QATIP Intermediate
AWS Lab 03
Setting Up AWS Secrets Manager and IAM user for Terraform Authentication

Contents

Lab Objectives

This lab presents methods by which multiple developers can authenticate Terraform dynamically without needing to store or share sensitive credentials directly.

Teaching Points

Step 1: Administrator Tasks

- The security team sets up **AWS Secrets Manager** to securely store Terraform authentication credentials.
- An **IAM User** is created with restricted access.

Step 2: Developer Tasks

- Developers retrieve authentication credentials using **AWS Secrets Manager**.
- Developers can **retrieve** credentials but **cannot modify** them.

Before you begin

1. Ensure you have completed Lab0 before attempting this lab.
2. In the IDE terminal pane, enter the following command...

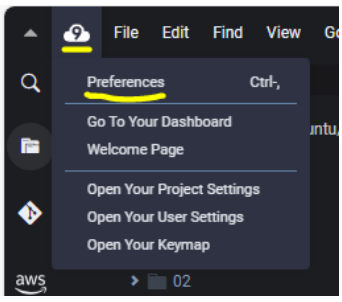
   cd ~/environment/aws-tf-int/labs/03

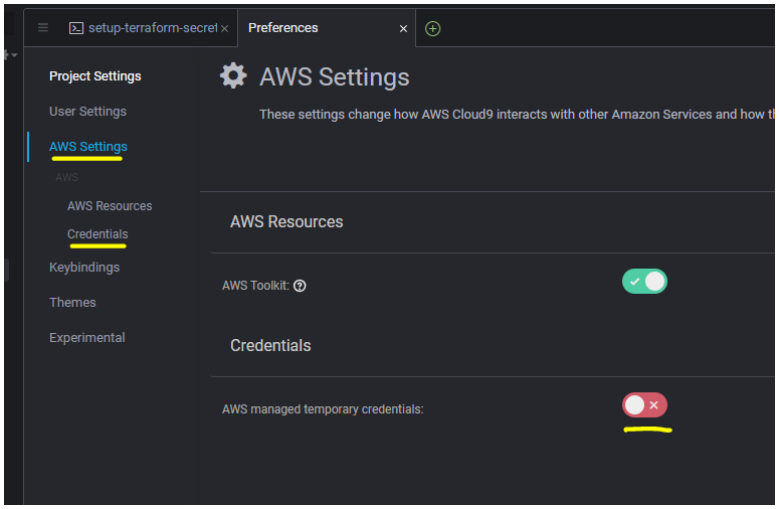
3. This shifts your current working directory to labs/03. Ensure all commands are executed in this directory
4. Close any open files and use the Explorer pane to navigate to and open the labs/03 folder.

Administrators Set Up AWS Secrets Manager and IAM User

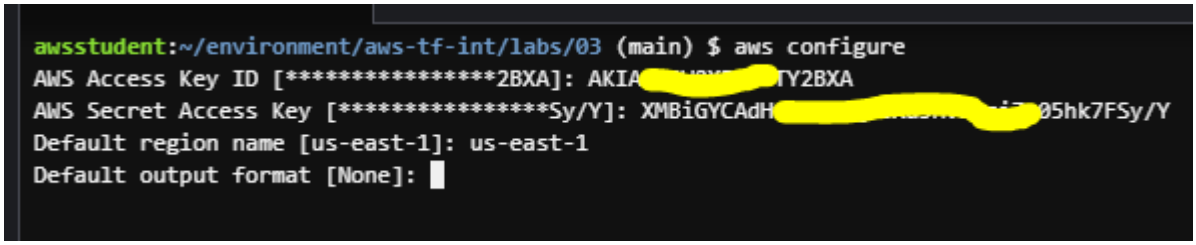
Lab set-up

1. Cloud9 uses temporary credentials by default which do not have sufficient authorization to configure Secrets Manager. Navigate to Preferences, AWS Settings, Credentials and disable temporary credentials...





