usage, memory usage).
   - Define log files to monitor (e.g., `/var/log/cloud-init.log`).
   - Choose to save the configuration to `config.json`.

8 Step 6: IAM Role Enhancements for CloudWatch Agent

Enhancing the IAM role ensures seamless integration with AWS Systems Manager, allowing dynamic management of the CloudWatch agent configuration.

8.1 Attaching `AmazonSSMManagedInstanceCore` Policy

1. **Navigate to IAM Console:**
   - Go to Services ¿ **IAM**.
2. **Select the Role:**
   - Click on **Roles** and select `cloudmonitorrole2024`.
3. **Attach Policy:**
   - Click **Add permissions** ¿ **Attach policies**.
   - Search for `AmazonSSMManagedInstanceCore`.
   - Select the policy and click **Attach policies**.

9 Step 7: Log Monitoring Setup

Setting up log monitoring ensures that logs from various AWS resources are correctly streamed to their respective CloudWatch log groups.

9.1 Configuring Log Streaming

1. **Edit `config.json`:**
   - Ensure that the log file paths and log group names are correctly specified.
2. **Start the CloudWatch Agent:**
   Initiate the CloudWatch agent with the specified configuration.
3. **Verify Agent Status:**
   Confirm that the CloudWatch agent is running as expected.

9.2 Setting Log Retention

4. **In CloudWatch Console:**
   - Navigate to **Logs** ¿ **Log groups**.
   - Select `monitorloggroupec22024`.
   - Click **Actions** ¿ **Edit retention**.
   - Set retention to **14 days**.
   - Click **Save**.

10 Step 8: CloudWatch Agent Logs and Data Transmission

Ensuring that the CloudWatch agent is functioning correctly involves verifying its logs and confirming data transmission to CloudWatch.

10.1 Verifying Agent Status

1. **Check Agent Status:**

   Confirm that the agent is running.

10.2 Confirming Data Transmission

2. **View Agent Logs:**

   - Look for messages indicating successful data transmission.

3. **Check CloudWatch Console:**

   - Navigate to CloudWatch ¿ **Logs** ¿ **Log groups**.
   - Select `monitorloggroupec22024` and verify that log streams are populated.

Figure 5: Figure 8: CloudWatch Agent Logs

11 Conclusion

By meticulously following the steps outlined in this manual, you've successfully designed and implemented a comprehensive cloud security monitoring tool using AWS CloudWatch Logs and the CloudWatch Console. This setup provides real-time visibility into your AWS resources, enabling proactive security management and ensuring compliance with organizational and regulatory standards. Regularly review and update your configurations to adapt to evolving security requirements and to leverage new features offered by AWS CloudWatch.