

PROJECT 1

1. Create a eks cluster using terraform and creating vpc , iam roles , worker nodes, logging for eks and giving acces to cloud watch through iam roles for worker nodes.

Creating eks cluster

The screenshot shows a Windows desktop environment with a terminal window open in the foreground. The terminal is running a PowerShell session titled 'powershell'. Inside the terminal, there are several error messages from Terraform, indicating issues with VPC configurations. The file 'main.tf' is currently being edited, showing the AWS provider configuration:

```
provider "aws" {
  region = "us-west-2"
}
```

Below the terminal, the status bar displays the current working directory as 'PS D:\VAMS\terraform eks>'.

main.tf

```

module "vpc" {
  source = "terraform-aws-modules/vpc/aws"
  version = "4.0.0"

  name = "eks-vpc"
  cidr = "10.0.0.0/16"

  azs     = ["us-west-2a", "us-west-2b"]
  private_subnets = ["10.0.1.0/24", "10.0.2.0/24"]
  public_subnets = ["10.0.101.0/24", "10.0.102.0/24"]

  enable_nat_gateway = true

  tags = []
  Terraform = "true"
  Environment = "dev"
}

```

Creating VPC

```

resource "eks_iam" {
  source  = "terraform-aws-modules/eks/aws/modules/iam"
  version = "18.24.2"

  cluster_name = "eks-cluster"
  tags = [
    { Name = "eks-iam" }
  ]
}

```

Creating necessary iam roles

```

resource "aws_launch_configuration" "eks_worker_lc" {
  name          = "eks-worker-lc"
  image_id      = "ami-0a0e8041c159fa8da" # Amazon EKS optimized AMI ID
  instance_type = "t2.medium"

  iam_instance_profile = aws_iam_instance_profile.eks_worker_instance_profile.name

  lifecycle {
    create_before_destroy = true
  }
}

resource "aws_autoscaling_group" "eks_worker_asg" {
  desired_capacity    = 2
  max_size            = 3
  min_size            = 1
  launch_configuration = aws_launch_configuration.eks_worker_lc.id
  vpc_zone_identifier = aws_subnet.eks_subnet[*].id

  tag {
    key        = "Name"
    value      = "eks-worker"
    propagate_at_launch = true
  }
}

with module.vpc.aws_eip.nat[0],
on .terraform\modules\vpc\main.tf line 1030, in resource "aws_eip" "nat":
1030: vpc = true

use domain attribute instead

(and one more similar warning elsewhere)

Apply complete! Resources: 63 added, 0 changed, 0 destroyed.
PS D:\AWS\Terraform\eks> []

```

Creating worker nodes

```

Terraform eks > logging.tf > ...
1 resource "aws_eks_cluster" "example" {
2   name     = "example"
3   role_arn = module.eks_iam.this_eks_cluster_role_arn
4   vpc_config {
5     subnet_ids = module.vpc.private_subnets
6   }
7
8   enabled_cluster_log_types = [
9     "api",
10    "audit",
11    "authenticator",
12    "controllerManager",
13    "scheduler"
14  ]
15
16

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

with module.vpc.aws_eip.nat[0],
on .terraform/modules/vpc/main.tf line 1030, in resource "aws_eip" "nat":
1030: vpc = true

use domain attribute instead

(and one more similar warning elsewhere)

Apply complete! Resources: 63 added, 0 changed, 0 destroyed.
PS D:\AWS\Terraform eks> []

LN 16, Col 1 Spaces: 2 UTF-8 CRLF 637 PM 7/15/2024

Enable eks logging

```

Terraform eks > access.tf > ...
1 resource "aws_iam_role_policy" "worker_nodes_cloudwatch" {
2   role      = module.eks_iam.this_worker_role_name
3
4   policy = jsonencode({
5     "Version" : "2012-10-17",
6     "Statement": [
7       {
8         "Action": [
9           "logs:CreateLogStream",
10          "logs:PutLogEvents"
11        ],
12        "Effect": "Allow",
13        "Resource": "*"
14      }
15    ]
16  })
17
18

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

with module.vpc.aws_eip.nat[0],
on .terraform/modules/vpc/main.tf line 1030, in resource "aws_eip" "nat":
1030: vpc = true

use domain attribute instead

(and one more similar warning elsewhere)

Apply complete! Resources: 63 added, 0 changed, 0 destroyed.
PS D:\AWS\Terraform eks> []

