

Zero Trust Architecture In Cloud Environments

MSc Research Project
MSc Cybersecurity

Sivaram pakalapati
Student ID:23231131

School of Computing
National College of Ireland

Supervisor: Liam McCabe

National College of Ireland
MSc Project Submission Sheet
School of Computing

StudentName: Sivaram pakalapati
Student ID: 23231131
Programme: MSc Cybersecurity **Year:** 2024
Module: Practicum Part2
Lecturer: Liam McCabe
Submission Due Date: 12/12/2024
Project Title: Zero Trust Architecture in Cloud environments
Word Count: 959 **Page Count:** 10

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:p.sivaram.....

Date:12/12/2024.....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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

Sivaram pakalapati
Student ID: 23231131

1 Introduction

This document provides a comprehensive guide to the configuration and setup of the AWS environment for the MSc research project titled Zero Trust Architecture in Cloud Environments. The project aims to implement a robust cloud infrastructure based on the Zero Trust security model, ensuring that no entity, whether internal or external, is inherently trusted.

The primary objective of this configuration is to establish a secure, scalable, and resilient environment utilizing key AWS components, including:

- Identity and Access Management (IAM)- To enforce strict user permissions and implement multi-factor authentication (MFA), following the principles of Zero Trust to verify each access attempt.
- Elastic Compute Cloud (EC2)- For scalable compute resources, configured with hardened instances and secure access controls to minimize attack surfaces.
- Virtual Private Cloud (VPC)- To create isolated network segments, enforce traffic inspection, and implement micro-segmentation, a core aspect of Zero Trust Architecture.

The setup prioritizes granular access control, network isolation, and continuous monitoring to align with the Zero Trust framework. This manual serves as a detailed reference for the configuration process, helping maintain a secure environment throughout the project lifecycle and beyond.

2 Tools and Technologies Used

Cloud Platform - Amazon Web Services (AWS)

AWS Services

- *IAM* - Identity and Access Management
- *VPC* - Virtual Private Cloud
- *EC2* - Elastic Compute Cloud
- *CloudTrail* - Monitoring and logging
- *AWS Config* - Resource compliance
- *SSM* - AWS Systems Manager

Operating System - Amazon Linux, Ubuntu

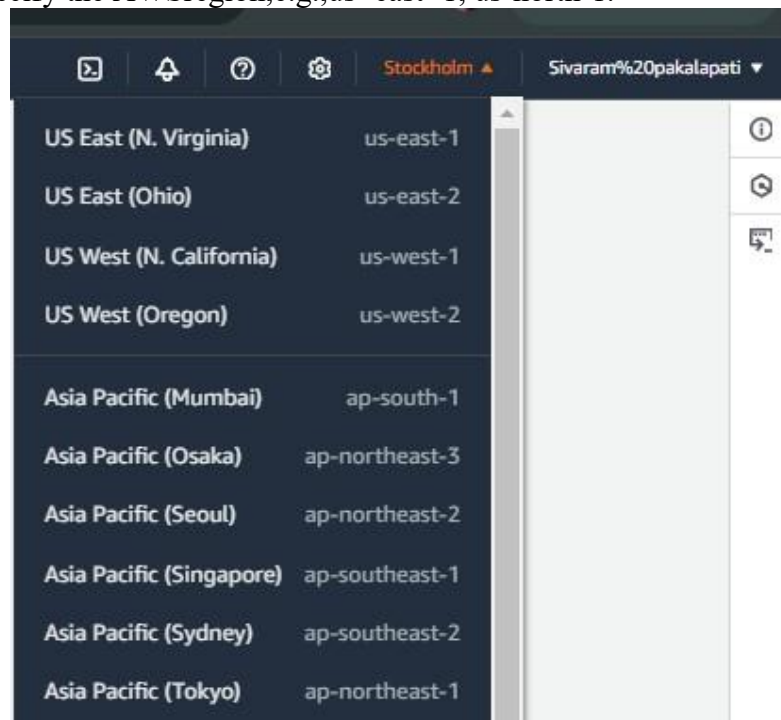
3 Project Environment

The AWS project environment was designed with a focus on security, scalability, and ease of management. The configuration includes:

- **AWS IAM for access control:** Implemented granular permissions to adhere to the principle of least privilege.
- **Amazon EC2 for compute resources:** Instances were selected based on project requirements to optimize performance and cost.
- **VPC for network isolation:** Configured with subnets and routing to enhance security and control traffic flow.

