Configuration Manual

MSc Industrial Internship
MSc in Cybersecurity

Ayushi Tripathi
Student ID: x21120935

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Ayushi Tripathi

Student ID: x21120935

Programme: MSc in Cybersecurity **Year:** 2022/23

Module: MSc Industrial Internship

Lecturer: Prof. Vikas Sahni

Submission Due Date: 06/01/2023

Project Title: Provisioning Secure Cloud Environment Using Policy-as-code and Infrastructure-as-code

Word Count: 528 **Page Count:** 12

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: Ayushi Tripathi

Date: 04/01/23

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

Ayushi Tripathi
Student ID: x21120935

1 Introduction

This document gives a summary of the essential requirements for the research endeavour and its suggested replication requirements. The object and the thesis are connected by this manual. The key elements of this thesis, as well as the necessary software and hardware, are all described here using code snippets.

2 Software Requirements

The entire project has been implemented using Visual Studio Code, Terraform CLI and Amazon Web Service CLI and Amazon Web Service Management Console.

- Visual Studio Code version 1.74
- Terraform CLI Version: 1.3.6 (AMD64)
- Amazon Web Service CLI version 2
- Amazon Web Service Management Console

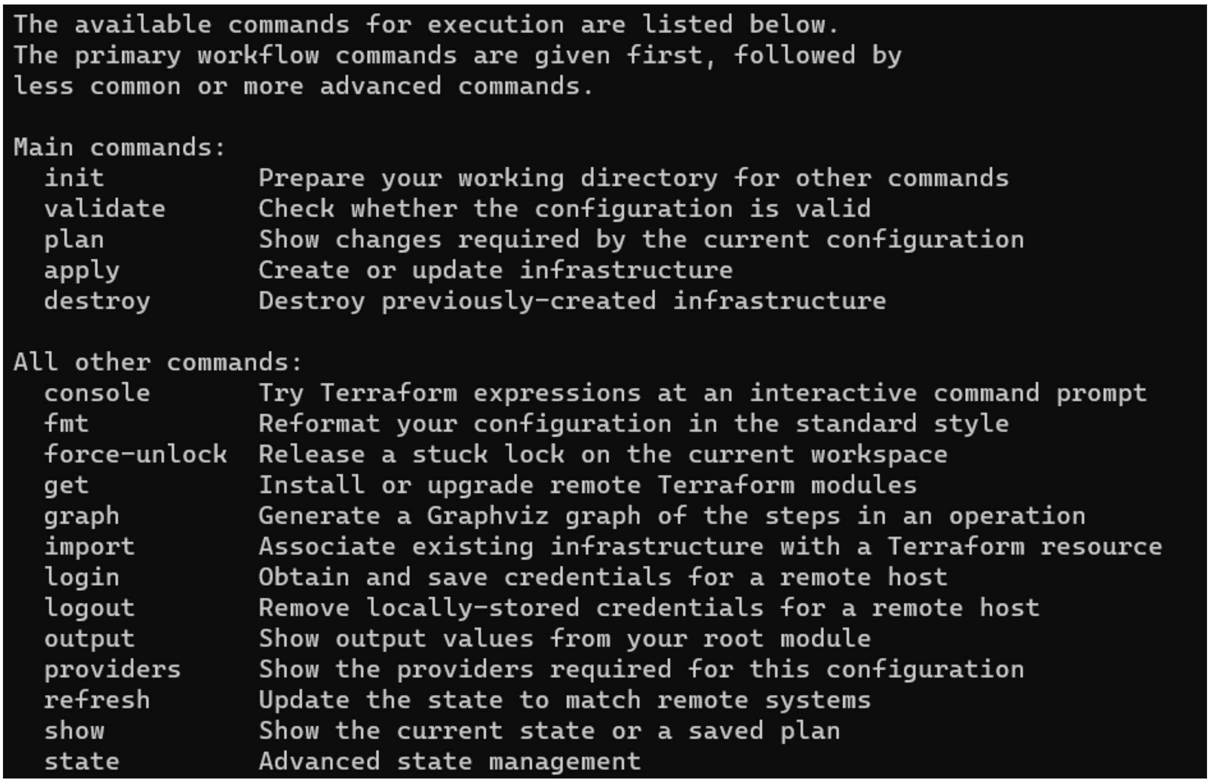
3 System Requirements

- Processor - Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz 1.80 GHz
- Memory - Installed RAM 12.0 GB (11.9 GB usable)
- System Type - Windows 11 64-bit operating system, x64-based processor
- Edition- Windows 11 Home Single Language
- Version - 22H2
- OS build - 22621.963

4 Installation

4.1 Terraform

Install Terraform CLI[1] from the official website depending upon the Operating System. Terraform executable path is extracted and added to ENV variables. The path is permanently added to the $Path variable if the Terraform executable is located in a different location.



```
The available commands for execution are listed below.
The primary workflow commands are given first, followed by
less common or more advanced commands.

Main commands:
  init          Prepare your working directory for other commands
  validate      Check whether the configuration is valid
  plan          Show changes required by the current configuration
  apply         Create or update infrastructure
  destroy       Destroy previously-created infrastructure

All other commands:
  console       Try Terraform expressions at an interactive command prompt
  fmt           Reformat your configuration in the standard style
  force-unlock  Release a stuck lock on the current workspace
  get           Install or upgrade remote Terraform modules
  graph         Generate a Graphviz graph of the steps in an operation
  import        Associate existing infrastructure with a Terraform resource
  login         Obtain and save credentials for a remote host
  logout        Remove locally-stored credentials for a remote host
  output        Show output values from your root module
  providers     Show the providers required for this configuration
  refresh       Update the state to match remote systems
  show          Show the current state or a saved plan
  state         Advanced state management
```

Figure 1 Terraform Installation

4.2 AWS CLI

1. Create an AWS user with administrative access and programmatic access under IAM policy. Keep a record of the access key ID and secret access key.
2. Run aws configure command on local machine and enter the AWS Access Key ID and the AWS Secret Access Key.
3. The aws_secret_access_key and aws_access_key_id will be added to the /$USER HOME/.aws/credentials file using the aws configure CLI command, and they will be used to authenticate the creation of the Terraform infrastructure in AWS (Gnanaguru, 2021).

