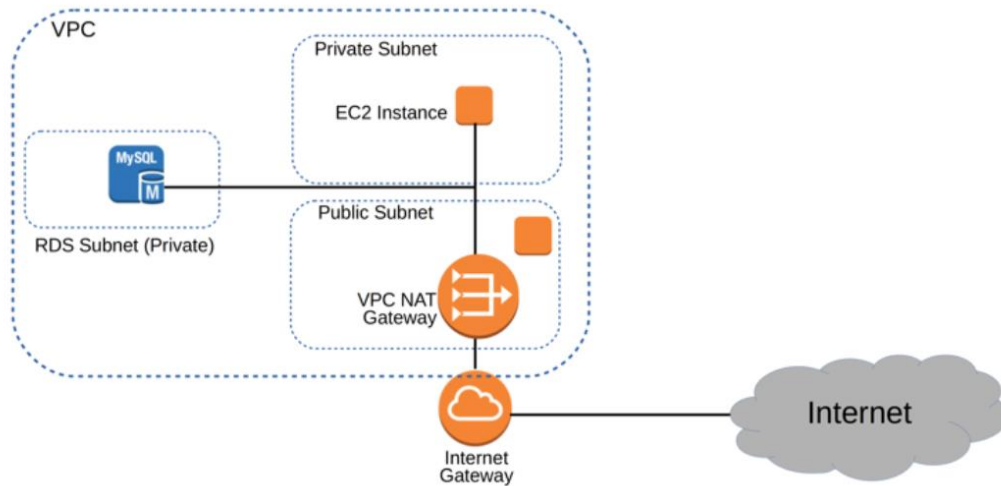


Hosting a website from an instance in a private subnet



1. Create a new VPC and name it a3VPC


- Log in to AWS Management Console
- Go to VPC Dashboard
- Click 'Create VPC'
 - Name tag: 'a3VPC'
 - IPv4 CIDR block: 10.0.0.0/16
 - No IPv6 CIDR block
 - Tenancy: Default
 - DNS hostnames: Enabled

vpc-04ae7ba417a847373 / a3VPC

Actions

Details

Info

<div>VPC ID</div> <div> vpc-04ae7ba417a847373</div>	<div>State</div> <div> Available</div>	<div>DNS hostnames</div> <div>Enabled</div>	<div>DNS resolution</div> <div>Enabled</div>
<div>Tenancy</div> <div>Default</div>	<div>DHCP options set</div> <div>dopt-64f6850f</div>	<div>Main route table</div> <div>rtb-02e41504d2bfa623 / a3RouteTable</div>	<div>Main network ACL</div> <div>acl-0cf7dad64dee3bd32</div>
<div>Default VPC</div> <div>No</div>	<div>IPv4 CIDR</div> <div>10.0.0.0/16</div>	<div>IPv6 pool</div> <div>—</div>	<div>IPv6 CIDR</div> <div>—</div>
<div>Route 53 Resolver DNS Firewall rule groups</div> <div>—</div>	<div>Owner ID</div> <div> 888742301715</div>		

- A VPC requires an internet gateway
- In the VPC Dashboard, click 'Internet Gateways', "Create internet gateway"
 - Name tag: a3InternetGateway
- Click "Action", "Attach to VPC"
 - Select: a3VPC

igw-08c08fa69e43397e5 / a3InternetGateway

Actions ▾

Details [Info](#)

Internet gateway ID

igw-08c08fa69e43397e5

State

Attached

VPC ID

vpc-04ae7ba417a847373 | a3VPC

Owner

888742301715

- The route table rtb-02e41504d2bfba623 has been automatically created and attached to a3VPC
 - I will use this route table for the private subnet
 - Click “Route Tables”, name this default route table “a3PrivateRouteTable”
- Create another route table for the public subnet
 - Name: a3PublicRouteTable
 - VPC: a3VPC
- Screenshots of these route tables will be taken later after subnet associations.
- Create a private subnet
 - Navigate to VPC Dashboard, click ‘Subnets’, click ‘Create subnet’
 - VPC ID: a3VPC
 - Subnet name: a3PrivateSubnet
 - Availability Zone: US East (Ohio) / us-east-2a
 - IPv4 CIDR block: 10.0.0.0/24
 - Auto-assign public IPv4 address: No
 - Route table association: a3PrivateRouteTable

