

Deploying with Terraform

Software Architecture

March 6, 2023

Brae Webb

Teacher Version

1 Before Class

Ensure you've had practice using the AWS Academy learner lab. It's preferable if you already have [terraform installed](#)¹. Please also have one of IntelliJ IDEA, PyCharm, or VSCode with the terraform plugin installed.

2 This Week

This week we are going to deploy TaskOverflow our Todo Application to AWS using a hosted database and a single server website.

Specifically, this week you need to:

- Authenticate Terraform to use the AWS learner lab.
- Configure an RDS database.

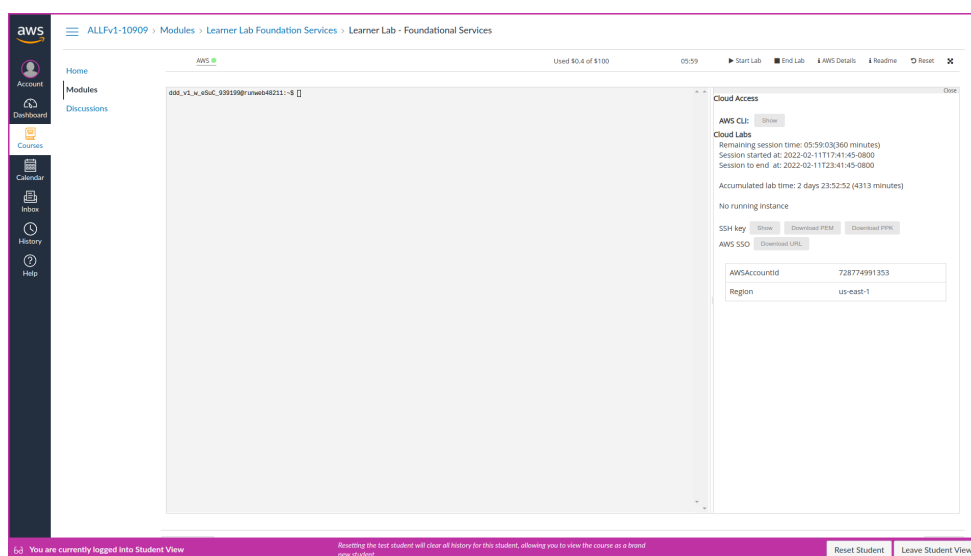
Path A Configure a single server and deploy the container.

Path B Configure a ECS cluster and deploy the container.

3 Using Terraform in AWS Learner Labs

Following the steps from the week four practical, start a learner lab in AWS Academy. For this practical, you do not need to create any resources in the AWS Console. The console can be used to verify that Terraform has correctly provisioned resources.

1. Once the learner lab has started, click on 'AWS Details' to display information about the lab.



¹<https://learn.hashicorp.com/tutorials/terraform/install-cli>

2. Click on the first 'Show' button next to 'AWS CLI' which will display a text block starting with [default].
3. Create a directory for this week's practical.
4. Within that directory create a `credentials` file and copy the contents of the text block into the file.
Do not share this file contents — do not commit it.
5. Create a `main.tf` file in the same directory with the following contents:

```
» cat main.tf

1 terraform {
2     required_providers {
3         aws = {
4             source = "hashicorp/aws"
5             version = "~> 4.0"
6         }
7     }
8 }

10 provider "aws" {
11     region = "us-east-1"
12     shared_credentials_files = [".credentials"]
13 }
```

The `terraform` block specifies the required external dependencies, here we need to use the AWS provider. The `provider` block configures the AWS provider, instructing it which region to use and how to authenticate (using the credentials file we created).

6. We need to initialise terraform which will fetch the required dependencies. This is done with the `terraform init` command.

```
$ terraform init
```

This command will create a `.terraform` directory which stores providers and a provider lock file, `.terraform.lock.hcl`.

7. To verify that we have setup Terraform correctly, use `terraform plan`.

```
$ terraform plan
```

As we currently have no resources configured, it should find that no changes are required. Note that this does not ensure our credentials are correctly configured as Terraform has no reason to try authenticating yet.

4 Deploying a Database in AWS

Info

This section manually deploys a Postgresql RDS instance, which is not the courses end goals but is a good way to get started with AWS. Latter this practical we will use terraform to create the database, so this section is optional and is better to be observed rather than actioned.

For the teacher

Instruct the class to observe you making the database and not to follow along.