LN 18, Col 1 Spaces: 2 UTF-8 CRLF 637 PM 7/15/2024

Giving access to cloud watch

Clusters | Elastic Kubernetes Service | ChatGPT

us-west-2.console.aws.amazon.com/eks/home?region=us-west-2#clusters

All Bookmarks

Amazon Elastic Kubernetes Service

EKS > Clusters

Clusters (1) info

Cluster name	Status	Kubernetes version	Support period	Provider
my-cluster	Active	1.29 Upgrade now	Standard support until March 23, 2025	EKS

CloudShell Feedback

86°F Mostly cloudy

Eks cluster created

The screenshot shows the AWS EKS Compute tab. On the left sidebar, under 'Clusters', there is a section for 'Amazon EKS Anywhere' and 'Related services' (Amazon ECR, AWS Batch). The main content area displays 'Nodes (1) info' with one node listed: 'ip-10-0-2-53.us-west-2.compute.internal' (t3.medium, example-20240715122745257600000013, Created 5 minutes ago, Status Ready). Below it is a 'Node groups (1) info' table with one entry: 'example-20240715122744243600000011' (Desired size 1, AMI release version 1.29.3-20240703, Launch template example-20240715122744243600000011, Status Active).

Nodes created

The screenshot shows the AWS VPC dashboard. The left sidebar includes sections for 'EC2 Global View', 'Virtual private cloud', 'Your VPCs' (Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, Peering connections), and 'Select a VPC above'. The main content area shows 'Your VPCs (1) info' with one VPC listed: 'eks-vpc' (VPC ID: vpc-0d5db414c65a32c54, State: Available, IPv4 CIDR: 10.0.0.0/16, IPv6 CIDR: -, DHCP options: dopt-0c).

Vpc created

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for 'Identity and Access Management (IAM)', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report), and 'CloudShell Feedback'. The main content area shows 'Permissions policies (1) info' with one policy listed: 'CloudWatchFullAccess' (Type: AWS managed, Attached entities: 1). It also shows a 'Permissions boundary (not set)' and a 'Generate policy based on CloudTrail events' section.

Cloud Watch access

Roles | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#roles

Gmail YouTube Maps

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report

CloudShell Feedback

86°F Mostly cloudy

Roles (16) Info

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.

Search

Role name	Trusted entities	Last activity
AWSserviceRoleForSupport	AWS Service: support (Service-Linked)	2 days ago
AWSserviceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service)	-
dms-vpc-role	AWS Service: dms	25 days ago
ec2-s3-role-access	AWS Service: ec2	25 days ago
EC2CloudWatchRole	AWS Service: ec2	-
example-eks-node-group-2024071512161882110000001	AWS Service: ec2	-
my-cluster-cluster-2024071512161882170000002	AWS Service: eks	-
rds-monitoring-role	AWS Service: monitoring.rds	25 days ago

Roles Anywhere Info

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

Manage

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 6:14 PM 7/15/2024

example-eks-node-group-2024071512161882110000001 ChatGPT

us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#roles/details/example-eks-node-group-2024071512161882110000001)section=permissions

Gmail YouTube Maps

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report

CloudShell Feedback

86°F Mostly cloudy

Permissions

Trust relationships Tags (2) Access Advisor Revoke sessions

Permissions policies (3) Info

You can attach up to 10 managed policies.

Filter by Type

Policy name	Type	Attached entities
AmazonEC2ContainerRegistryReadOnly	AWS managed	1
AmazonEKS_CNI_Policy	AWS managed	1
AmazonEKSWorkerNodePolicy	AWS managed	1

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 6:15 PM 7/15/2024

my-cluster-cluster-2024071512161882170000002 ChatGPT

us-east-1.console.aws.amazon.com/iam/home?region=us-west-2#roles/details/my-cluster-cluster-2024071512161882170000002)section=permissions

Gmail YouTube Maps

aws Services Search [Alt+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report

CloudShell Feedback

86°F Mostly cloudy

You can attach up to 10 managed policies.