subnet-0a156672fc17deb41 / a3PrivateSubnet

Actions ▾

Details

Subnet ID

subnet-0a156672fc17deb41

Available IPv4 addresses

251

VPC

vpc-04ae7ba417a847373 | a3VPC

Auto-assign public IPv4 address

No

Outpost ID

–

Subnet ARN

arn:aws:ec2:us-east-2:888742301715:subnet/subnet-0a156672fc17deb41

IPv6 CIDR

–

Route table

rtb-02e41504d2bfba623 | a3PrivateRouteTable

Auto-assign IPv6 address

No

IPv4 CIDR reservations

–

State

Available

Availability Zone

us-east-2a

Network ACL

acl-0cf7dad64dee3bd32

Auto-assign customer-owned IPv4 address

No

IPv6 CIDR reservations

–

IPv4 CIDR

10.0.0.0/24

Availability Zone ID

use2-az1

Default subnet

No

Customer-owned IPv4 pool

–

Owner

888742301715

- Create a public subnet
 - VPC ID: a3VPC
 - Subnet name: a3PublicSubnet
 - Availability Zone: US East (Ohio) / us-east-2a
 - IPv4 CIDR block: 10.0.1.0/24
 - Auto-assign public IPv4 address: Yes
 - Route table association: a3PublicRouteTable

subnet-066dbeb3489e773c2 / a3PublicSubnet Actions

Details

Subnet ID subnet-066dbeb3489e773c2	Subnet ARN arn:aws:ec2:us-east-2:888742301715:subnet/subnet-066dbeb3489e773c2	State Available	IPv4 CIDR 10.0.1.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone us-east-2a	Availability Zone ID use2-az1
VPC vpc-04ae7ba417a847373 a3VPC	Route table rtb-07f40accea94dc6eb a3PublicRouteTable	Network ACL acl-0cf7dad64dee3bd32	Default subnet No
Auto-assign public IPv4 address Yes	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -	Owner 888742301715

- Allocate an elastic IP address for the NAT Gateway
 - Navigate to VPC Dashboard, click "Elastic IPs", "Allocate Elastic IP address"
 - Public IPv4 address pool: Amazon's pool of IPv4 addresses
 - Add tag: Key: Name, Value: a3ElasticIP

Elastic IP addresses (1) Actions Allocate Elastic IP address

< 1 >

<input type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID
<input type="checkbox"/>	a3ElasticIP	3.138.81.226	Public IP	eipalloc-050c73ea2721c16d7	-

- Create a NAT Gateway
 - Navigate to VPC Dashboard, click "NAT Gateways", "Create NAT gateway"
 - Name: a3NATGateway
 - Subnet: a2PublicSunet
 - Connectivity type: Public
 - allocate elastic IP address: a3ElasticIP

nat-07f0092bce363831c / a3NATGateway Delete

Details [Info](#)

NAT gateway ID nat-07f0092bce363831c	Connectivity type Public	State Available	State message Info -
Elastic IP address 3.138.81.226	Private IP address 10.0.1.35	Network interface ID eni-03005d8ce9815f020	VPC vpc-04ae7ba417a847373 / a3VPC
Subnet subnet-066dbeb3489e773c2 / a3PublicSubnet	Created 2021/09/24 14:04 GMT+10	Deleted -	

- Edit a3PrivateRouteTable to point internet-bound traffic to a3NATGateway
 - Select a3RouteTable, click "Actions", "Edit routes", "Add routes":
 - Destination: 0.0.0.0/0, Target: a3InternetGateway

- Destination: 0.0.0.0/0, Target: a3NATGateway

rtb-02e41504d2bfba623 / a3PrivateRouteTable Actions ▼

Details [Info](#)

Route table ID rtb-02e41504d2bfba623	Main Yes	Explicit subnet associations subnet-0a156672fc17deb41 / a3PrivateSubnet	Edge associations –
VPC vpc-04ae7ba417a847373 a3VPC	Owner ID 888742301715		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Edit routes