Key elements of the project environment include:

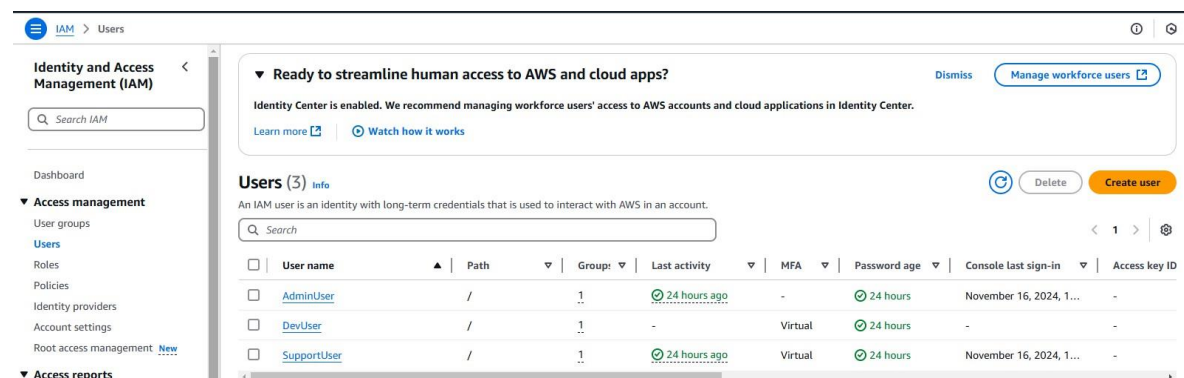
- **Region:** Specify the AWS region, e.g., us-east-1, us-north-1.



4 IAM Configuration

4.1.1 User Groups Setup

Three user groups were created to streamline access control:



1. AdminGroup

- Purpose - Full access for administrative tasks.
- Policies Attached - AdministratorAccess
- MFA Requirement - Enabled for enhanced security.

2. DevGroup

- Purpose - Developer access with limited permissions for EC2 and S3 services.
- Policies Attached - AmazonEC2FullAccess, AmazonS3FullAccess
- MFA Requirement - Enabled (Virtual MFA setup required for users).

3. SupportGroup

- Purpose - Read-only access for monitoring and support personnel.
- Policies Attached - ReadOnlyAccess
- MFA Requirement - Enabled for all users to prevent unauthorized access.

4.1.2 Enable MFA:

- Configure virtual MFA for each user using Google Authenticator or Authy.

The screenshot shows the AWS IAM console interface for setting up a virtual MFA device for the user 'AdminUser'. The breadcrumb navigation is 'IAM > Users > AdminUser > Assign MFA device'. On the left, a progress indicator shows 'Step 1: Select MFA device' and 'Step 2: Set up device' (which is the active step). The main content area is titled 'Set up device' with an 'Info' link. It contains three numbered steps: 1. 'Authenticator app' - A virtual MFA device is an application running on your device that you can configure by scanning a QR code. It instructs to install a compatible application like Google Authenticator, Duo Mobile, or Authy, and provides a link to 'See a list of compatible applications'. 2. A QR code is displayed, with instructions to open the authenticator app, choose 'Show QR code', and scan the code. Alternatively, a secret key can be typed, with a link to 'Show secret key'. 3. 'Type two consecutive MFA codes below'. It prompts to 'Enter a code from your virtual app below' with a text input field labeled 'MFA Code 1'. Below that, it says 'Wait 30 seconds, and enter a second code entry.' with another text input field labeled 'MFA Code 2'.