Filter by Type

Policy name	Type	Attached entities
AmazonEKSClusterPolicy	AWS managed	1
AmazonEKSVPCResourceController	AWS managed	1
my-cluster-cluster	Customer inline	0
my-cluster-cluster-ClusterEncryption202...	Customer managed	1

▶ Permissions boundary (not set)

▼ Generate policy based on CloudTrail events

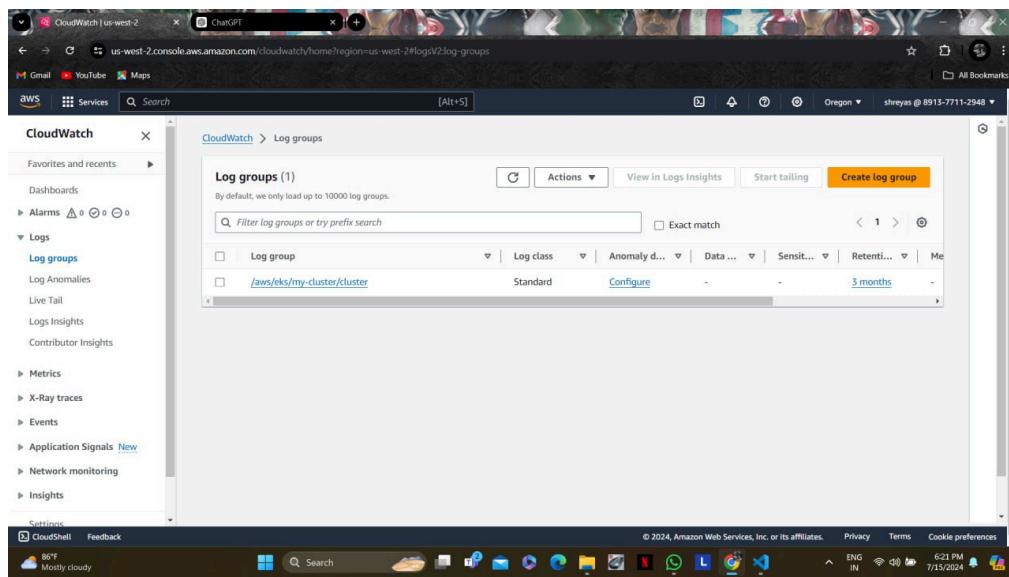
You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

Generate policy

No requests to generate a policy in the past 7 days.

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 6:16 PM 7/15/2024

Necessary iam roles



Eks logs in cloudwatch

2. Enable state locking using terraform through s3 and Dynamodb

```

File Edit Selection View Go Run Terminal Help ⏎ → 🔍 Kubernetes
EXPLORER ... provider.tf terraform.exe main.tf variables.tf terraform.tfvars outputs.tf
KUBERNETES
  terraform
    terraform.aws
      LICENSES.txt
      main.tf
      outputs.tf
      provider.tf
      variables.tf
      terraform.lock.hcl
      terraform.exe
      terraform.tfvars
      variables.tf
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
you run "terraform init" in the future.
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
PS D:\Kubernetes>

```

84°F Partly cloudy

The screenshot shows the Visual Studio Code interface with the "Kubernetes" workspace. The Explorer sidebar shows files like provider.tf, terraform.exe, main.tf, variables.tf, terraform.tfvars, and outputs.tf. The main editor window displays the content of main.tf, which includes a provider block for AWS VPC. The terminal tab shows the output of the "terraform init" command, indicating successful initialization. The status bar at the bottom shows the current weather and date.

main.tf

```

File Edit Selection View Go Run Terminal Help ⏎ → 🔍 Kubernetes
EXPLORER ... provider.tf terraform.exe main.tf variables.tf terraform.tfvars outputs.tf
KUBERNETES
  terraform
    terraform.aws
      LICENSES.txt
      main.tf
      outputs.tf
      provider.tf
      variables.tf
      terraform.lock.hcl
      terraform.exe
      terraform.tfvars
      variables.tf
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
you run "terraform init" in the future.
Terraform has been successfully initialized!
You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.
If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
PS D:\Kubernetes>

```

84°F Partly cloudy

This screenshot is similar to the previous one, showing the Visual Studio Code interface with the "Kubernetes" workspace. The Explorer sidebar shows provider.tf, terraform.exe, main.tf, variables.tf, terraform.tfvars, and outputs.tf. The main editor window displays the content of provider.tf, which includes a required_providers block for AWS and a provider block for AWS with a specific region. The terminal tab shows the output of the "terraform init" command for provider.tf, indicating successful initialization. The status bar at the bottom shows the current weather and date.

provider.tf

```

provider "aws" {
  variable "vpc.cidr" {
    type = string
    default = "10.0.0.0/16"
  }
  variable "vpc.name" {
    type = string
    default = "terraform-demo-vpc"
  }
}

```

variables.tf

variables.tf

```

vpc.cidr = "10.0.0.0/16"
vpc.name = "terraform-demo-vpc"

```

terraform.tfvars

terraform.tfvars

```

output "vpc_id" {
  description = "The ID of the VPC"
  value = aws_vpc.demo_vpc.id
}

```

outputs.tf

outputs.tf

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with options like EC2 Global View, Virtual private cloud, Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, Carrier gateways, DHCP option sets, Elastic IPs, Managed prefix lists, Endpoints, Endpoint services, NAT gateways, and Peering connections. The main area is titled "Your VPCs (1) info" and shows a table with one row:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options
terraform-demo-vpc	vpc-0d0bad8bx6f5e76ab	Available	10.0.0.0/16	-	dopt-0c

Below the table, it says "Select a VPC above". At the bottom of the page, there's a footer with links for CloudShell, Feedback, and various system icons.

