

Module 7 Lab 2: VPC NAT

VPCs - Create VPC

VPCs > Create VPC

Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block, for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag ⓘ

IPv4 CIDR block* ⓘ

IPv6 CIDR block
☒ No IPv6 CIDR Block ⓘ
☐ Amazon provided IPv6 CIDR block

Tenancy ⓘ

* Required

Cancel Create

A new VPC, My VPC was created. This VPC will be home to two subnets.

Subnets - Create subnet

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag ⓘ

VPC* ⓘ

Availability Zone ⓘ

| VPC CIDRs | CIDR | Status | Status Reason |
|-----------|-------------|------------|---------------|
| | 10.0.0.0/16 | associated | |

IPv4 CIDR block* ⓘ

* Required

Cancel Create

The subnet will be based in the “My VPC” VPC, with the AZ us-west-1a.

VPC - Subnets

The screenshot displays the AWS Subnets page. A table lists several subnets, including 'Public 1'. An 'Actions' dropdown menu is open for 'Public 1', showing options like 'Delete subnet', 'Create flow log', 'Modify auto-assign IP settings', 'Edit IPv6 CIDRs', 'Edit network ACL association', 'Edit route table association', 'Share subnet', and 'Add/Edit Tags'. Below the table, the details for the selected subnet 'subnet-01eabb8989487eac0' are shown. The details include: Subnet ID, VPC (vpc-00d522b0b5c9e556), Available IPv4 Addresses (251), Availability Zone (us-west-1a), Network ACL (acl-0a44baae0c2a29), Auto-assign public IPv4 address (No), and Outpost ID (-). The 'Route Table' is 'rtb-00376893ebd9e1c74' and the 'Network ACL' is 'acl-09e23e26a4'.

The public subnet will need to be auto-assigned a public IPv4 address.

Subnets - Modify auto-assign IP settings

The screenshot shows the 'Modify auto-assign IP settings' page for the subnet 'subnet-01eabb8989487eac0'. The page has a header 'Subnets > Modify auto-assign IP settings' and a title 'Modify auto-assign IP settings'. Below the title, there is a description: 'Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.' The 'Subnet ID' is 'subnet-01eabb8989487eac0'. The 'Auto-assign IPv4' checkbox is checked, and the 'Enable auto-assign public IPv4 address' option is selected. At the bottom, there is a 'Required' label and 'Cancel' and 'Save' buttons.

This setting allows all instances launched in this public subnet to be auto-assigned a IPv4.

Subnets - Create subnet

[Subnets](#) > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

| Name tag | Public 2 | ? | | | | | | |
|-------------------|---|---------------|------|--------|---------------|-------------|------------|--|
| VPC* | vpc-00d5522b0b5c9e556 | ? | | | | | | |
| Availability Zone | us-west-1b | ? | | | | | | |
| VPC CIDRs | <table><thead><tr><th>CIDR</th><th>Status</th><th>Status Reason</th></tr></thead><tbody><tr><td>10.0.0.0/16</td><td>associated</td><td></td></tr></tbody></table> | | CIDR | Status | Status Reason | 10.0.0.0/16 | associated | |
| CIDR | Status | Status Reason | | | | | | |
| 10.0.0.0/16 | associated | | | | | | | |
| IPv4 CIDR block* | 10.0.2.0/24 | ? | | | | | | |

* Required

[Cancel](#) [Create](#)

The second public subnet is assigned to the “My VPC” VPC.

Subnets - Modify auto-assign IP settings

[Subnets](#) > Modify auto-assign IP settings

Modify auto-assign IP settings

Enable the auto-assign IP address setting to automatically request a public IPv4 or IPv6 address for an instance launched in this subnet. You can override the auto-assign IP settings for an instance at launch time.