4.1.3 Assign Roles and Policies:

- AdminUser - Full administrative access (AdministratorAccess policy).
- DevUser - Access to EC2, S3, and Lambda (custom role with least privilege).
- SupportUser - Read-only access for troubleshooting (custom role).

DevUser
Info
Delete

Summary

ARN
arn:aws:iam::180294204053:user/DevUser

Console access
Enabled with MFA

Access key 1
Create access key

Created
November 16, 2024, 15:08 (UTC+03:00)

Last console sign-in
Never

Permissions
Groups (1)
Tags
Security credentials
Last Accessed

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type
All types

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Group DevGroup
<input type="checkbox"/>	AmazonRDSFullAccess	AWS managed	Group DevGroup
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Group DevGroup

5 EC2 Configuration

5.1.1 EC2 Instances

- Instance Type* - t2.micro for development and testing (Free Tier eligible).
- Operating System* - Amazon Ubuntu Instance for its stability and integration with AWS services.
- Key Pair* - Created a key pair named ProjectKeyPair for secure SSH access to instances.

EC2 > Instances > i-0fe460bd5f2d66f8c

Instance summary for i-0fe460bd5f2d66f8c (ubuntu instance)

Updated less than a minute ago

Refresh
Connect
Instance state
Actions

Instance ID i-0fe460bd5f2d66f8c	Public IPv4 address 18.206.179.209 open address	Private IPv4 addresses 172.31.35.245
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-18-206-179-209.compute-1.amazonaws.com open address
Hostname type IP name: ip-172-31-35-245.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-35-245.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 18.206.179.209 [Public IP]	VPC ID vpc-09dd64ad5b104942a	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-02302e44ed4a21254	
IMDSv2 Required	Instance ARN arn:aws:ec2:us-east-1:180294204053:instance/i-0fe460bd5f2d66f8c	

Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags

Running on ssh, you will need to give necessary permissions to the pem file, then contact administrator for add you IP address for access.

```

Select ubuntu@ip-172-31-35-245: ~
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Nov 15 08:56:47 2024 from 18.206.107.29
ubuntu@ip-172-31-35-245:~$
ubuntu@ip-172-31-35-245:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=2.33 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=2.05 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=2.16 ms

^C--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.052/2.180/2.328/0.113 ms
ubuntu@ip-172-31-35-245:~$

```

5.1.2 Security Groups

Security groups were configured as follows:

VPC > Security Groups > sg-078238da174427fd1 - ZTA-SG-eu-north-1c > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