Filter routes Both ▼ < 1 > ⚙️

Destination ▼	Target ▼	Status ▼	Propagated ▼
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-07f0092bce363831c	Active	No

- Edit a3PublicRouteTable to point internet-bound traffic to a3InternetGateway
 - Select a3RouteTable, click “Actions”, “Edit routes”, “Add routes”:
 - Destination: 0.0.0.0/0, Target: a3InternetGateway
 - Destination: 0.0.0.0/0, Target: a3InternetGateway

rtb-07f40acce94dc6eb / a3PublicRouteTable Actions ▼

Details [Info](#)

Route table ID rtb-07f40acce94dc6eb	Main No	Explicit subnet associations subnet-066db3489e773c2 / a3PublicSubnet	Edge associations –
VPC vpc-04ae7ba417a847373 a3VPC	Owner ID 888742301715		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Edit routes

Filter routes Both ▼ < 1 > ⚙️

Destination ▼	Target ▼	Status ▼	Propagated ▼
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-08c08fa69e43397e5	Active	No

2. Create an instance in a private subnet

- Create a key pair in the EC2 Dashboard
 - Name: a3Key
 - Key pair type: RSA
 - File format: ppk

Key pairs (1) Info

Filter key pairs

Actions

Create key pair

<input type="checkbox"/>	Name	Type	Fingerprint	ID
<input type="checkbox"/>	a3Key	rsa	ea:8d:a4:82:65:1f:c9:5c:49:8b:b2:ec:5c:...	key-0329f365caac7de72

- Launch an instance in a3PrivateSubnet
- Navigate to EC2 Dashboard and click 'Launch instance'
- Step 1: Select 'Amazon Linux 2 AMI (HVM) SSD Volume Type 64-bit (x86)'
- Step 2: Choose the Instance Type 't2.micro'
- Step 3: Configure instance details:
 - Network: a3VPC
 - Subnet: a3PrivateSubnet
 - Auto-assign Public IP: Use subnet setting (Disable)
 - Advanced Details: User data: insert the following code:

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
mkdir var
cd /var
mkdir www
cd /var/www
mkdir html
cd /var/www/html
touch index.html
cat << EOF > index.html
<!DOCTYPE html>
<html lang="en">
<body>
<h1 style="color:MediumTurquoise; font-family:Broadway; font-size:500%; text-align:center">Private Subnet</h1>
</body>
</html>
EOF
```
- Step 4: Add Storage: Keep the default selection of 8 GiB General Purpose SSD (gp2)
- Step 5: Add Tags: Key 'Name', Value 'a3PrivateInstance'
- Step 6: Select an existing security group: sg-0d559e64f02375dbc (default)
- Step 7: Review Instance Launch
- Select the key pair 'a3Key'
- Launch a3PrivateInstance

Instance summary for i-00bd9cf0a91c30874 (a3PrivateInstance) Info		
Updated less than a minute ago		
Instance ID i-00bd9cf0a91c30874 (a3PrivateInstance)	Public IPv4 address –	Private IPv4 addresses 10.0.0.99
IPv6 address –	Instance state Running	Public IPv4 DNS –
Private IPv4 DNS ip-10-0-0-99.us-east-2.compute.internal	Instance type t2.micro	Elastic IP addresses –
VPC ID vpc-04ae7ba417a847373 (a3VPC)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	IAM Role –
Subnet ID subnet-0a156672fc17deb41 (a3PrivateSubnet)		

3. Create an instance in a public subnet

- Launch an instance in a3PublicSubnet
- Step 1: Select 'Amazon Linux 2 AMI (HVM) SSD Volume Type 64-bit (x86)'
- Step 2: Choose the Instance Type 't2.micro'
- Step 3: Configure instance details:
 - Network: a3VPC
 - Subnet: a3PublicSubnet
 - Auto-assign Public IP: Use subnet setting (Enable)
- Step 4: Add Storage: Keep the default selection of 8 GiB General Purpose SSD (gp2)
- Step 5: Add Tags: Key 'Name', Value 'a3PublicInstance'
- Step 6: Select an existing security group: sg-0d559e64f02375dbc (default)
- Step 7: Review Instance Launch
- Select the key pair 'a3Key' and launch a3PublicInstance

Instance summary for i-042ba6af9af5a64a5 (a3PublicInstance) Info		
Updated less than a minute ago		
Instance ID i-042ba6af9af5a64a5 (a3PublicInstance)	Public IPv4 address 18.221.33.179 open address	Private IPv4 addresses 10.0.1.64
IPv6 address –	Instance state Running	Public IPv4 DNS ec2-18-221-33-179.us-east-2.compute.amazonaws.com open address
Private IPv4 DNS ip-10-0-1-64.us-east-2.compute.internal	Instance type t2.micro	Elastic IP addresses –
VPC ID vpc-04ae7ba417a847373 (a3VPC)	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	IAM Role –
Subnet ID subnet-066dbeb3489e773c2 (a3PublicSubnet)		

- Access a3PrivateInstance from a3PublicInstance
- On my Windows device, open Pageant and add the a3Key key pair
- Open SSH PuTTY:
 - Host Name: use the public DNS address of a3PublicInstance: ec2-18-221-33-179.us-east-2.compute.amazonaws.com
 - In SSH-Auth, click 'Allow agent forwarding' and add the key pair a3Key
 - In the PuTTY terminal, log in as 'ec2-user'
 - Access a3PrivateInstance using its private IP address: ssh [ec2-user@10.0.0.99](#)