Subnet ID subnet-003bca5fc8dddc34f

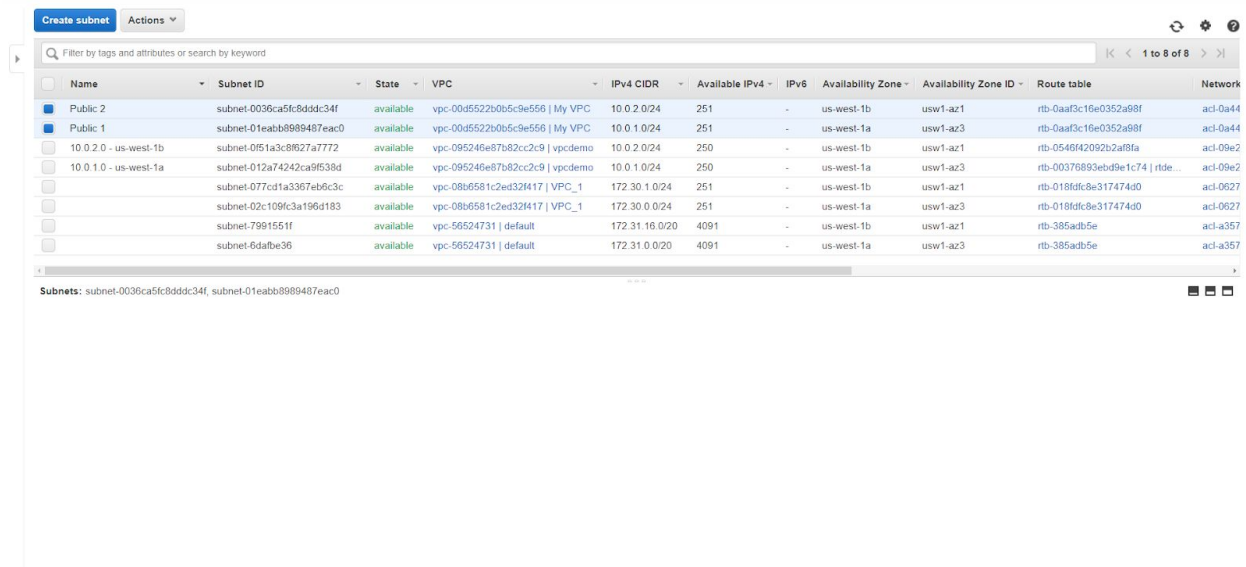
Auto-assign IPv4 ☒ Enable auto-assign public IPv4 address ?

* Required

[Cancel](#) [Save](#)

The second public subnet will also need auto-assigned IP addresses.