Figure 1: Remote database deployment diagram

This is the last time we will heavily use the AWS user interface in the practicals. If you already feel confident in the AWS environment skip this section and move on to the next one.

For the teacher

Give students time to start the labs, could take up to 10 minutes.

To get started let's jump into the lab environment and have a look at AWS RDS which is an AWS managed database service. To get to the RDS service either search it or browse Services -> Database -> RDS as shown below.



Now we are in the management page for all our database instances, for today we just want to get a small instance running to explore the service. Head to “DB Instances (0/40)”.



This page should appear familiar as it's very similar to the AWS EC2 instance page. Let us create a new database by hitting the "Create Database" button.



Warning

In the next section we cannot use the Easy Create method as it tries to create a IAM account which is not allowed in the labs. Going forward we would typically do this using Terraform so we can easily avoid these restrictions.

For the teacher

Feel free to talk about the other offerings here, but make sure to flame Oracle and Microsoft SQL Server. A good thing to point out is the Amazon Aurora which is the serverless version of RDS.

We will be creating a standard database so select standard and Postgresql. We will use version 14 which is a fairly recent release.

Choose a database creation method [Info](#)

☒ Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

☐ Amazon Aurora



☒ MySQL



☐ MariaDB



☐ PostgreSQL



☐ Oracle



☐ Microsoft SQL Server



Edition

☒ MySQL Community



Known issues/limitations

Review the [Known issues/limitations](#) [to learn about potential compatibility issues with specific database versions.](#)

Version

MySQL 8.0.27



For today we are going to use “Free Tier” but in the future, you may wish to explore the different deployment options. Please peruse the available different options.

For the teacher

Walk through what Multi-AZ means aka Multiple Availability Zones.

Templates

Choose a sample template to meet your use case.

☐ **Production**
Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
This instance is intended for development use outside of a production environment.

☒ **Free tier**
Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.
[Info](#)

Availability and durability

Deployment options [Info](#)

The deployment options below are limited to those supported by the engine you selected above.

- ☒ **Single DB instance (not supported for Multi-AZ DB cluster snapshot)**
Creates a single DB instance with no standby DB instances.
- ☐ **Multi-AZ DB instance (not supported for Multi-AZ DB cluster snapshot)**
Creates a primary DB instance and a standby DB instance in a different AZ. Provides high availability and data redundancy, but the standby DB instance doesn't support connections for read workloads.
- ☐ **Multi-AZ DB Cluster - new**
Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.

Now we need to name our database and create credentials to connect via. Here is where you can enter in credentials for the main account of the database.

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

☐ Auto generate a password

Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm password [Info](#)

For exploring the process select t2.micro, which should be adequate for our needs.

For the teacher

May want to mention that burstable is not recommended for consistently used databases. Usually DBs are memory focused and thus the standard or memory optimised are used.

DB instance class

DB instance class [Info](#)

☐ Standard classes (includes m classes)

☐ Memory optimized classes (includes r and x classes)

☒ Burstable classes (includes t classes)

db.t2.micro

1 vCPUs

1 GiB RAM

Not EBS Optimized



☐ Include previous generation classes

For storage we will leave all the default options.

Storage

Storage type [Info](#)

General Purpose SSD (gp2)
Baseline performance determined by volume size

Allocated storage

20

GiB

(Minimum: 20 GiB. Maximum: 16,384 GiB) Higher allocated storage **may improve** IOPS performance.

You might see better baseline performance with your selected volume size by specifying General Purpose SSD storage. [Learn more about using Provisioned IOPS storage for consistent performance.](#)

Storage autoscaling [Info](#)

Provides dynamic scaling support for your database's storage based on your application's needs.

☒

Enable storage autoscaling
Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

Maximum storage threshold [Info](#)

Charges will apply when your database autoscales to the specified threshold

1000

GiB

Minimum: 21 GiB. Maximum: 16,384 GiB

In connectivity we need to make sure our instance is publicly available. Usually you don't want to expose your databases publicly and, would instead, have a web server sitting in-front. For our learning purposes though we are gonna expose it directly just like we did with our EC2 instances early in the course.

When selecting public access as yes we have to create a new Security Group, give this Security Group a sensible name.

9

Connectivity



Virtual private cloud (VPC) [Info](#)

VPC that defines the virtual networking environment for this DB instance.