4.3 Visual Studio Code

1. Install Visual Studio Code[2]

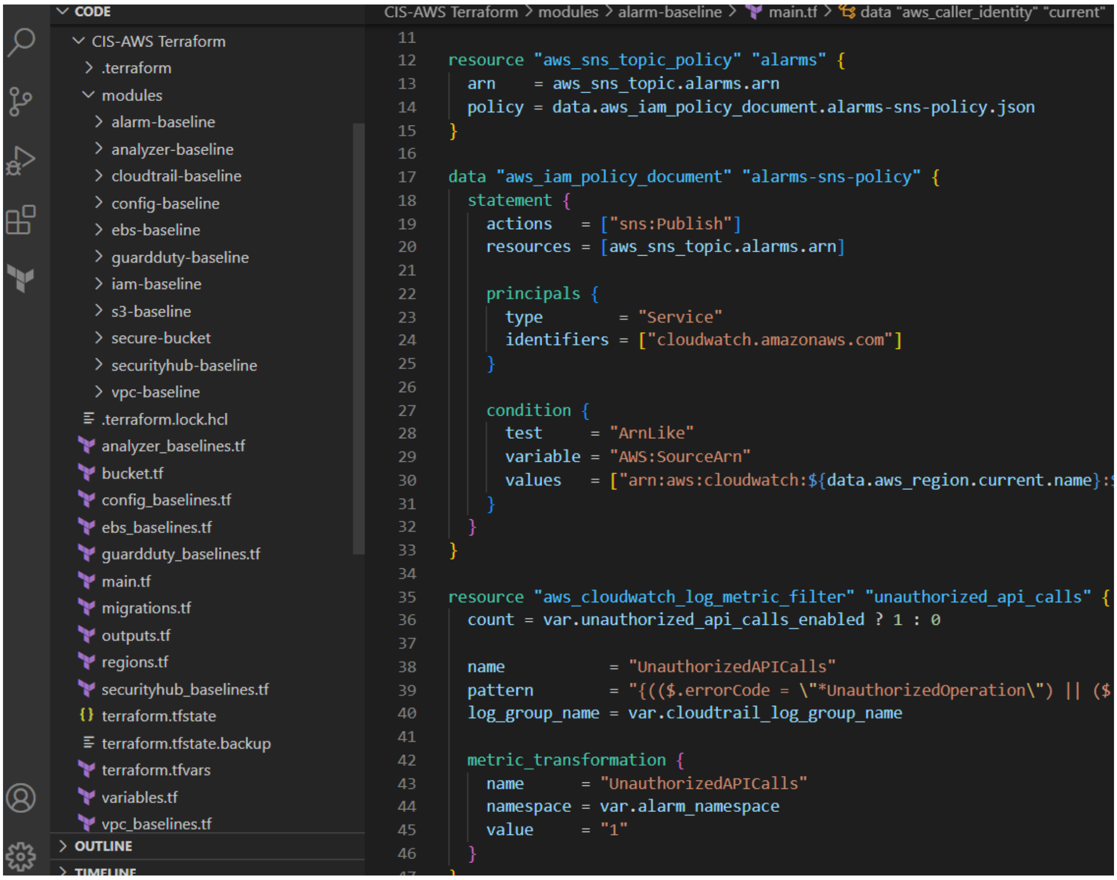
[1] https://developer.hashicorp.com/terraform/downloads

[2] https://code.visualstudio.com/Download

5 Steps to Reproduce

5.1 Policy Compliant AWS Architecture

1. Extract CIS-AWS Terraform folder in appropriate directory in Visual Studio Code.



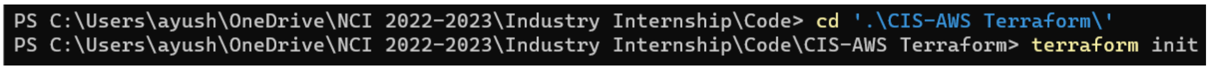
```
resource "aws_sns_topic_policy" "alarms" {
  arn    = aws_sns_topic.alarms.arn
  policy = data.aws_iam_policy_document.alarms-sns-policy.json
}

data "aws_iam_policy_document" "alarms-sns-policy" {
  statement {
    actions   = ["sns:Publish"]
    resources = [aws_sns_topic.alarms.arn]

    principals {
      type        = "Service"
      identifiers = ["cloudwatch.amazonaws.com"]
    }

    condition {
      test     = "ArnLike"
      variable = "AWS:SourceArn"
      values   = ["arn:aws:cloudwatch:${data.aws_region.current.name}:
    }
  }
}

resource "aws_cloudwatch_log_metric_filter" "unauthorized_api_calls" {
  count = var.unauthorized_api_calls_enabled ? 1 : 0

  name           = "UnauthorizedAPICalls"
  pattern        = "{(($.errorCode = \"*UnauthorizedOperation\") || ($
  log_group_name = var.cloudtrail_log_group_name

  metric_transformation {
    name      = "UnauthorizedAPICalls"
    namespace = var.alarm_namespace
    value     = "1"
  }
```

Figure 2 CIS-AWS Terraform

2. Open the command prompt in the directory where the code is located. The main.tf file should be present in the same location.