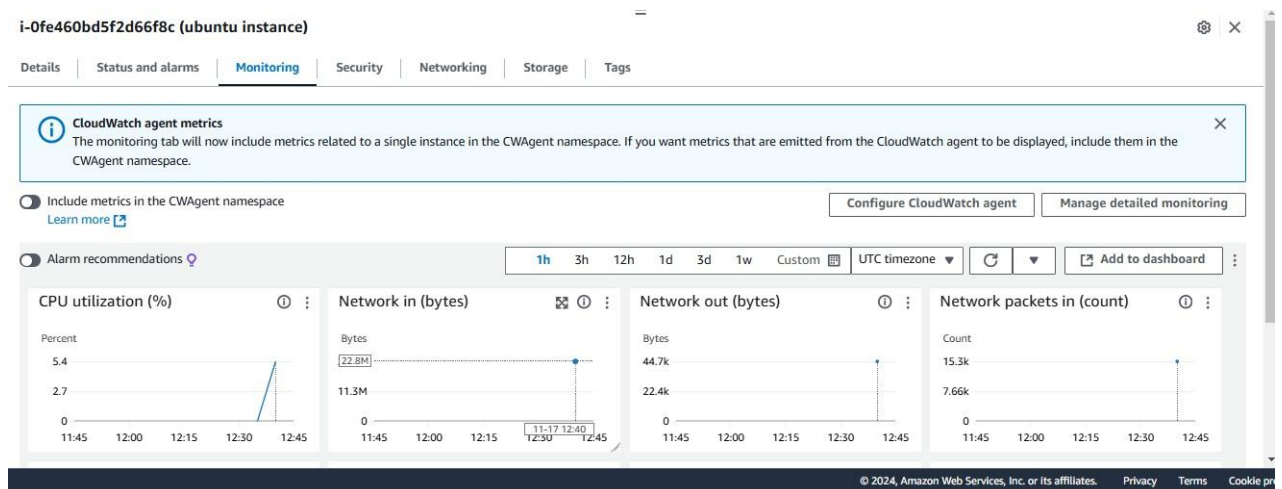
Security group rule ID	Type	Protocol	Port range	Source	Description - optional	
sg-r-0a98fa4e718c562fe	HTTP	TCP	80	My IP		Delete
sg-r-0b8d6d105e1998e3a	HTTPS	TCP	443	My IP	102.219.208.154/32	Delete
sg-r-07cff22f3eb787a0a	SSH	TCP	22	My IP	102.219.208.154/32	Delete
sg-r-0a52c799dfb30e6d4	SSH	TCP	22	Custom	192.168.100.0/24	Delete

[Add rule](#) Cancel Preview changes Save rules

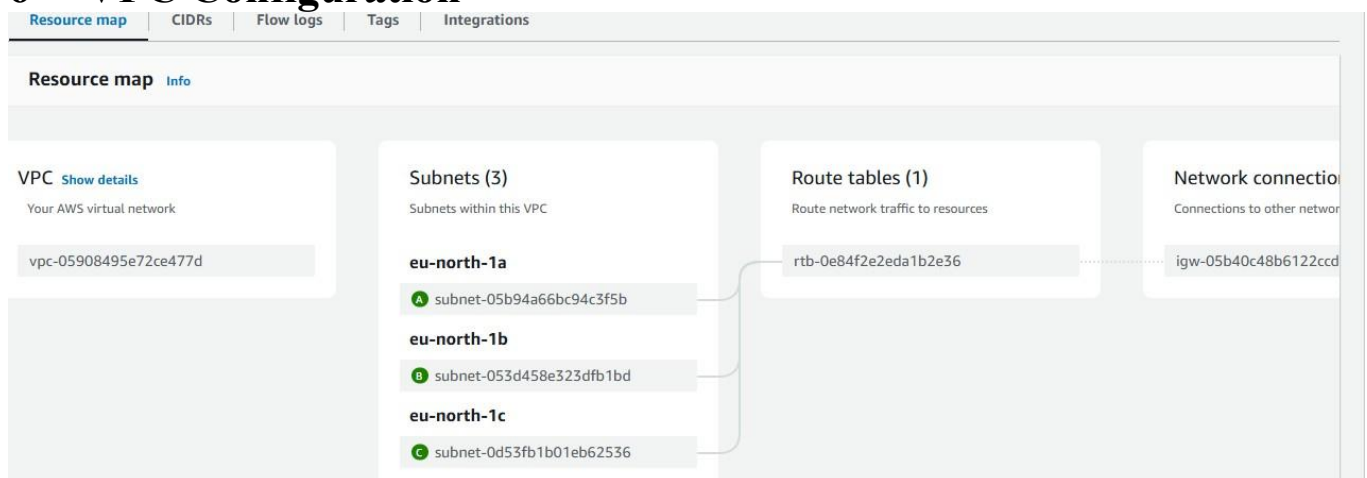
- **AdminSG:**
 - Allows unrestricted inbound traffic on all ports for administrative access (restricted by IP).
 - Outbound traffic is unrestricted for management tasks.
- **WebAppSG:**
 - *Inbound:* HTTP (port 80), HTTPS (port 443) allowed from admin IP.
 - *Outbound:* All traffic allowed.
- **SSH:**
 - *Inbound* - SSH (port 22) traffic allowed only from IP addresses allowed.
 - *Outbound:* All traffic allowed

5.1.3 Instance Monitoring and Logging

- Enabled CloudWatch monitoring for all instances.
- Configured AWS Systems Manager for centralized management and automation.