Default VPC (vpc-07f8e8ea0408a9db9) ▼

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

Subnet group [Info](#)

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default-vpc-07f8e8ea0408a9db9 ▼

Public access [Info](#)

☒ Yes

Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☐ No

RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group

Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.



Choose existing

Choose existing VPC security groups



Create new

Create new VPC security group

New VPC security group name

todoapp-manual

Availability Zone [Info](#)

No preference ▼

▼ Additional configuration

Database port [Info](#)

TCP/IP port that the database will use for application connections.

3306



We will leave the authentication as password based but we need to expand the “Additional configuration”. Fill in the “Initial Database Name” section to be “todo”, this is similar to what we had in the Docker Composes environment variable.

For the teacher

The other options here are to do with the parameters used to start the database, it is uncommon to have to change these but this is where any settings you would pass in via cli to the db would be set.

Database authentication

Database authentication options [Info](#)

- ☒ **Password authentication**
Authenticates using database passwords.
- ☐ **Password and IAM database authentication**
Authenticates using the database password and user credentials through AWS IAM users and roles.
- ☐ **Password and Kerberos authentication**
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

▼ Additional configuration

Database options, backup enabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled.

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

Option group [Info](#)

Now we can click create which will take some time.

Estimated monthly costs

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free:

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier.](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page.](#)

 You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

Cancel

Create database

Depending on your database it may take 10 to 30 minutes to create, the larger and more complicated the setup the longer it usually takes. The database will also do a initial backup when its created.

RDS > Databases

Databases

☒ Group resources

 Modify Actions ▼ Restore from S3 Create database



DB identifier



Role ▼



Engine ▼



Region & AZ ▼



Size ▼



Status ▼



CPU



todoapp-manual

Instance

MySQL Community

us-east-1f

db.t2.micro

 Backing-up

100%

When the database has finished being created you can select it to view the configuration and details. In this menu we also see the endpoint address which we will need to copy into our docker compose file.

12

Successfully created database `todoapp-manual`

View connection details

RDS > Databases > todoapp-manual

todoapp-manual

Modify

Actions

Summary

DB identifier todoapp-manual	CPU <div><div></div></div> 10.83%	Status Available	Class db.t2.micro
Role Instance	Current activity <div><div></div></div> 0 Connections	Engine MySQL Community	Region & AZ us-east-1f

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Connectivity & security

<div>Endpoint & port</div> <div>Endpoint todoapp-manual.cwf1cdgoxax.us-east-1.rds.amazonaws.com</div> <div>Port 3306</div>	<div>Networking</div> <div>Availability Zone us-east-1f</div> <div>VPC vpc-07f8e8ea0408a9db9</div> <div>Subnet group default-vpc-07f8e8ea0408a9db9</div> <div>Subnets subnet-0556db549e22800f1 subnet-0da793726639bd6d8 subnet-091ee1d302ae831a9 subnet-0b932c4d6a4154b2a subnet-0416084227ea643b4 subnet-05d92ccc16a62294f</div>	<div>Security</div> <div>VPC security groups todoapp-manual2 (sg-0cc1a6ba52b85e23c) Active</div> <div>Publicly accessible Yes</div> <div>Certificate authority rds-ca-2019</div> <div>Certificate authority date August 23, 2024, 03:08 (UTC±3:08)</div>
--	---	---

5 RDS Database with Terraform

Now would be a good time to browse the documentation for the RDS database in Terraform: https://registry.terraform.io/providers/hashicorp/aws/latest/docs/resources/db_instance. Using our manual configuration, we can come up with a resource with the appropriate parameters as below:

```
» cat main.tf
1 locals {
2   password = "foobarbaz" # this is bad
3 }
4
5 resource "aws_db_instance" "todoapp-database" {
6   allocated_storage = 20
7   max_allocated_storage = 1000
8   engine = "postgresql"
9   engine_version = "14"
10  instance_class = "db.t2.micro"
11  name = "todo"
12  username = "todo"
```

```

13 password = local.password
14 parameter_group_name = "default.postgresql14"
15 skip_final_snapshot = true
16 vpc_security_group_ids = [aws_security_group.todo-database.id]
17 publicly_accessible = true

19 tags = {
20     Name = "todo-database"
21 }
22 }