3. Rum Terraform commands

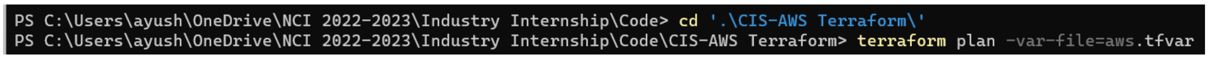
- Terraform init



```
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code> cd '.\CIS-AWS Terraform\'
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code\CIS-AWS Terraform> terraform init
```

Figure 3 Terraform init

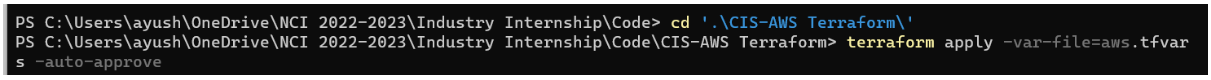
- Terraform plan



```
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code> cd '.\CIS-AWS Terraform\'
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code\CIS-AWS Terraform> terraform plan -var-file=aws.tfvar
```

Figure 4 Terraform plan

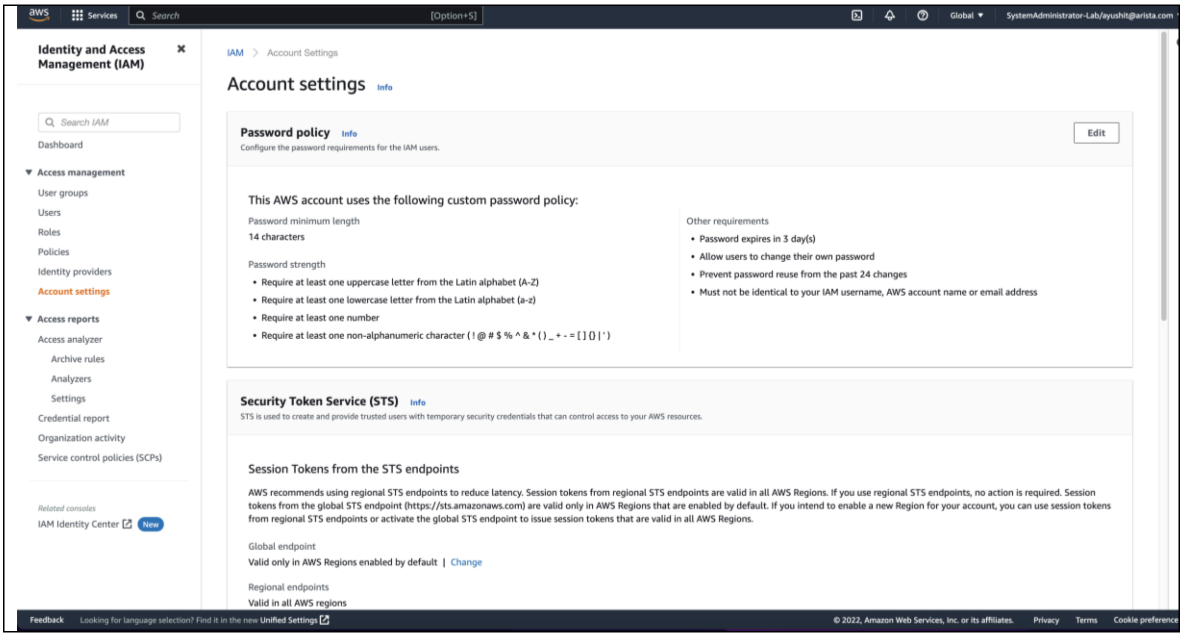
- Terraform apply



```
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code> cd '.\CIS-AWS Terraform\'
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code\CIS-AWS Terraform> terraform apply -var-file=aws.tfvar
s -auto-approve
```

Figure 5 Terraform apply

4. Verify it on AWS Management Console as shown below.



Account settings

Password policy

Configure the password requirements for the IAM users.

This AWS account uses the following custom password policy:

Password minimum length
14 characters

Password strength
- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # $ % ^ & * ( ) _ + - = [ ] { } | ')

Other requirements
- Password expires in 3 day(s)
- Allow users to change their own password
- Prevent password reuse from the past 24 changes
- Must not be identical to your IAM username, AWS account name or email address

Security Token Service (STS)

STS is used to create and provide trusted users with temporary security credentials that can control access to your AWS resources.

Session Tokens from the STS endpoints

AWS recommends using regional STS endpoints to reduce latency. Session tokens from regional STS endpoints are valid in all AWS Regions. If you use regional STS endpoints, no action is required. Session tokens from the global STS endpoint (https://sts.amazonaws.com) are valid only in AWS Regions that are enabled by default. If you intend to enable a new Region for your account, you can use session tokens from regional STS endpoints or activate the global STS endpoint to issue session tokens that are valid in all AWS Regions.

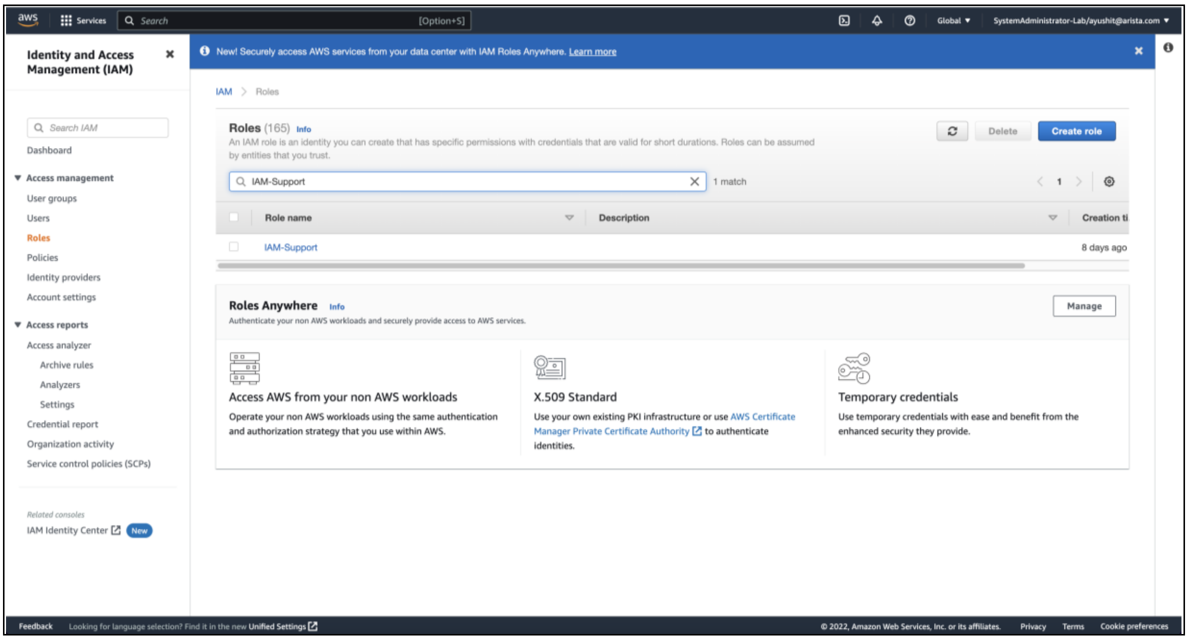
Global endpoint
Valid only in AWS Regions enabled by default | Change