```
ec2-user@ip-10-0-0-99:~  
login as: ec2-user  
Authenticating with public key "a3Key" from agent  
Last login: Sat Sep 25 01:47:21 2021 from 1.144.111.146  
  
  _ | ( _ | _ )  
  _ | \ _ | _ |  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-1-64 ~]$ ssh ec2-user@10.0.0.99  
Last login: Sat Sep 25 01:47:37 2021 from ip-10-0-1-64.us-east-2.compute.interna  
l  
  
  _ | ( _ | _ )  
  _ | \ _ | _ |  
Amazon Linux 2 AMI  
  
https://aws.amazon.com/amazon-linux-2/  
[ec2-user@ip-10-0-0-99 ~]$
```

- Display the directory structure for the webserver

```
ec2-user@ip-10-0-0-99:/var/www/html  
[ec2-user@ip-10-0-0-99 ~]$ cd /var/www/html  
[ec2-user@ip-10-0-0-99 html]$ ls  
index.html  
[ec2-user@ip-10-0-0-99 html]$
```

- Display the HTML code for the index file

vim index.html

```
ec2-user@ip-10-0-0-99:/var/www/html  
<?DOCTYPE html>  
<html lang="en">  
<body>  
<h1 style="color:MediumTurquoise; font-family:Broadway; font-size:500%; text-align:center">Private Subnet</h1>  
</body>  
</html>
```

4. Create an RDS instance in a private subnet

- An RDS instance requires a Subnet Group with subnets in at least two availability zones
- Create another private subnet in a new availability zone
 - Navigate to VPC Dashboard, click "Subnets", "Create subnet"
 - VPC: a3VPC
 - Availability Zone: US East (Ohio) / us-east-2b
 - IPv4 CIDR block: 10.0.2.0/24
 - Name: a3PrivateSubnetB

subnet-0d189e77da09e3c3d / a3PrivateSubnetB			
Details			
Subnet ID subnet-0d189e77da09e3c3d	Subnet ARN arn:aws:ec2:us-east-2:888742301715:subnet/subnet-0d189e77da09e3c3d	State Available	IPv4 CIDR 10.0.2.0/24
Available IPv4 addresses 251	IPv6 CIDR -	Availability Zone us-east-2b	Availability Zone ID use2-az2
VPC vpc-04ae7ba417a847373 a3VPC	Route table rtb-02e41504d2bfa623 a3PrivateRouteTable	Network ACL acl-0cf7dad64dee3bd32	Default subnet No
Auto-assign public IPv4 address No	Auto-assign IPv6 address No	Auto-assign customer-owned IPv4 address No	Customer-owned IPv4 pool -
Outpost ID -	IPv4 CIDR reservations -	IPv6 CIDR reservations -	Owner 888742301715

- Navigate to RDS Dashboard, click “Subnet Groups”, “Create DB Subnet Group”
 - Name: a3SubnetGroup
 - Description: a3SubnetGroup
 - VPC: a3VPC
 - Availability Zones: us-east-2a & us-east-2b
 - Subnets: a3PrivateSubnet & a3PrivateSubnetB

a3subnetgroup		
Subnet group details		
VPC ID vpc-04ae7ba417a847373		
ARN arn:aws:rds:us-east-2:888742301715:subgrp:a3subnetgroup		
Description a3SubnetGroup		
Subnets (2)		
Availability zone	Subnet ID	CIDR block
us-east-2a	subnet-0a156672fc17deb41	10.0.0.0/24
us-east-2b	subnet-0d189e77da09e3c3d	10.0.2.0/24

- Navigate to RDS Dashboard, click “Databases”, “Create database”
 - Database creation method: Standard create
 - Engine options: MariaDB 10.4.13
 - Templates: Free tier
 - Settings:
