

<b>AWS Environment Limitations.....</b>	<b>2</b>
Observed Limitations.....	2
<b>1. IAM Roles and Policies.....</b>	<b>2</b>
What Was Implemented in Code.....	2
How It Is Supposed to Work:.....	2
Restrictions Encountered:.....	2
<b>2. RDS Database Instance.....</b>	<b>2</b>
What Was Implemented in Code.....	2
How It Is Supposed to Work.....	2
Restriction Encountered.....	3
<b>3. AWS WAF Web ACL.....</b>	<b>3</b>
What Was Implemented in Code:.....	3
How It Is Supposed to Work.....	3
Restriction Encountered.....	3
<b>4. ACM Certificate Import.....</b>	<b>3</b>
What Was Implemented in Code.....	3
How It Is Supposed to Work.....	3
Restriction Encountered.....	3
<b>5. S3 Object Lock and Advanced Security Features.....</b>	<b>3</b>
What Was Implemented in Code.....	3
How It Is Supposed to Work.....	3
Restriction Encountered.....	4
<b>Mitigation and Validation.....</b>	<b>4</b>
<b>Evidences.....</b>	<b>4</b>

## **AWS Environment Limitations**

### **Observed Limitations**

During deployment, several AWS services could not be fully provisioned due to restrictive IAM policies enforced by the AWS Voclabs student environment. The following actions were explicitly denied by the sandbox account:

- IAM role creation (iam:CreateRole)
- IAM user creation (iam:CreateUser)
- RDS database instance creation (rds:CreateDBInstance)
- WAF Web ACL creation (wafv2:CreateWebACL)
- ACM certificate import (acm:ImportCertificate)
- S3 Object Lock configuration (s3:GetBucketObjectLockConfiguration)

### **1. IAM Roles and Policies**

#### **What Was Implemented in Code**

- Trust policy allowing EC2 service to assume the role
- Attachment of AWS managed policies (e.g., CloudWatch logging, SSM access)
- Role designed following the principle of least privilege

#### **How It Is Supposed to Work:**

- Terraform creates the IAM role
- EC2 instances assume the role at runtime
- No long-term credentials are stored on instances
- Access to AWS services is controlled via attached policies

#### **Restrictions Encountered:**

- IAM roles could not be created
- IAM users could not be created
- Terraform failed at the IAM resource stage with 403 AccessDenied errors

### **2. RDS Database Instance**

#### **What Was Implemented in Code**

- An RDS instance in private database subnets
- Storage encryption enabled
- Security group allowing access only from application security group
- No public accessibility

#### **How It Is Supposed to Work**

- RDS instance is created inside private subnets
- Database is unreachable from the internet
- Only application instances can connect via security group rules
- Encryption protects data at rest

## **Restriction Encountered**

The sandbox account denied: *rds:CreateDBInstance*

### **3. AWS WAF Web ACL**

#### **What Was Implemented in Code:**

- A WAFv2 Web ACL
- AWS Managed Rules (Common Rule Set)
- Association with the Application Load Balancer

#### **How It Is Supposed to Work**

- WAF inspects incoming HTTP/HTTPS requests
- Blocks common attacks such as SQL injection and XSS
- Provides CloudWatch metrics for visibility
- Acts as an application-layer perimeter defense

#### **Restriction Encountered**

- WAF resource definition was valid
- Creation failed at apply stage due to permission restrictions

### **4. ACM Certificate Import**

#### **What Was Implemented in Code**

- TLS private key generation
- Self-signed certificate creation
- Import of certificate into AWS Certificate Manager (ACM)

#### **How It Is Supposed to Work**

- Certificate is imported into ACM
- Attached to HTTPS listener on ALB
- Enables encrypted HTTPS traffic

#### **Restriction Encountered**

- HTTPS listener could not be fully configured
- HTTP listener remained active

### **5. S3 Object Lock and Advanced Security Features**

#### **What Was Implemented in Code**

- Query or configure Object Lock settings
- Enable secure storage and logging buckets
- Apply server-side encryption (SSE-S3)

#### **How It Is Supposed to Work**

- Object Lock prevents deletion or tampering of audit logs
- Enhances compliance and forensic integrity
- Encryption ensures data confidentiality

## Restriction Encountered

- The sandbox explicitly denied: `s3:GetBucketObjectLockConfiguration`
- S3 buckets were created successfully
- Server-side encryption (SSE-S3) was enabled and visible in AWS Console

## Mitigation and Validation

Despite these restrictions:

- All blocked resources were correctly defined in Terraform
- Terraform validation succeeded (terraform validate)
- Network infrastructure deployed successfully
- Security groups and routing enforced isolation
- Port scanning verified that:
  - Only intended ports were exposed
  - Databases and private subnets were unreachable externally