Regional endpoints
Valid in all AWS regions

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

Figure 6 IAM Password Policy



New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

Roles (165)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

IAM-Support | 1 match | 1

☐	Role name	Description	Creation ti
☐	IAM-Support		8 days ago

Roles Anywhere

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

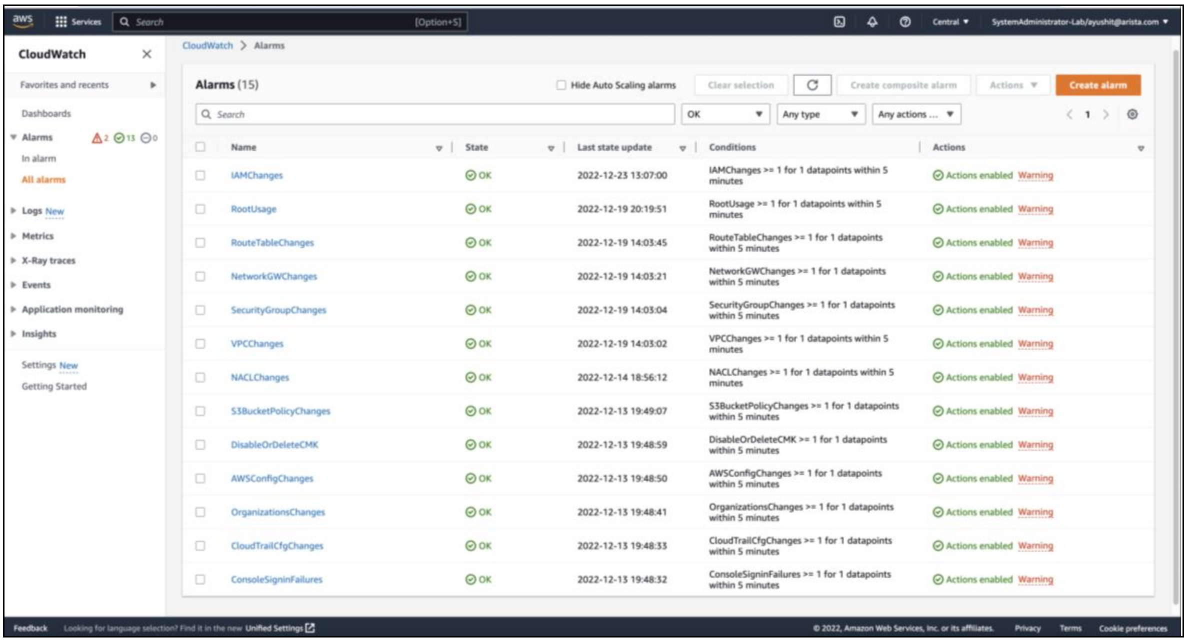
Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

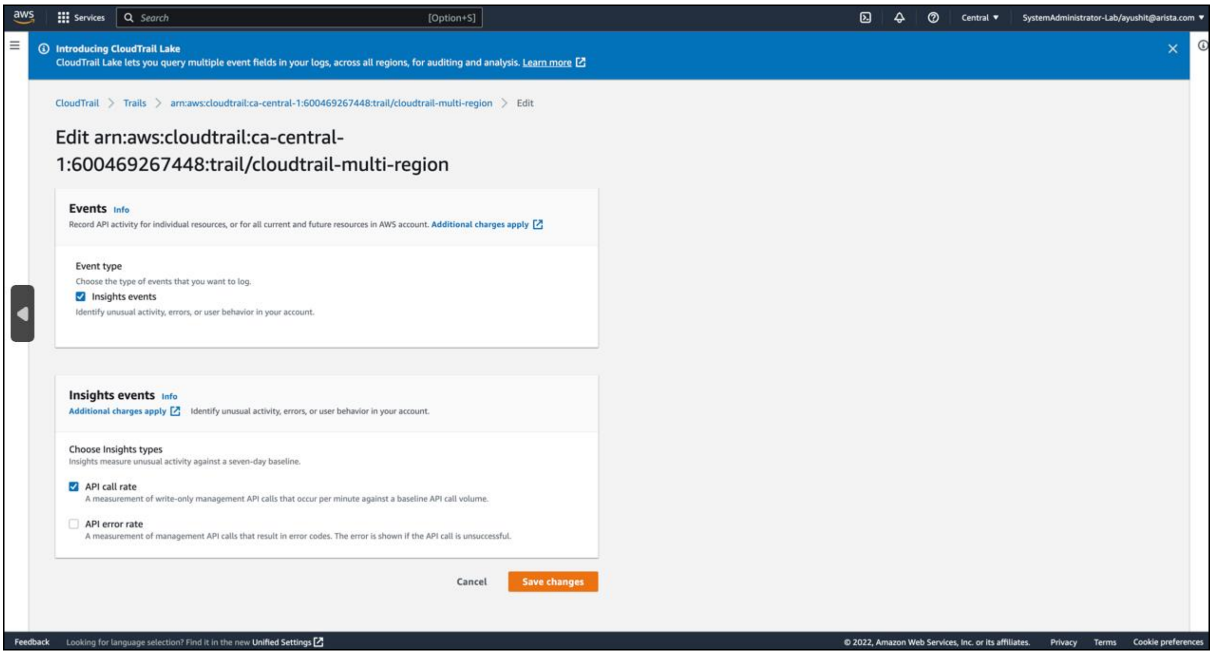
Figure 7 IAM Support role



Alarms (15)