 - DB instance identifier: a3Database
 - Master username: admin
 - Master password: *****
 - DB instance class: db.t2.micro
 - Storage: General Purpose SSD (gp2) 20 GiB
 - VPC: a3VPC
 - Subnet group: a3subnetgroup
 - Public access: No
 - VPC security group: Choose existing: default
 - Availability Zone: us-east-2a
 - Database port: 3306

a3database

Modify
Actions

Summary

DB identifier a3database	CPU -	Status Available	Class db.t2.micro
Role Instance	Current activity	Engine MariaDB	Region & AZ us-east-2a

Connectivity & security
Monitoring
Logs & events
Configuration
Maintenance & backups
Tags

Connectivity & security

<div>Endpoint & port</div> <div>Endpoint a3database.cfz03euto6rv.us-east-2.rds.amazonaws.com</div> <div>Port 3306</div>	<div>Networking</div> <div>Availability Zone us-east-2a</div> <div>VPC a3VPC (vpc-04ae7ba417a847373)</div> <div>Subnet group a3subnetgroup</div> <div>Subnets subnet-0d189e77da09e3c3d subnet-0a156672fc17deb41</div>	<div>Security</div> <div>VPC security groups default (sg-0d559e64f02375dbc) (active)</div> <div>Publicly accessible No</div> <div>Certificate authority rds-ca-2019</div> <div>Certificate authority date August 23, 2024, 03:08 (UTC+3:08)</div>
---	---	---

5. Access the database and create a table

- I access a3Database from a3PublicInstance
- Open SSH PuTTY: Host Name: ec2-user@18.221.33.179
- Install the MySQL command-line client

```
sudo su
yum install mariadb
```

```

root@ip-10-0-1-64:/home/ec2-user
Installed:
  mariadb.x86_64 1:5.5.68-1.amzn2

Complete!
[root@ip-10-0-1-64 ec2-user]#

```

- Connect to a3Database using the database endpoint

```
mysql -h a3database.cfz03euto6rv.us-east-2.rds.amazonaws.com -P 3306 -u admin -p
```

```

root@ip-10-0-1-64:/home/ec2-user
[root@ip-10-0-1-64 ec2-user]# mysql -h a3database.cfz03euto6rv.us-east-2.rds.amazonaws.com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 10.4.13-MariaDB-log Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>

```

- Create a table

```
create database student_registrations;
use student_registrations;
create table students (Name varchar(255), sID int);
insert into students (Name, sID) values ('Joe', 20221177);
show tables;
select * from students;
```

```
root@ip-10-0-1-64:/home/ec2-user
MariaDB [student_registrations]> show tables;
+-----+
| Tables_in_student_registrations |
+-----+
| students                         |
+-----+
1 row in set (0.00 sec)

MariaDB [student_registrations]> select * from students;
+-----+-----+
| Name | sID |
+-----+-----+
| Joe  | 20221177 |
+-----+-----+
1 row in set (0.00 sec)

MariaDB [student_registrations]>
```

You successfully deleted vpc-04ae7ba417a847373 / a3VPC

Your VPCs (1) [Info](#)

<input type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 pool
<input type="checkbox"/>	-	vpc-3ee17855	Available	172.31.0.0/16	-	-