VPC - Subnets

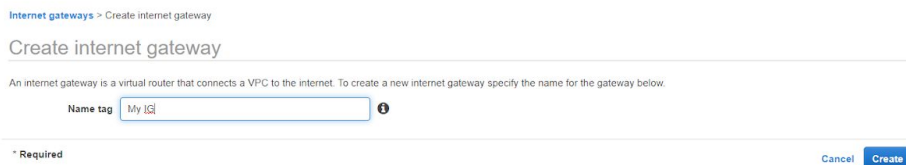


| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 | Availability Zone | Availability Zone ID | Route table | Network |
|-----------------------|--------------------------|-----------|---------------------------------|----------------|----------------|------|-------------------|----------------------|---------------------------------|----------|
| Public 2 | subnet-0036ca5fc8dddc34f | available | vpc-00d5522b0b5c9e556 My VPC | 10.0.2.0/24 | 251 | - | us-west-1b | usw1-az1 | rtb-0aaf3c16e0352a98f | acl-0a44 |
| Public 1 | subnet-01eabb8989487eac0 | available | vpc-00d5522b0b5c9e556 My VPC | 10.0.1.0/24 | 251 | - | us-west-1a | usw1-az3 | rtb-0aaf3c16e0352a98f | acl-0a44 |
| 10.0.2.0 - us-west-1b | subnet-0f51a3c8627a7772 | available | vpc-095246e87b62cc2c9 vpcdemo | 10.0.2.0/24 | 250 | - | us-west-1b | usw1-az1 | rtb-0546f42092b2af8fa | acl-09e2 |
| 10.0.1.0 - us-west-1a | subnet-012a74242ca9f538d | available | vpc-095246e87b62cc2c9 vpcdemo | 10.0.1.0/24 | 250 | - | us-west-1a | usw1-az3 | rtb-00376893ebd9e1c74 rtde... | acl-09e2 |
| | subnet-077cd1a3367eb6c3c | available | vpc-08b6581c2ed324417 VPC_1 | 172.30.1.0/24 | 251 | - | us-west-1b | usw1-az1 | rtb-018dfdc8e317474d0 | acl-0627 |
| | subnet-02c109fc3a196d183 | available | vpc-08b6581c2ed324417 VPC_1 | 172.30.0.0/24 | 251 | - | us-west-1a | usw1-az3 | rtb-018dfdc8e317474d0 | acl-0627 |
| | subnet-7991551f | available | vpc-56524731 default | 172.31.16.0/20 | 4091 | - | us-west-1b | usw1-az1 | rtb-385adb5e | acl-a357 |
| | subnet-6dafbe36 | available | vpc-56524731 default | 172.31.0.0/20 | 4091 | - | us-west-1a | usw1-az3 | rtb-385adb5e | acl-a357 |

Subnets: subnet-0036ca5fc8dddc34f, subnet-01eabb8989487eac0

Two public subnets within the “My VPC” VPC have been created.

Internet gateways - Create internet gateway



Internet gateways > Create internet gateway

Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag

* Required

Cancel Create

An Internet Gateway (IG) is required to provide a route table target for internet traffic and performs network address translation (NAT) for instances assigned IPv4 addresses.

VPC - Internet Gateways

| Name | ID | State | VPC | Owner |
|------------|----------------------|----------|---------------------|--------------|
| My IG | igw-059a249ffe61f... | detached | - | 758287676861 |
| igwdemo | igw-0cab531e67b... | attached | vpc-095246e87b8... | 758287676861 |
| igwVPC_1 | igw-0d062499a67... | attached | vpc-08b6581c2ed... | 758287676861 |
| igwdefault | igw-2e29224a | attached | vpc-56524731 d... | 758287676861 |

Note that “My IG” is detached and needs to be assigned a VPC.

VPC - Internet Gateways

Internet gateways > Attach to VPC

Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC: vpc-00d5522b0b5c9e55d

AWS Command Line

| VPC ID | Name |
|-----------------------|--------|
| vpc-00d5522b0b5c9e55d | My VPC |

* Required

Cancel Attach

Note that only one IG can be attached to a VPC at any given time. Thus, other VPC's are not available for attaching.

Route Tables - Create route table

[Route Tables](#) > Create route table

Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag ⓘ

VPC* ↕ ⓘ

* Required

[Cancel](#) [Create](#)

A route table will determine where network traffic is directed. A new one route table is created.

Route Tables - Edit routes

[Route Tables](#) > Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|-------------|-----------------------|--------|------------|
| 10.0.0.0/16 | local | active | No |
| 0.0.0.0/0 | igw-059a249ffe61ff04c | | No |

[Add route](#)

* Required

[Cancel](#) [Save routes](#)

The route for My IG is updated to route traffic from outside the network.

Route Tables - Edit subnet associations

[Route Tables](#) > Edit subnet associations

Edit subnet associations

Route table: rtb-024d574a4ee9a5389 (Public Route Table)

Associated subnets: [subnet-0036ca5fc8dddc34f](#) [subnet-01eabb8989487eac0](#)

Filter by attributes or search by keyword

< < 1 to 2 of 2 > >

| <input type="checkbox"/> | Subnet ID | IPv4 CIDR | IPv6 CIDR | Current Route Table |
|-------------------------------------|-------------------------------------|-------------|-----------|---------------------|
| <input checked="" type="checkbox"/> | subnet-01eabb8989487eac0 Public 1 | 10.0.1.0/24 | - | Main |
| <input checked="" type="checkbox"/> | subnet-0036ca5fc8dddc34f Public 2 | 10.0.2.0/24 | - | Main |

* Required

[Cancel](#) [Save](#)

For this lab, both subnets are associated with “Public Route Table”. This will allow both subnets to connect to the Internet via the “My IG” Internet Gateway.