Name	State	Last state update	Conditions	Actions
IAMChanges	OK	2022-12-23 13:07:00	IAMChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
RootUsage	OK	2022-12-19 20:19:51	RootUsage >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
RouteTableChanges	OK	2022-12-19 14:03:45	RouteTableChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
NetworkGWChanges	OK	2022-12-19 14:03:21	NetworkGWChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
SecurityGroupChanges	OK	2022-12-19 14:03:04	SecurityGroupChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
VPCChanges	OK	2022-12-19 14:03:02	VPCChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
NACLChanges	OK	2022-12-14 18:56:12	NACLChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
S3BucketPolicyChanges	OK	2022-12-13 19:49:07	S3BucketPolicyChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
DisableOrDeleteCMK	OK	2022-12-13 19:48:59	DisableOrDeleteCMK >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
AWSConfigChanges	OK	2022-12-13 19:48:50	AWSConfigChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
OrganizationsChanges	OK	2022-12-13 19:48:41	OrganizationsChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
CloudTrailCfgChanges	OK	2022-12-13 19:48:33	CloudTrailCfgChanges >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning
ConsoleSigninFailures	OK	2022-12-13 19:48:32	ConsoleSigninFailures >= 1 for 1 datapoints within 5 minutes	Actions enabled Warning

Figure 8 Alarms



aws
Services
Search
[Option+S]
Central
SystemAdministrator-Lab/ayushit@arista.com
CloudTrail > Trails > arn:aws:cloudtrail:ca-central-1:600469267448:trail/cloudtrail-multi-region > Edit
Info
Additional charges apply
Info
Cancel
Save changes
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Introducing CloudTrail Lake
CloudTrail Lake lets you query multiple event fields in your logs, across all regions, for auditing and analysis. Learn more

Edit arn:aws:cloudtrail:ca-central-1:600469267448:trail/cloudtrail-multi-region

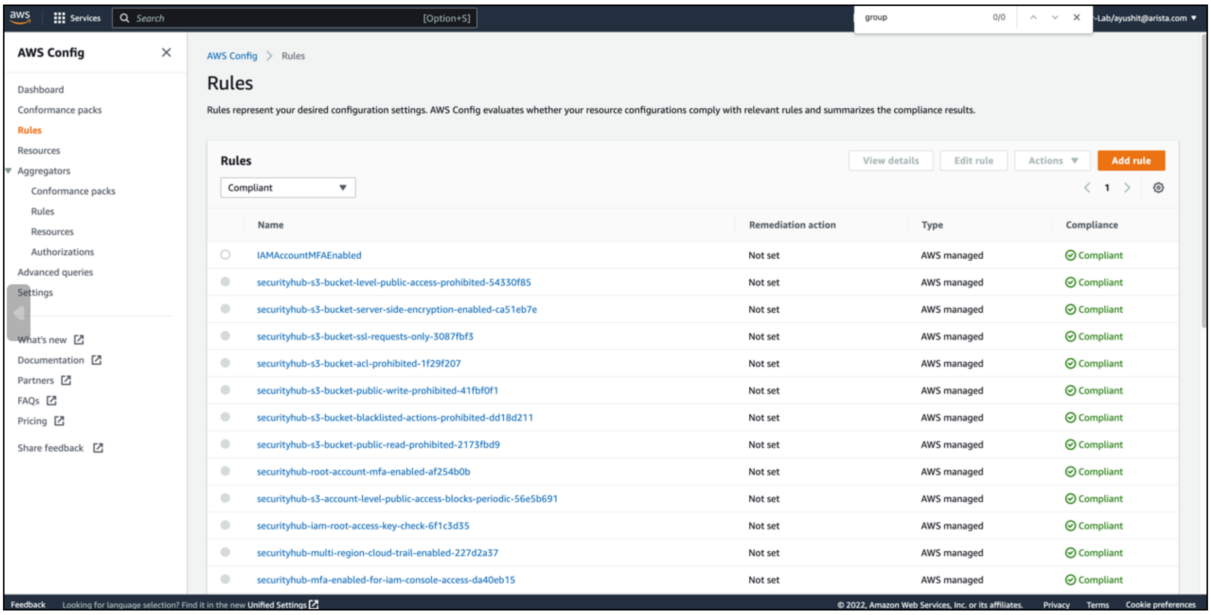
Events
Record API activity for individual resources, or for all current and future resources in AWS account. Additional charges apply

Event type
Choose the type of events that you want to log.
☑ Insights events
Identify unusual activity, errors, or user behavior in your account.

Insights events
Additional charges apply Identify unusual activity, errors, or user behavior in your account.

Choose Insights types
Insights measure unusual activity against a seven-day baseline.
☑ API call rate
A measurement of write-only management API calls that occur per minute against a baseline API call volume.
□ API error rate
A measurement of management API calls that result in error codes. The error is shown if the API call is unsuccessful.