6 VPC Configuration



6.1.1 VPC and Subnet Design

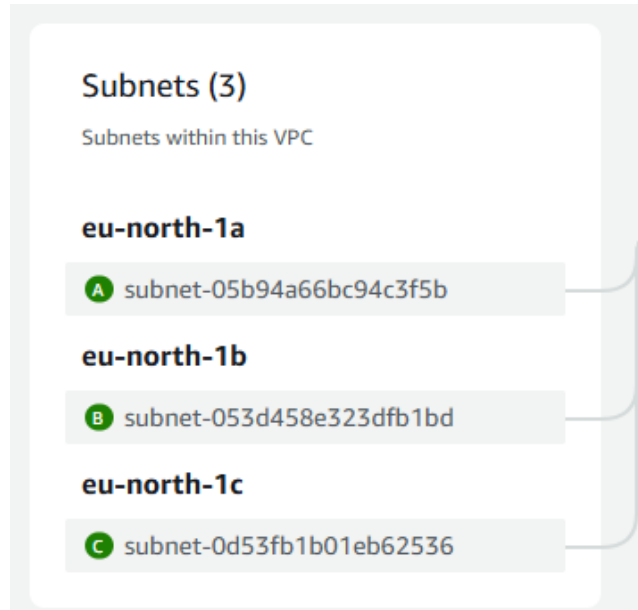
- *VPC Name* - ProjectVPC_north
- *CIDR Block* - 172.31.0.0/16

VPC > Your VPCs > vpc-05908495e72ce477d

vpc-05908495e72ce477d / ProjectVPC_north [Actions](#)

Details	Info
VPC ID vpc-05908495e72ce477d	State ✔ Available
Tenancy Default	DHCP option set dopt-0cb0a8957877ef577
Default VPC Yes	IPv4 CIDR 172.31.0.0/16
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -
	DNS hostnames Enabled
	Main route table rtb-0e84f2e2eda1b2e36
	IPv6 pool -
	Owner ID 180294204053
	DNS resolution Enabled
	Main network ACL acl-0c001169e18a23965
	IPv6 CIDR (Network border group) -

- **Subnets:**



6.1.2 Internet Gateway and NAT Gateway

- An Internet Gateway was attached to enable internet access for resources in the public subnet. A NAT Gateway was created to allow instances in the private subnet to access the internet securely.

VPC > Internet gateways > igw-05b40c48b6122ccd1

igw-05b40c48b6122ccd1 / gateway Actions ▼

Details [Info](#)

Internet gateway ID igw-05b40c48b6122ccd1	State Attached	VPC ID vpc-05908495e72ce477d ProjectVPC north	Owner 180294204053
----------------------------------------------	-------------------	-------------------------------------------------------------------------------------	-----------------------

Tags Manage tags

< 1 > ⚙

Key	Value
Name	gateway

6.1.3 Route Tables

- Configured a main route table for public subnet traffic via the Internet Gateway.
- A separate route table was created for the private subnet to route internet-bound traffic through the NAT Gateway.

VPC > Route tables > rtb-0e84f2e2eda1b2e36

rtb-0e84f2e2eda1b2e36 Actions ▾

Details [Info](#)

Route table ID rtb-0e84f2e2eda1b2e36	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-05908495e72ce477d ProjectVPC_north	Owner ID 180294204053		

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Routes (2) Both ▾ Edit routes

Destination ▾	Target ▾	Status ▾	Propagated ▾
0.0.0.0/0	igw-05b40c48b6122ccd1	Active	No
172.31.0.0/16	local	Active	No