Vpc created

The screenshot shows the Amazon S3 Buckets page. On the left, there are tabs for General purpose buckets and Directory buckets. The main area is titled "General purpose buckets (1) info" and shows a table with one row:

Name	AWS Region	IAM Access Analyzer	Creation date
terraform-shreyas-s3-backend-demo-bucket	US West (Oregon) us-west-2	View analyzer for us-west-2	July 16, 2024, 00:00:30 (UTC+05:30)

At the bottom, there's a footer with links for CloudShell, Feedback, and various system icons.

S3 bucket created

The screenshot shows the DynamoDB Tables page. On the left, there's a sidebar with options for Dashboard, Tables, Explore items, PartiQL editor, Backups, Exports to S3, Imports from S3, Integrations, Reserved capacity, and Settings. The main area is titled "Tables (1) info" and shows a table with one row:

Name	Status	Partition key	Sort key	Indexes	Deletion protection	Read capacity mode
terraform-shreyas-s3-backend-demo-table	Active	LockID (\$)	-	0	Off	Provisioned (5)

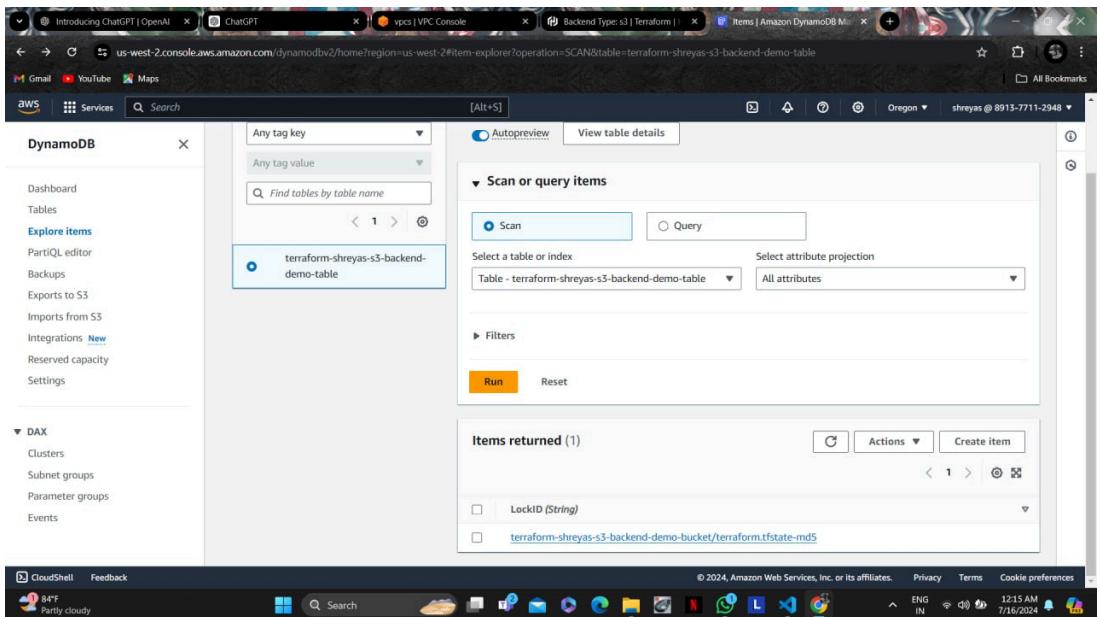
At the bottom, there's a footer with links for CloudShell, Feedback, and various system icons.

Dynamodb table created

The screenshot shows a Visual Studio Code (VS Code) interface with the following details:

- File Explorer:** Shows the project structure under "KUBERNETES".
- Editor:** Displays a Terraform configuration file (main.tf) containing code to set up an S3 backend and a DynamoDB table.
- Terminal:** Shows the command "powershell" is currently active.
- Status Bar:** Shows the terminal is at line 6, column 62, with 4 spaces, using CRLF line endings, and the current date and time as 7/16/2024.

backend.tf



State locking(Lock ID)