Figure 9 Cloud Trail Event Logging Enabled by Default



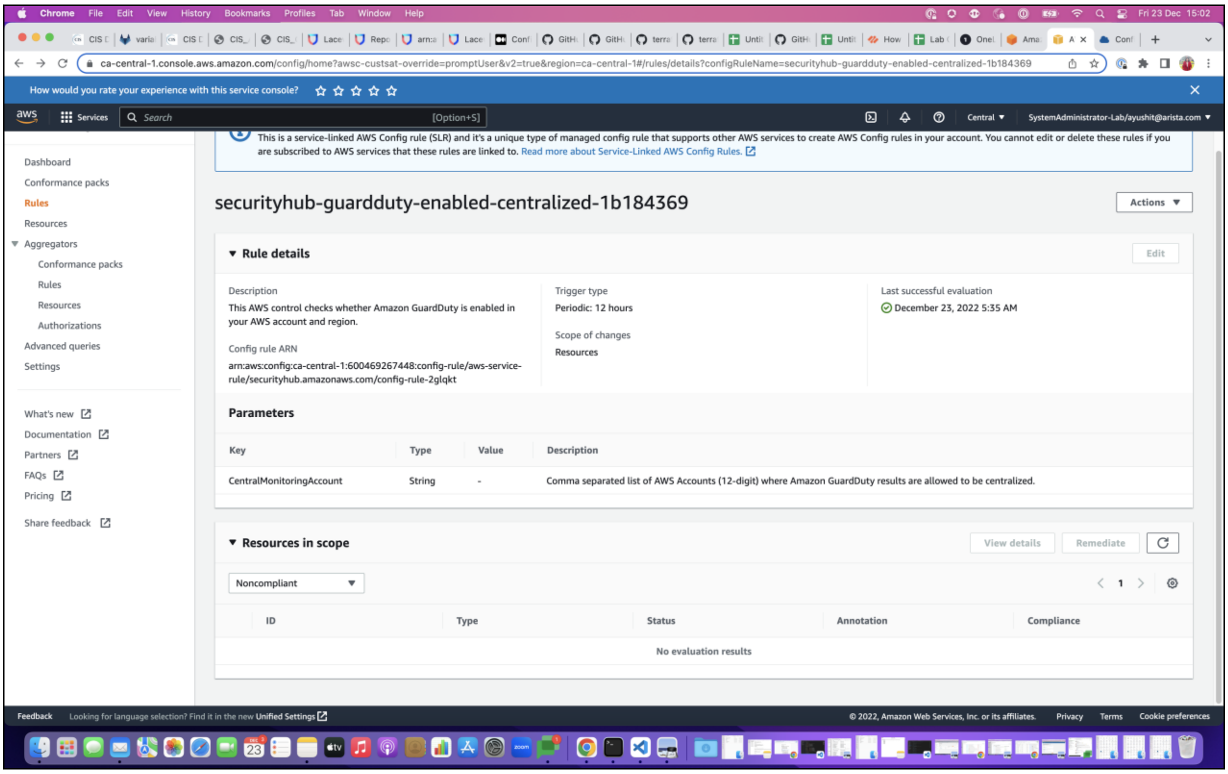
Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

Name	Remediation action	Type	Compliance
IAMAccountMFAEnabled	Not set	AWS managed	Compliant
securityhub-s3-bucket-level-public-access-prohibited-54330f85	Not set	AWS managed	Compliant
securityhub-s3-bucket-server-side-encryption-enabled-ca51eb7e	Not set	AWS managed	Compliant
securityhub-s3-bucket-ssl-requests-only-3087fbf3	Not set	AWS managed	Compliant
securityhub-s3-bucket-acl-prohibited-1f29f207	Not set	AWS managed	Compliant
securityhub-s3-bucket-public-write-prohibited-41fbf0f1	Not set	AWS managed	Compliant
securityhub-s3-bucket-blacklisted-actions-prohibited-dd18d211	Not set	AWS managed	Compliant
securityhub-s3-bucket-public-read-prohibited-2173fbd9	Not set	AWS managed	Compliant
securityhub-root-account-mfa-enabled-af254b0b	Not set	AWS managed	Compliant
securityhub-s3-account-level-public-access-blocks-periodic-56e5b691	Not set	AWS managed	Compliant
securityhub-iam-root-access-key-check-6f1c3d35	Not set	AWS managed	Compliant
securityhub-multi-region-cloud-trail-enabled-227d2a37	Not set	AWS managed	Compliant
securityhub-mfa-enabled-for-iam-console-access-da40eb15	Not set	AWS managed	Compliant

Figure 10 AWS Config Rules



ca-central-1.console.aws.amazon.com/config/home?awsc-custsat-override=promptUser&v2=true&region=ca-central-1#/rules/details?configRuleName=securityhub-guardduty-enabled-centralized-1b184369

This is a service-linked AWS Config rule (SLR) and it's a unique type of managed config rule that supports other AWS services to create AWS Config rules in your account. You cannot edit or delete these rules if you are subscribed to AWS services that these rules are linked to. Read more about Service-Linked AWS Config Rules.

securityhub-guardduty-enabled-centralized-1b184369

Rule details

Description
This AWS control checks whether Amazon GuardDuty is enabled in your AWS account and region.

Config rule ARN
arn:aws:config:ca-central-1:600469267448:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-2glqkt