## Evidences

```
aws_lb.app_lb: Still creating... [2m30s elapsed]
aws_lb.app_lb: Still creating... [2m40s elapsed]
aws_lb.app_lb: Creation complete after 2m41s [id=arn:aws:elasticloadbalancing:us-east-1:254282169394:loadbalancer/app/app-alb/3febe5502fb2af21]
aws_lb_listener.http: Creating...
aws_lb_listener.http: Creation complete after 0s [id=arn:aws:elasticloadbalancing:us-east-1:254282169394:listener/app/app-alb/3febe5502fb2af21/3c5ce80a0f964a40]

Error: creating IAM Role (ec2-app-role): operation error IAM: CreateRole, https response error StatusCode: 403, RequestID: fdbb8764-e18a-4937-99be-dfd94330f354, api error AccessDenied: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::254282169394:role/ec2-app-role because no identity-based policy allows the iam:CreateRole action

with aws iam role.ec2_role,
on iam.tf line 1, in resource "aws iam_role" "ec2_role":
1: resource "aws iam_role" "ec2_role" {

Error: reading S3 Bucket (security-logs-20260204144234784700000001) object lock configuration: operation error S3: GetObjectLockConfiguration, https response error StatusCode: 403, RequestID: 3ZRGHC54DD06VEANK, HostID: bcf10Tsm26z7f3X50/RRy03X+mhbZn5ngrcPVeIsD3ogstulFqazI8kOsLER+o5JETzvzEFsUuZLmTB935RG8dWREffCcCb3S5, api error AccessDenied: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: s3:GetBucketObjectLockConfiguration on resource: "arn:aws:s3:::security-logs-20260204144234784700000001" with an explicit deny in an identity-based policy

with aws s3 bucket.log_bucket,
on logging.tf line 2, in resource "aws_s3_bucket" "log_bucket":
2: resource "aws_s3_bucket" "log_bucket" {
```

*Figure 1: Terraform execution log showing successful Application Load Balancer (ALB) creation, followed by a permission denial when attempting to create an IAM role (iam:CreateRole). The error indicates that the AWS Academy student account does not allow IAM role creation due to restricted identity-based policies.*

```

Error: creating RDS DB Instance (terraform-20260204144254140200000003): operation error RDS: CreateDBInstance, https response error StatusCode: 403, RequestID: 3fc6bb69-d478-416d-b809-90e60590ad0e, api error AccessDenied: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: rds:CreateDBInstance on resource: arn:aws:rds:us-east-1:254282169394:db:terraform-20260204144254140200000003 because no identity-based policy allows the rds:CreateDBInstance action

with aws_db_instance.default,
on rds.tf line 8, in resource "aws_db_instance" "default":
8: resource "aws_db_instance" "default" {

Error: reading S3 Bucket (student-records-storage-02770b9f) object lock configuration: operation error S3: GetObjectLockConfiguration, https response error StatusCode: 403, RequestID: 3ZRRMQWRACSNKTM8, HostID: FLZIRIak-N9-d29P27gbXV70Qu/adCPyeffsvMYPOSroXGRkvQyVbQlyjbd/6aM1ltakhFvcey7RnuSvRfawQ=, api error AccessDenied: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: s3:GetBucketObjectLockConfiguration on resource: "arn:aws:s3:::student-records-storage-02770b9f" with an explicit deny in an identity-based policy

with aws_s3_bucket.secure_storage,
on s3.tf line 9, in resource "aws_s3_bucket" "secure_storage":
9: resource "aws_s3_bucket" "secure_storage" {

```

*Figure 2: Terraform error output demonstrating access denial for S3 Object Lock configuration (s3:GetBucketObjectLockConfiguration) and Amazon RDS instance creation (rds:CreateDBInstance). These failures are caused by explicit policy restrictions in the AWS Academy student environment, despite the Terraform configuration being syntactically valid.*

```

on s3.tf line 9, in resource "aws_s3_bucket" "secure_storage":
9: resource "aws_s3_bucket" "secure_storage" {

Error: importing ACM Certificate: operation error ACM: ImportCertificate, https response error StatusCode: 400, RequestID: c3fic2fb-accb-484f-be86-ea977087e64b, api error AccessDeniedException: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: acm:ImportCertificate on resource: arn:aws:acm:us-east-1:254282169394:certificate/* because no identity-based policy allows the acm:ImportCertificate action

with aws_acm_certificate.imported_selfsigned,
on tls_acm.tf line 22, in resource "aws_acm_certificate" "imported_selfsigned":
22: resource "aws_acm_certificate" "imported_selfsigned" {

Error: creating WAFv2 WebACL (app-waf): operation error WAFV2: CreateWebACL, https response error StatusCode: 400, RequestID: dc6d4a22-d8ce-4778-8cb6-8a4ba2314c49, api error AccessDeniedException: User: arn:aws:sts::254282169394:assumed-role/voclabs/user4735178-ISSYE_LAILIYAH_BINTI_SOPINGI is not authorized to perform: wafv2:CreateWebACL on resource: arn:aws:wafv2:us-east-1:254282169394:regional/managedruleset/*/* because no identity-based policy allows the wafv2:CreateWebACL action

with aws_wafv2_web_acl.web_acl,
on waf.tf line 1, in resource "aws_wafv2_web_acl" "web_acl":
1: resource "aws_wafv2_web_acl" "web_acl" {

terraform $ Preparing your terminal...

```

*Figure 3: Terraform execution result showing access denial for importing an ACM certificate (acm:ImportCertificate) and creating an AWS WAFv2 Web ACL (wafv2:CreateWebACL). The errors confirm that advanced security services are restricted under the AWS Academy lab account and cannot be provisioned programmatically.*