VPC - Create security group

[VPC](#) / [Security groups](#) / Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: [Info](#)

Name cannot be edited after creation.

Description: [Info](#)

VPC: [Info](#)

Inbound rules

| Type | Protocol | Port range | Source | Description - optional | |
|------|----------|------------|--------|---|---------------------------------------|
| HTTP | TCP | 80 | Custom | <input type="text" value="Q..."/> <small>0.0.0.0/0</small> | <input type="button" value="Delete"/> |

Outbound rules

| Type | Protocol | Port range | Destination | Description - optional | |
|-------------|----------|------------|-------------|---|---------------------------------------|
| All traffic | All | All | Custom | <input type="text" value="Q..."/> <small>0.0.0.0/0</small> | <input type="button" value="Delete"/> |

A new security group for Web server access.

EC2 - Choose a AMI

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Q Search for an AMI by entering a search term e.g. "Windows"

Quick Start

My AMIs

AWS Marketplace

Community AMIs

☐ Free tier only (1)

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-06fcc10bc2c8943f

Amazon Linux 2018.03.0 (HVM), SSD Volume Type - ami-0d3ca10672b0e670

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-066d92ac6f03efca

SUSE Linux Enterprise Server 15 SP1 (HVM), SSD Volume Type - ami-02d732ce729636eb0

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0f56279347d2a43e

Are you launching a database instance? Try Amazon RDS.

Amazon RDS

Launch a database using RDS

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-00c3060e4c264a493

A EC2 instance will provide the basis for a web server that connects to Amazon RDS.

EC2 - Instance Type

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GB memory, EBS only)

| | Family | Type | vCPUs (1) | Memory (GiB) | Instance Storage (GiB) (1) | EBS Optimized Available (1) | Network Performance (1) | IPv6 Support (1) |
|-------------------------------------|-----------------|-------------|-----------|--------------|----------------------------|-----------------------------|-------------------------|------------------|
| <input type="checkbox"/> | General purpose | t2.nano | 1 | 0.5 | EBS only | - | Low to Moderate | Yes |
| <input checked="" type="checkbox"/> | General purpose | t2.micro | 1 | 1 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | General purpose | t2.small | 1 | 2 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | General purpose | t2.medium | 2 | 4 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | General purpose | t2.large | 2 | 8 | EBS only | - | Low to Moderate | Yes |
| <input type="checkbox"/> | General purpose | t2.xlarge | 4 | 16 | EBS only | - | Moderate | Yes |
| <input type="checkbox"/> | General purpose | t2.2xlarge | 8 | 32 | EBS only | - | Moderate | Yes |
| <input type="checkbox"/> | General purpose | t3a.nano | 2 | 0.5 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.micro | 2 | 1 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.small | 2 | 2 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.medium | 2 | 4 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.large | 2 | 8 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.xlarge | 4 | 16 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3a.2xlarge | 8 | 32 | EBS only | Yes | Up to 5 Gigabit | Yes |
| <input type="checkbox"/> | General purpose | t3.nano | 2 | 0.5 | EBS only | Yes | Up to 5 Gigabit | Yes |

Cancel Previous Review and Launch Next: Configure Instance Details

A t2.micro instance is selected.

EC2 - Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances (i) 1 Launch into Auto Scaling Group (i)

Purchasing option (i) ☐ Request Spot instances

Network (i) vpc-004522b065c5a556 | My VPC [Create new VPC](#)

Subnet (i) subnet-f1c4b46909487eac0 | Public 1 | us-west-1a [Create new subnet](#)

Auto-assign Public IP (i) ☐ Use subnet setting (Enable)

Placement group (i) ☐ Add instance to placement group

Capacity Reservation (i) Open [Create new Capacity Reservation](#)

IAM role (i) None [Create new IAM role](#)

Shutdown behavior (i) Stop

Stop - Hibernate behavior (i) ☐ Enable hibernation as an additional stop behavior

Enable termination protection (i) ☐ Protect against accidental termination

Monitoring (i) ☐ Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy (i) Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy

T2/T3 Unlimited (i) ☐ Enable
Additional charges may apply

File systems (i) [Add file systems](#) [Create new file system](#)

Network interfaces (i)

Advanced Details

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

The network selected is “My VPC”.