Trigger type
Periodic: 12 hours

Scope of changes
Resources

Last successful evaluation
December 23, 2022 5:35 AM

Parameters

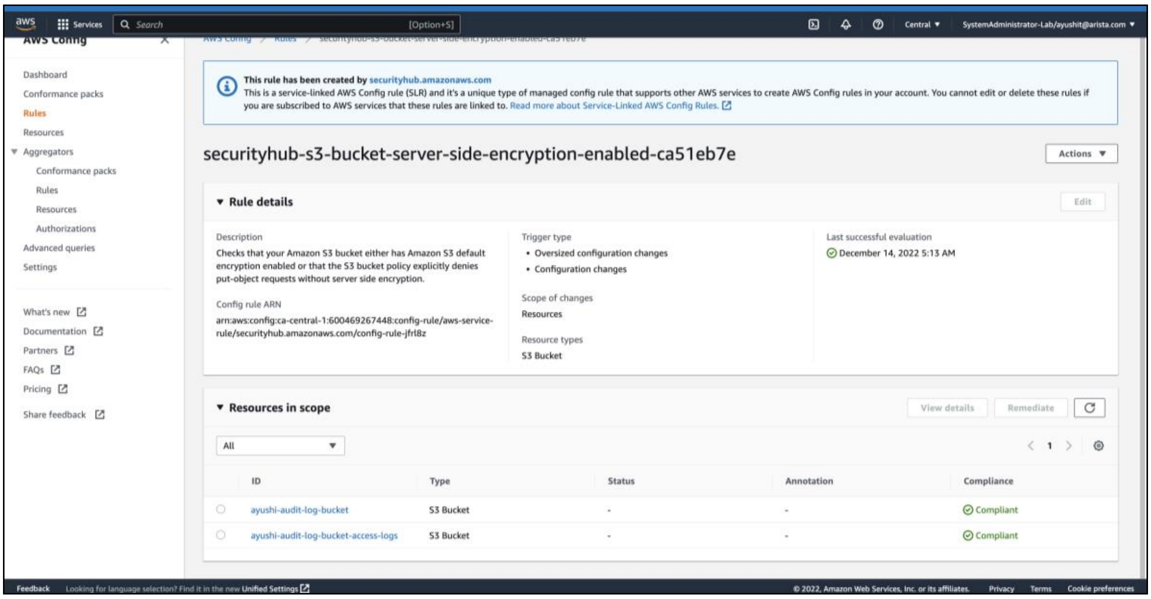
Key	Type	Value	Description
CentralMonitoringAccount	String	-	Comma separated list of AWS Accounts (12-digit) where Amazon GuardDuty results are allowed to be centralized.

Resources in scope

ID	Type	Status	Annotation	Compliance

No evaluation results

Figure 11 Guard Duty Enabled



This rule has been created by securityhub.amazonaws.com
This is a service-linked AWS Config rule (SLR) and it's a unique type of managed config rule that supports other AWS services to create AWS Config rules in your account. You cannot edit or delete these rules if you are subscribed to AWS services that these rules are linked to. Read more about Service-Linked AWS Config Rules.

securityhub-s3-bucket-server-side-encryption-enabled-ca51eb7e

▼ **Rule details**

Description
Checks that your Amazon S3 bucket either has Amazon S3 default encryption enabled or that the S3 bucket policy explicitly denies put-object requests without server side encryption.

Config rule ARN
arn:aws:config:ca-central-1:600469267448:config-rule/aws-service-rule/securityhub.amazonaws.com/config-rule-jfrl8z

Trigger type
- Oversized configuration changes
- Configuration changes

Scope of changes
Resources

Resource types
S3 Bucket

Last successful evaluation
✓ December 14, 2022 5:13 AM

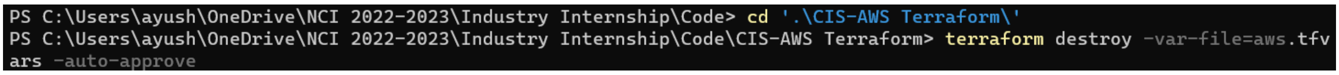
▼ **Resources in scope**

	ID	Type	Status	Annotation	Compliance
○	ayushi-audit-log-bucket	S3 Bucket	-	-	✓ Compliant
○	ayushi-audit-log-bucket-access-logs	S3 Bucket	-	-	✓ Compliant

Figure 12 Server-Side Encryption Enabled for S3 Bucket

- Similarly, all other features can be verified on the AWS Management Console.

- Terraform Destroy to destroy all the resources after scanning from Lacework.

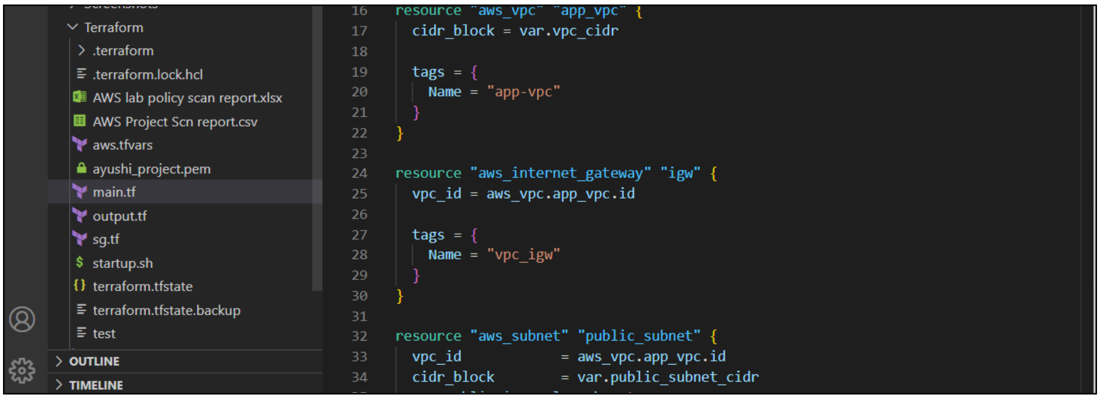


```
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code> cd '.\CIS-AWS Terraform\'
PS C:\Users\ayush\OneDrive\NCI 2022-2023\Industry Internship\Code\CIS-AWS Terraform> terraform destroy -var-file=aws.tfv
ars -auto-approve
```

Figure 13 Terraform Destroy

5.2 Policy Compliant Apache Webserver

1. Extract Terraform folder in appropriate directory in Visual Studio Code.

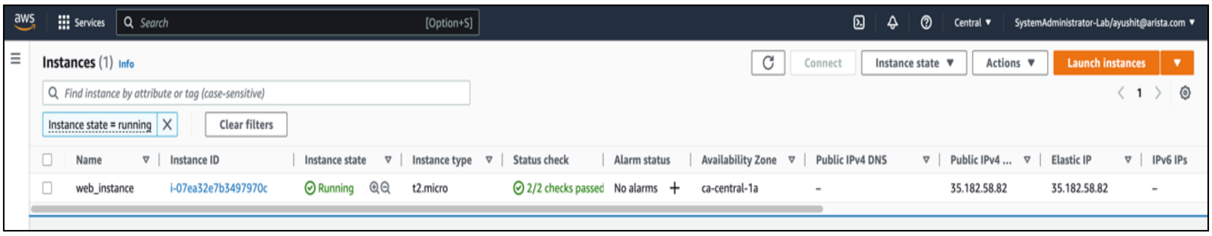


```
resource "aws_vpc" "app_vpc" {
  cidr_block = var.vpc_cidr

  tags = {
    Name = "app-vpc"
  }
}

resource "aws_internet_gateway" "igw" {
  vpc_id = aws_vpc.app_vpc.id

  tags = {
    Name = "vpc_igw"
  }
}

resource "aws_subnet" "public_subnet" {
  vpc_id            = aws_vpc.app_vpc.id
  cidr_block        = var.public_subnet_cidr
```