2. Use "**aws configure**" to supply explicit credentials, providing the Access Key and Secret Access Key generated for your student account, as documented earlier. (Navigate to QA.QWIKLABS if you have not noted these down). Configure us-east-1 as your default region and leave default output format empty....



3. Update the Cloud9 environment to install **jq**, a lightweight command-line tool for parsing, filtering, and transforming JSON data...

   sudo apt-get update && sudo apt-get install -y jq

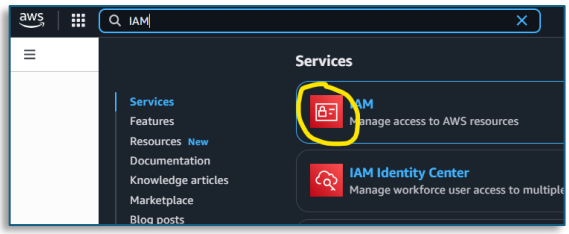
Administration creates an IAM User and Secret

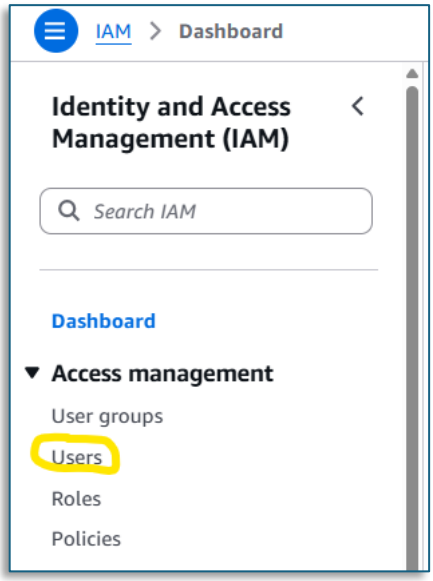
1. Examine the script **setup-terraform-secrets.sh** in **aws-tf-int/labs/03**
2. Ensure lab shell scripts are executable...