EC2 - Configure Instance Details

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Placement group (i) ☐ Add instance to placement group

Capacity Reservation (i) Open [Create new Capacity Reservation](#)

IAM role (i) None [Create new IAM role](#)

Shutdown behavior (i) Stop

Stop - Hibernate behavior (i) ☐ Enable hibernation as an additional stop behavior

Enable termination protection (i) ☐ Protect against accidental termination

Monitoring (i) ☐ Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy (i) Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy

T2/T3 Unlimited (i) ☐ Enable
Additional charges may apply

File systems (i) [Add file systems](#) [Create new file system](#)

Network interfaces (i)

Advanced Details

Metadata accessible (i) Enabled

Metadata version (i) V1 and V2 (token optional)

Metadata token response hop limit (i) 1

User data (i) ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#!bin/bash -ex
yum -y update
yum -y install httpd php mysql php-mysql
chkconfig httpd on
/etc/init.d/httpd start
cd /var/www/html
wget https://s3.us-west-2.amazonaws.com/us-west-2-govs-training/govus-gp1/gov-1-whenphpapp.jar
tar xvfz app.jar
chmod +x app.jar
cd /var/www/html
cd /var/www/html/ids.conf.php
```

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

The script provided in User data will install a web server on the EC2 instance and runs an app configured to point to Amazon RDS.

EC2 - Add Storage

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

| Volume Type (1) | Device (1) | Snapshot (1) | Size (GiB) (1) | Volume Type (1) | IOPS (1) | Throughput (MB/s) (1) | Delete on Termination (1) | Encryption (1) |
|-----------------|------------|------------------------|----------------|---------------------------|------------|-----------------------|-------------------------------------|----------------|
| Root | /dev/xvda | snap-00a5302a9e1c67d18 | 8 | General Purpose SSD (gp2) | 100 / 3000 | N/A | <input checked="" type="checkbox"/> | Not Encrypted |

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

CancelPreviousReview and LaunchNext: Add Tags

Default storage was selected.

EC2 - Add Tags

1. Choose AMI2. Choose Instance Type3. Configure Instance4. Add Storage5. Add Tags6. Configure Security Group7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

| Key (128 characters maximum) | Value (256 characters maximum) | Instances (1) | Volumes (1) |
|------------------------------|--------------------------------|-------------------------------------|-------------------------------------|
| Name | Web Server | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

Add another tag (Up to 50 tags maximum)

CancelPreviousReview and LaunchNext: Configure Security Group

Tags established for the EC2 instance.

EC2 - Configure Security Group

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

| Security Group ID | Name | Description | Actions |
|---|------------|------------------------------|-------------|
| <input type="checkbox"/> sg-0286085730c4d5657 | default | default VPC security group | Copy to new |
| <input checked="" type="checkbox"/> sg-04b7bc3629b0f799 | Web server | My Web Server Security Group | Copy to new |

Inbound rules for sg-04b7bc3629b0f799 (Selected security groups: sg-04b7bc3629b0f799)

| Type | Protocol | Port Range | Source | Description |
|------|----------|------------|-----------|-------------|
| HTTP | TCP | 80 | 0.0.0.0/0 | |

[Cancel](#) [Previous](#) [Review and Launch](#)

The preconfigured Web server security group is selected.

EC2 - Warning

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review


Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☐ Create a new security group ☒ Select an existing security group

| Security Group ID | Name | Description | Actions |
|---|------------|------------------------------|-------------|
| <input type="checkbox"/> sg-0286085730c4d5657 | default | default VPC security group | Copy to new |
