National College of Ireland

Project Submission Sheet

Student Name: Rithesh Clinton Sequeira

Student ID: 23339021

Programme: MSCCLOUD **Year:** 2025

Module: Research Project

Supervisor: Luis Bernardo Pulido Gaytan

Submission Due Date: Aug 11 2025

Project Title: Zero Trust Architecture

Word Count: 775 **Page Count** 3

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 references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: Rithesh Clinton Sequeira

Date: 07/08/2025

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**
5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

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

AI Acknowledgement Supplement

1 [Insert Module Name]

2 [Insert Title of your assignment]

Your Name/Student Number	Course	Date

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

3 AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool

4 Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

[Insert Tool Name]	
[Insert Description of use]	
[Insert Sample prompt]	[Insert Sample response]

5 Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

6 Additional Evidence:

[Place evidence here]

7 Additional Evidence:

[Place evidence here]

Configuration Manual

Rithesh Clinton Sequeira
Student ID: 23339021

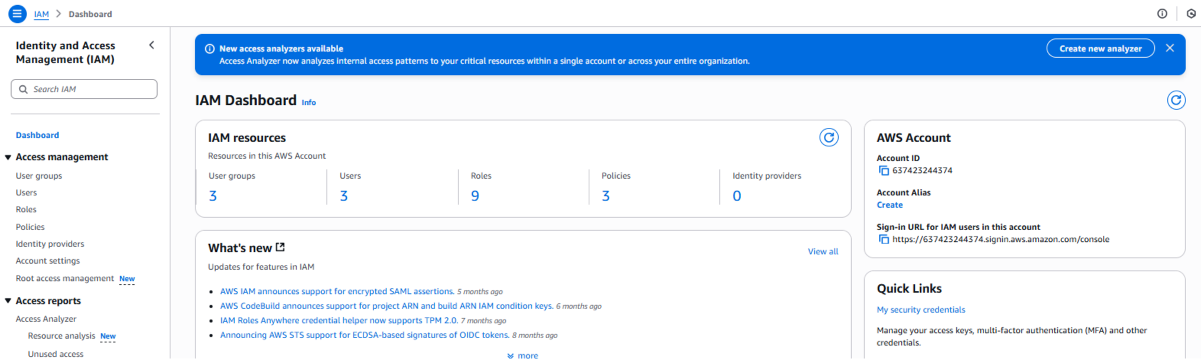
8 Project Environment Setup

The implementation of the Zero Trust Architecture (ZTA) began with setting up a secure and auditable cloud environment within Amazon Web Services (AWS). An AWS root account was created solely for initial setup, with its access restricted thereafter to comply with best practices. Dedicated IAM users were configured using the principle of least privilege, assigning only the minimum permissions required for specific roles (e.g., Admin, Developer, Analyst). Multi-factor authentication (MFA) was enforced on all users.

The project utilized core AWS services including IAM (for identity and access management), CloudTrail (for auditing API activity), CloudWatch (for monitoring and alerting), EC2 (for hosting test workloads), and S3 (for storage of logs and configuration artifacts). The environment was provisioned in the eu-west-1 (Ireland) region to maintain consistency and reduce latency.

Initial account-level security hardening was performed, including disabling root access to the AWS Management Console and implementing explicit deny policies for sensitive operations like unrestricted S3 bucket access and privilege escalation. All configuration changes were logged centrally via CloudTrail and streamed to CloudWatch for real-time visibility.

Development and automation were facilitated using the AWS Console, AWS CLI, and Visual Studio Code. Scripts for automating account setup and policy enforcement were maintained in GitHub. While Terraform was considered, the implementation relied on native tooling for greater transparency during demonstration and testing.



New access analyzers available
Access Analyzer now analyzes internal access patterns to your critical resources within a single account or across your entire organization.

IAM Dashboard

IAM resources
Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
3	3	9	3	0

What's new
Updates for features in IAM

- AWS IAM announces support for encrypted SAML assertions. 5 months ago
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 6 months ago
- IAM Roles Anywhere credential helper now supports TPM 2.0. 7 months ago
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. 8 months ago

AWS Account
Account ID
637423244374
Account Alias
Create
Sign-in URL for IAM users in this account
https://637423244374.signin.aws.amazon.com/console

Quick Links
My security credentials
Manage your access keys, multi-factor authentication (MFA) and other credentials.