```

Remember to create an appropriate security group as we did through the user interface.

```

1 resource "aws_security_group" "todo-database" {
2     name = "todo-database"
3     description = "Allow inbound Postgresql traffic"

5     ingress {
6         from_port = 5432
7         to_port = 5432
8         protocol = "tcp"
9         cidr_blocks = ["0.0.0.0/0"]
10    }

12    egress {
13        from_port = 0
14        to_port = 0
15        protocol = "-1"
16        cidr_blocks = ["0.0.0.0/0"]
17        ipv6_cidr_blocks = [ "::/0" ]
18    }

20    tags = {
21        Name = "todo-database"
22    }
23 }

```

6 Container on AWS

As we mentioned in the Infrastructure as Code notes [1], in this course we will use Docker to configure machines and Terraform to configure infrastructure. AWS has the ability to deploy Docker containers using a service known as Elastic Container Service (ECS). We will cover ECS and deploying manually via EC2 so you can use the method you feel most comfortable with.

For this practical we have made available a docker container running the todo application which you can use to deploy to AWS. This container is available on Github under the CSSE6400 organisation <https://ghcr.io/csse6400/taskoverflow:latest>. This container is very similar to what you have been building in the practicals but contains a simple UI and some extra features for the future practicals.

6.1 Setup

All of the different ways that we can deploy our application we have already decided that we are gonna offload the database to AWS. This means that we can move all the "state" of our application away from our containerised environment.

To start off we are gonna use what we had above to create a database and the default terraform. Edit your files so that they match what's provided below:

6.2 [Path A] EC2

Congrats you have chosen to go down the EC2 path which builds on what we experienced in the previous practicals.

6.2.1 Finished Terraform

```
» cat main.tf

terraform {
  required_providers {
    aws = {
      source = "hashicorp/aws"
      version = "~> 4.0"
    }
  }
}

provider "aws" {
  region = "us-east-1"
  shared_credentials_files = ["/credentials"]
  default_tags {
    tags = {
      Course = "CSSE6400"
      Name = "TaskOverflow"
      Automation = "Terraform"
    }
  }
}

locals {
  image = "ghcr.io/csse6400/taskoverflow:latest"
  database_username = "administrator"
  database_password = "VerySecurePasswordByYourBoiEvan"
}

resource "aws_db_instance" "database" {
  allocated_storage = 20
  max_allocated_storage = 1000
  engine = "postgres"
  engine_version = "14"
```

```

instance_class = "db.t4g.micro"
db_name = "todo"
username = local.database_username
password = local.database_password
parameter_group_name = "default.postgres14"
skip_final_snapshot = true
vpc_security_group_ids = [aws_security_group.database.id]
publicly_accessible = true
}

resource "aws_security_group" "database" {
  name = "todo-database"
  description = "Allow inbound Postgres traffic"

  ingress {
    from_port = 5432
    to_port = 5432
    protocol = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }

  egress {
    from_port = 0
    to_port = 0
    protocol = "-1"
    cidr_blocks = ["0.0.0.0/0"]
    ipv6_cidr_blocks = [ "::/0" ]
  }
}

resource "aws_instance" "todo" {
  ami = "ami-005f9685cb30f234b"
  instance_type = "t2.micro"
  key_name = "vockey"

  user_data_replace_on_change = true
  user_data = <<-EOT
#!/bin/bash
yum update -y
yum install -y docker
service docker start
systemctl enable docker
usermod -a -G docker ec2-user
docker run --restart always -e SQLALCHEMY_DATABASE_URI=postgresql://${local.
  database_username}:${local.database_password}@${aws_db_instance.database.address
}:${aws_db_instance.database.port}/${aws_db_instance.database.db_name} -p
  6400:6400 ${local.image}
EOT

  security_groups = [aws_security_group.todo.name]

```



```

}

resource "aws_security_group" "todo" {
  name = "todo"
  description = "TaskOverflow Security Group"

  ingress {
    from_port = 6400
    to_port = 6400
    protocol = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }

  ingress {
    from_port = 22
    to_port = 22
    protocol = "tcp"
    cidr_blocks = ["0.0.0.0/0"]
  }

  egress {
    from_port = 0
    to_port = 0
    protocol = "-1"
    cidr_blocks = ["0.0.0.0/0"]
  }
}

output "url" {
  value = "http://${aws_instance.todo.public_ip}:6400/"
}

```

6.3 [Path B] ECS

Congrats you have chosen to go down the ECS path which mimics the same environment that you have via Docker Compose but as a service on AWS. This path is new for the course this year so please let your tutors know any particular issues you have.