| <input checked="" type="checkbox"/> sg-04b7bc3629b0f799 | Web server | My Web Server Security Group | Copy to new |

Warning

 **Warning**
You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

[Continue](#)

Inbound rules for sg-04b7bc3629b0f799 (Selected security groups: sg-04b7bc3629b0f799)

| Type | Protocol | Port Range | Source | Description |
|------|----------|------------|-----------|-------------|
| HTTP | TCP | 80 | 0.0.0.0/0 | |

[Cancel](#) [Previous](#) [Review and Launch](#)

This security warning is expected but okay for this lab as SSH will not be used to administrate.

EC2 - Review Instance Launch

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Free tier eligible Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0d3caf10672b8e870

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs Virtualization type: hvm

Instance Type

| Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GiB) | EBS-Optimized Available | Network Performance |
|---------------|----------|-------|--------------|------------------------|-------------------------|---------------------|
| t2.micro | Variable | 1 | 1 | EBS only | - | Low to Moderate |

Security Groups

| Security Group ID | Name | Description |
|---------------------|------------|------------------------------|
| sg-04b7bc3629b07f99 | Web server | My Web Server Security Group |

All selected security groups inbound rules

| Type | Protocol | Port Range | Source | Description |
|------|----------|------------|-----------|-------------|
| HTTP | TCP | 80 | 0.0.0.0/0 | |

Instance Details

Number of instances: 1

Network: vpc-00055220b05d9d556

Subnet: **subnet-01eab05989487eac0**

EBS-optimized: No

Monitoring: No

Termination protection: No

Shutdown behavior: Stop

Stop - Hibernate behavior: Disabled

Capacity Reservation: open

IAM role: None

Tenancy: default

Host ID: Not applicable

Host resource group name: Not applicable

Attestation: Not applicable

Kernel ID: Use default

RAM disk ID: Use default

Metadata accessible: Enabled

Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data: Not applicable

Assign Public IP: Use subnet setting (Enabled)

Assign IPv6 IP: Use subnet setting (Enabled)

Network interfaces: Not applicable

| Device | Network Interface | Subnet |
|--------|-----------------------|--------------------------|
| eth0 | New network interface | subnet-01eab05989487eac0 |

Storage

| Volume Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Throughput (MB/s) | Delete on Termination | Encrypted |
|-------------|-----------|------------------------|------------|-------------|------------|-------------------|-----------------------|---------------|
| Root | /dev/xvda | snap-00a5302a9e1c67d18 | 8 | gp2 | 100 / 3000 | N/A | Yes | Not Encrypted |

Tags

| Key | Value | Instances | Volumes |
|------|------------|--------------------------|--------------------------|
| Name | Web Server | <input type="checkbox"/> | <input type="checkbox"/> |

Cancel Previous **Launch**

The correct subnet has been set.

EC2 - Launch Instances

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Instance Details

Number of instances: 1

Network: vpc-00055220b05d9d556

Subnet: **subnet-01eab05989487eac0**

EBS-optimized: No

Monitoring: No

Termination protection: No

Shutdown behavior: Stop

Stop - Hibernate behavior: Disabled

Capacity Reservation: open

IAM role: None

T2/T3 Unlimited: Disabled

Host ID: Not applicable

Host resource group name: Not applicable

Attestation: Not applicable

Kernel ID: Use default

RAM disk ID: Use default

Metadata accessible: Enabled

Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data: Not applicable

Assign Public IP: Use subnet setting (Enabled)

Assign IPv6 IP: Use subnet setting (Enabled)

Network interfaces: Not applicable

| Device | Network Interface | Subnet |
|--------|-----------------------|--------------------------|
| eth0 | New network interface | subnet-01eab05989487eac0 |

Storage