Figure 1: IAM Dashboard

9 ZTA Implementation Details

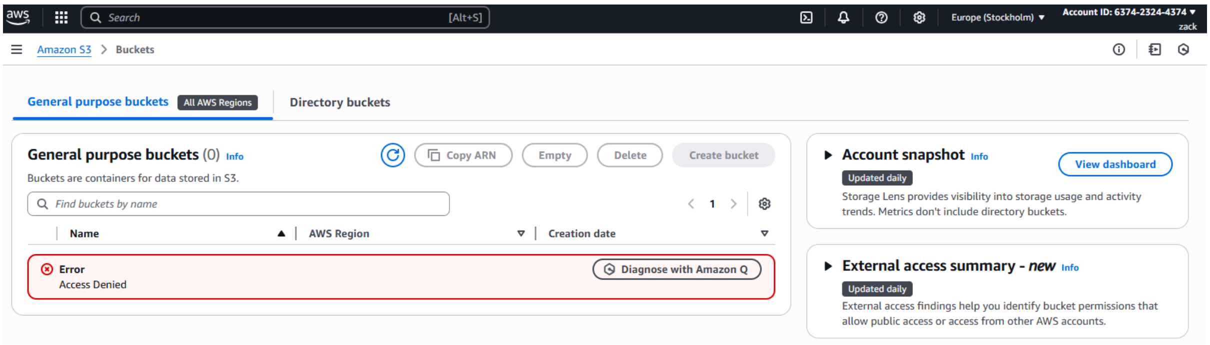
The implementation of the Zero Trust Architecture (ZTA) framework in the AWS environment was achieved by a series of layered access control, logging writers, and active monitoring alerts.

First, IAM policies (JSON code attached) were designed to introduce rigid separation of roles. Rather than allowed by a wide-ranging administration, roles were provided to the users depending on their area of operation (e.g., ZT-Admin, ZT-Audit, ZT-DevOps). Both policies had been using the identity-based access control (IBAC) to make sure that users have only the access to conduct the specified actions and to limited areas of AWS resources. Access abuse was reduced via adoption of DenyAllExceptListedActions strategy in sensitive position.

One of the main parts of ZTA is transparency and auditability. All the regions of AWS cloud trail were enabled and all the API requests whether made through the console, SDK or CLI were logged and archived as secure logs to the S3 bucket. This made it traceable such as in privilege modifications and failed logins.

AWS CloudWatch alarms were set to increase the level of threat detection in real time. An example is that the RootLoginAttempts measure was tracked and a notification created in effect when root logins were detected which contravenes the ZTA principles (Alarm configuration code attached). Events were defined with such boundaries as multiple failed-login attempts, abrupt changes of IAM roles, the deactivation of MFA.

A mock attacker simulation in order to validate monitoring was made: incorrect successful-login caused by a wrong password was initiated. This corresponded to the appropriate CloudWatch alarm that submitted a notification through SNS, resulting in the fact that monitoring and alert processes were operational.



Buckets are containers for data stored in S3.

Error
Access Denied

Storage Lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets.

External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

10 System Requirements

The successful deployment and testing of the Zero Trust Architecture (ZTA) project required both hardware and software components, as well as access to specific cloud infrastructure services. The requirements were categorized as follows:

10.1 Hardware Requirements

10.1.1 Client Machine:

- Processor: Minimum Intel Core i5 (8th Gen) or AMD Ryzen 5
- RAM: 8 GB minimum (16 GB recommended for performance during testing)

  - Storage: 50 GB free disk space (SSD preferred)
  - Network: Stable internet connection with at least 10 Mbps bandwidth

10.2 Software Requirements

10.2.1 Operating System:

  - Windows 10/11 (64-bit) or macOS 12+/Ubuntu 20.04+

10.2.2 Development and Monitoring Tools:

  - AWS CLI (v2.x)
  - Python 3.8+ (for scripting and automation)
  - Visual Studio Code / PyCharm (IDE)
  - AWS CloudTrail and CloudWatch (preconfigured in AWS console)
  - Postman (for API testing)

10.3 Cloud Infrastructure Requirements

10.3.1 AWS Services Utilized:

  - IAM (Identity and Access Management) for user and policy configuration
  - CloudTrail for logging and audit trails
  - CloudWatch for real-time monitoring and alerts
  - S3 (Simple Storage Service) for secure log storage
  - SNS (Simple Notification Service) for alert notifications
  - EC2 (optional, for testing isolated VM access scenarios)

10.4 Security Requirements

- **Authentication:**
  - Multi-Factor Authentication (MFA) enabled for all AWS accounts
  - Enforced password policy: minimum 12 characters, complexity rules
- **Access Control:**
  - Principle of Least Privilege enforced through custom IAM policies
  - No root access allowed; monitored via alerts

10.5 Additional Requirements

- AWS Free Tier account (or budgeted credits for testing)
- Email or SMS service (linked to SNS) for alarm verification
- Git/GitHub for version control and project tracking