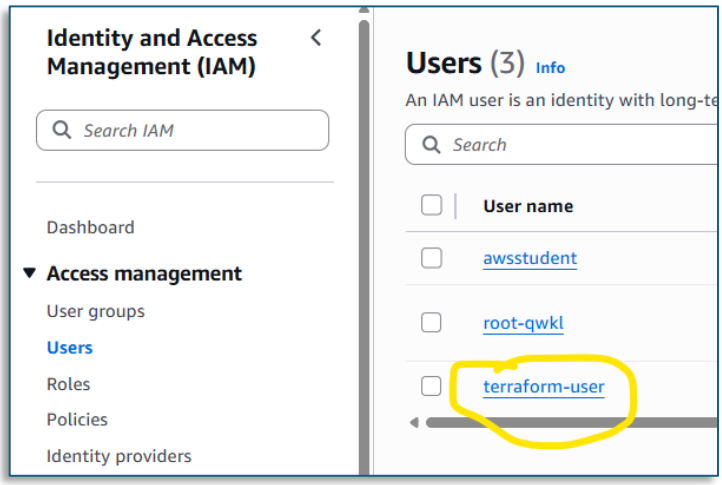
   chmod +x setup-terraform-secrets.sh

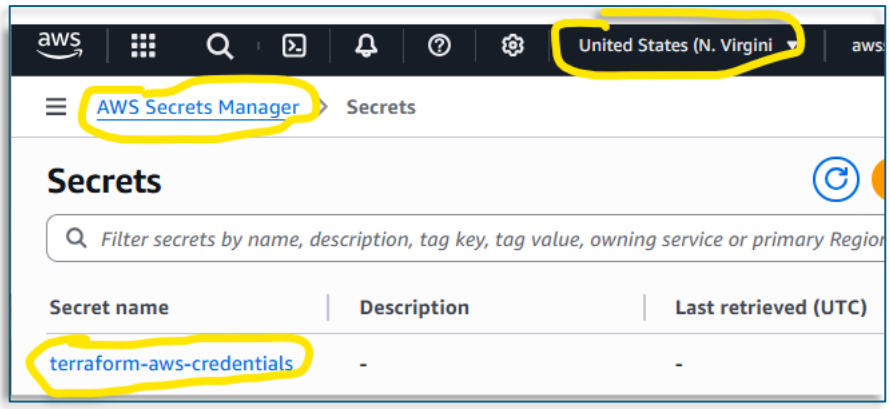
   chmod +x retrieve-aws-credentials.sh

3. Execute the script: **./setup-terraform-secrets.sh**
4. To verify the secret is created you can run **aws secretsmanager get-secret-value --secret-id terraform-aws-credentials**
5. Switch to the Console and ensure the IAM user and secret are created successfully.







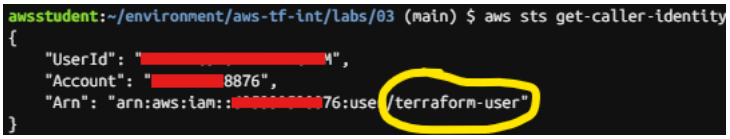


Developers Retrieve IAM Credentials from AWS Secrets Manager

Developers retrieve stored credentials using AWS CLI and export them as environment variables.

Define Parameters and Secure Retrieval Function

1. Examine the script **retrieve-aws-credentials.sh** in **aws-tf-int/labs/03**
2. Execute the script: **./retrieve-aws-credentials.sh**
3. Check stored credentials: **cat aws_credentials.env**
4. Reload credentials in a new session: **source aws_credentials.env**
5. Verify that you are now using the terraform-user credentials by running: **aws sts get-caller-identity**



Verify Authentication & Run Terraform

Developers now use Terraform with the retrieved AWS credentials.

1. Update line 18 of **main.tf** with a unique S3 bucket name of your choice and save the change.
2. Ensure AWS credentials are loaded: **source aws_credentials.env**
3. Initialize Terraform: **terraform init**

4. Test infrastructure deployment: **terraform plan**
5. Deploy the infrastructure: **terraform apply**
6. Verify the AWS resources in the AWS Console.

Using IAM Roles with Terraform

The preceding steps outlined the method of using IAM Users and Secrets Manager. As an alternative, we will now switch to using IAM Roles with temporary credentials, which improves security and aligns with best practices. In production environments, Terraform developers would perform steps in the 'Assuming a role' section below, all other tasks would be performed by cloud administrators. In the lab, you will perform all steps.

Revert to Lab IAM Identity (awsstudent)

1. Before assuming a role, ensure you are no longer using the 'terraform-user' credentials.
2. Run the following in your terminal:

```
unset AWS_ACCESS_KEY_ID
unset AWS_SECRET_ACCESS_KEY
unset AWS_SESSION_TOKEN
```

3. Verify your identity (should return 'awsstudent'):

```
aws sts get-caller-identity
```

Create the Role and Attach Policies

1. Update the provided file **trust-policy.json**, replacing **<AccountID>** with your actual AWS account ID. Save the changes.

2. Create the IAM Role and attach AdministratorAccess (This is very broad access, in production environments the level of access granted to this role would be more limited):

aws iam create-role --role-name TerraformRole --assume-role-policy-document file://trust-policy.json

aws iam attach-role-policy --role-name TerraformRole --policy-arn arn:aws:iam::aws:policy/AdministratorAccess

Assume the Role

As a terraform developer you would authenticate to google cloud with normal credentials, typically with minimal permissions, but including the ability to assume a role. As you action your terraform files, this role is assumed, with sufficient permissions to manage AWS infrastructure as needed.

1. Uncommment all the currently commented-out lines in **main.tf**
2. Update line 13, replacing **<Account_ID>** with you lab account ID
3. Save the changes
4. Re-initialize Terraform: **terraform init -upgrade**
5. Test infrastructure deployment: **terraform plan**
6. Deploy the infrastructure: **terraform apply**
7. Note the output showing the Role being used during command execution...

Lab clean-up

1. Run **terraform destroy** and confirm with **yes**

Congratulations, you have completed this lab