6.3.1 Finished Terraform

```

% cat main.tf

terraform {
  required_providers {
    aws = {
      source = "hashicorp/aws"
      version = "~> 4.0"
    }
  }
}

```

```

    }
}

provider "aws" {
    region = "us-east-1"
    shared_credentials_files = ["/credentials"]
    default_tags {
        tags = {
            Course = "CSSE6400"
            Name = "TaskOverflow"
            Automation = "Terraform"
        }
    }
}

locals {
    image = "ghcr.io/csse6400/taskoverflow:latest"
    database_username = "administrator"
    database_password = "VerySecurePasswordByYourBoiEvan"
}

resource "aws_db_instance" "database" {
    allocated_storage = 20
    max_allocated_storage = 1000
    engine = "postgres"
    engine_version = "14"
    instance_class = "db.t4g.micro"
    db_name = "todo"
    username = local.database_username
    password = local.database_password
    parameter_group_name = "default.postgres14"
    skip_final_snapshot = true
    vpc_security_group_ids = [aws_security_group.database.id]
    publicly_accessible = true
}

resource "aws_security_group" "database" {
    name = "todo-database"
    description = "Allow inbound Postgres traffic"

    ingress {
        from_port = 5432
        to_port = 5432
        protocol = "tcp"
        cidr_blocks = ["0.0.0.0/0"]
    }

    egress {
        from_port = 0
        to_port = 0
    }
}

```

```

    protocol = "-1"
    cidr_blocks = ["0.0.0.0/0"]
    ipv6_cidr_blocks = [ "::/0" ]
  }
}

data "aws_iam_role" "lab" {
  name = "LabRole"
}

resource "aws_ecs_cluster" "taskoverflow" {
  name = "taskoverflow"
}

resource "aws_ecs_task_definition" "todo" {
  family = "todo"
  network_mode = "awsvpc"
  requires_compatibilities = ["FARGATE"]
  cpu = 1024
  memory = 2048
  execution_role_arn = data.aws_iam_role.lab.arn

  container_definitions = <<DEFINITION
[
  {
    "image": "${local.image}",
    "cpu": 1024,
    "memory": 2048,
    "name": "todo",
    "networkMode": "awsvpc",
    "portMappings": [
      {
        "containerPort": 6400,
        "hostPort": 6400
      }
    ],
    "environment": [
      {
        "name": "SQLALCHEMY_DATABASE_URI",
        "value": "postgresql://${local.database_username}:${local.database_password}
          @${aws_db_instance.database.address}:${aws_db_instance.database.port}/${
            aws_db_instance.database.db_name}"
      }
    ],
    "logConfiguration": {
      "logDriver": "awslogs",
      "options": {
        "awslogs-group": "/taskoverflow/todo",
        "awslogs-region": "us-east-1",
        "awslogs-stream-prefix": "ecs",

```

```

        "awslogs-create-group": "true"
    }
}
}
]
DEFINITION
}

data "aws_vpc" "default" {
    default = true
}

data "aws_subnets" "private" {
    filter {
        name = "vpc-id"
        values = [data.aws_vpc.default.id]
    }
}

resource "aws_ecs_service" "taskoverflow" {
    name = "taskoverflow"
    cluster = aws_ecs_cluster.taskoverflow.id
    task_definition = aws_ecs_task_definition.todo.arn
    desired_count = 1
    launch_type = "FARGATE"

    network_configuration {
        subnets = data.aws_subnets.private.ids
        security_groups = [aws_security_group.todo.id]
        assign_public_ip = true
    }
}

resource "aws_security_group" "todo" {
    name = "todo"
    description = "TaskOverflow Security Group"

    ingress {
        from_port = 6400
        to_port = 6400
        protocol = "tcp"
        cidr_blocks = ["0.0.0.0/0"]
    }

    ingress {
        from_port = 22
        to_port = 22
        protocol = "tcp"
        cidr_blocks = ["0.0.0.0/0"]
    }
}

```

```
egress {  
  from_port = 0  
  to_port = 0  
  protocol = "-1"  
  cidr_blocks = ["0.0.0.0/0"]  
}  
}
```

6.4 [Path C] EKS / K8S

This path is not available in the course yet but we recommend that if you liked the course to have a look at Kubernetes as it is widely used in industry.

References

- [1] B. Webb, "Infrastructure as code," March 2022. <https://csse6400.uqcloud.net/handouts/iac.pdf>.