Figure 14 Terraform Folder

2. Run the Terraform init, plan and apply commands as shown previously.

3. Verify the creation of Apache Webserver by enter the IP found on AWS Management Console.

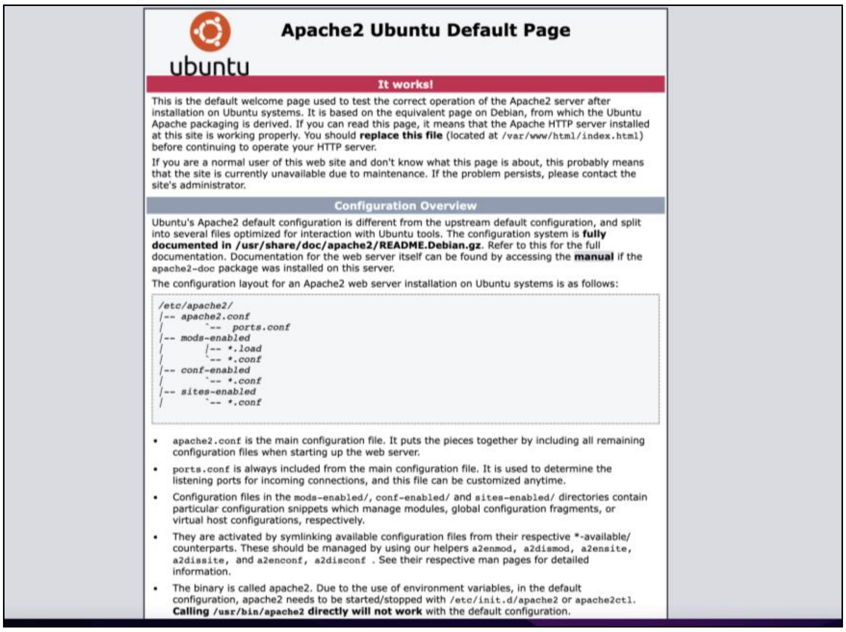


Instances (1)

Instance state = running

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs
□	web_instance	i-07ea32e7b3497970c	Running	t2.micro	2/2 checks passed	No alarms +	ca-central-1a	-	35.182.58.82	35.182.58.82	-

Figure 15 Ec2 Instance Creation



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf` . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Figure 16 Apache Webserver

4. Terraform destroy after scanning from Tenable.io

6 References

Gnanaguru, S. (2021, June 19). Create Apache Web Server in AWS Using Terraform. Retrieved December 30, 2022, from DEV: https://dev.to/chefgs/create-apache-web-server-in-aws-using-terraform-1fpj#install-and-configure-aws-cli

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ayushi Tripathi Student number: x21120935

Company: Arista Networks Month Commencing: October 2022

In the month of October, the following activities were performed

- Finalised the Research Topic.
- Investigated current solutions accessible through research papers.
- Requested for access to various labs and tools.

Employer comments

Grnated access to compute clouds, Terraform and some other compute resources (notably security tools related ones) for the initial exploration phase.

Student Signature: Ayushi Tripathi Date: 15/11/2022

Industry Supervisor Signature: DocuSigned by: Ian O'Brien 05C45D10A947471... Date: 11/17/2022

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ayushi Tripathi Student number: x21120935

Company: Arista Networks Month Commencing: November 2022

In the month of November, the following activities were performed

- Completed lab setup for AWS.
- Learnt about the implementation of Infrastructure-as-a-Code tool (Terraform).
- Learnt about Industry standards and Benchmarks and how can they be implemented as Policy-as-a-code for automation.
- Completed and tested the code on a Cloud Service Provider (AWS).
- Ran a complete policy scan report on the Ec2 instance to identify the missing controls.

Employer comments

Since the intention is to evaluate the overall usefulness of Terraform on the compliance of a multi-cloud setup - this is very much the initial stages. since this work is done, Ayushi has moved on to start with GCP and we will get some compare / contrast with that.

Student Signature: Ayushi Tripathi Date: 01//2022

Industry Supervisor Signature: DocuSigned by: Ian O'Brien 05C45D10A947471... Date: 6-Dec-2022

19. Appendix H – Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: Ayushi Tripathi Student number: x21120935

Company: Arista Networks Month Commencing: December 2022

In the month of December, the following activities were performed

- Completed all activities required for creating AWS infrastructure compliant with CIS Amazon Web Services Foundations v1.4.0 and AWS Foundational Security Best Practices v1.0.0
- Scanned the account using Lacework for security misconfigurations and missing controls
- Completed the recommendations and technical controls which have been implemented for Ubuntu Linux 20.04 LTS in order to get the Apache webserver compliant as per CIS Ubuntu Linux 20.04 LTS Benchmark
- Recorded the demo video

Employer comments

Ayushi was very diligent to the security aspects of this – making sure that all her colleagues understood the implications of what she was doing, and the documentation she needed for the project. We also had a good illustration of the effectiveness of this technique when a user complained about losing access to a resource and then we realized because they were provisioned in the Lab environment that was part of the test. This was a good finding.

Student Signature: Ayushi Tripathi Date: 23rd/12/2022

Industry Supervisor Signature: Ian O'Brien Date: 03rd-Jan-2023