| Volume Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Throughput (MB/s) | Delete on Termination | Encrypted |
|-------------|-----------|------------------------|------------|-------------|------------|-------------------|-----------------------|---------------|
| Root | /dev/xvda | snap-00a5302a9e1c67d18 | 8 | gp2 | 100 / 3000 | N/A | Yes | Not Encrypted |

Tags

| Key | Value | Instances | Volumes |
|------|------------|--------------------------|--------------------------|
| Name | Web Server | <input type="checkbox"/> | <input type="checkbox"/> |

Cancel Previous **Launch**

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key** file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel **Launch Instances**

Proceeding without a key pair is okay for this lab.

EC2 Dashboard

The screenshot shows the AWS Management Console EC2 Dashboard. At the top, there's a table listing instances. Below it, the details for the selected instance 'Web Server' (i-074b2c0a9f19ee042) are displayed. The instance is running in the us-west-1a availability zone, using the t2.micro instance type. It has a public IPv4 address of 54.183.211.18. The details are organized into sections: Description, Status Checks, Monitoring, and Tags.

| Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public | IPv4 Public IP | IPv6 | Key Name | Monitoring | Launch Time | Security Groups | Owner |
|-----------------|---------------------|---------------|-------------------|----------------|---------------|--------------|--------|----------------|------|------------|------------|--------------------------------|-----------------|--------------|
| Web Server | i-074b2c0a9f19ee042 | t2.micro | us-west-1a | running | Intializing | None | Yes | 54.183.211.18 | - | - | disabled | May 23, 2020 at 1:41:04 PM ... | Web server | 758287676661 |
| EC2 Private ... | i-06b33ae3d0115132 | t2.micro | us-west-1b | stopped | - | None | - | - | - | vpc-igdemo | disabled | May 22, 2020 at 7:51:36 PM ... | vpc-igdemo2 | 758287676661 |
| EC2 Public S... | i-0e58bca702e0f5ea | t2.micro | us-west-1a | stopped | - | None | - | - | - | vpc-igdemo | disabled | May 22, 2020 at 7:42:29 PM ... | vpc-igdemo | 758287676661 |

Instance: i-074b2c0a9f19ee042 (Web Server) Public IP: 54.183.211.18

Description

- Instance ID: i-074b2c0a9f19ee042
- Instance state: running
- Instance type: t2.micro
- Findings: Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)
- Private DNS: ip-10-0-1-208.us-west-1.compute.internal
- Private IPs: 10.0.1.208
- Secondary private IPs: -
- VPC ID: vpc-00d552b0e5c3e556 (My VPC)
- Subnet ID: subnet-01eab89994d7ead0 (Public 1)
- Network interfaces: eni0
- SourceDest check: True
- T2/T3 Unlimited: Disabled
- EBS-optimized: False
- Root device type: ebs
- Root device: /dev/xvda
- Block devices: /dev/xvda
- Capacity Reservation: -
- Capacity Reservation Settings: Open
- Outpost Arm: -

Status Checks

- Public DNS (IPv4): -
- IPv4 Public IP: 54.183.211.18
- IPv6 IPs: -
- Elastic IPs: -
- Availability zone: us-west-1a
- Security groups: Web server, view inbound rules, view outbound rules
- Scheduled events: No scheduled events
- AMI ID: amzn-ami-hvm-2018.03.0.20200514.0-885_64-g2 (ami-0d3caf10672b8870)
- Platform: -
- AMI role: -
- Key pair name: -
- Owner: 758287676661
- Launch time: May 23, 2020 at 1:41:04 PM UTC-7 (less than one hour)
- Termination protection: False
- Lifecycle: normal
- Monitoring: basic
- Alarm status: None
- Kernel ID: -
- RAM disk ID: -
- Placement group: -
- Partition number: -
- Virtualization: hvm
- Reservation: i-0d9526b0cc1e9a31
- AMI launch index: 0
- Tenancy: default

An IPv4 public IP has been assigned.

Chrome Browser - Web server

The screenshot shows a web browser window with the address bar displaying '54.183.211.18'. The page content includes the AWS logo and a form with the following fields:

- Endpoint:
- Database:
- Username:
- Password:
- Submit:

The public facing subnet attached web server is ready for the Amazon RDS endpoint.

Subnets - Create subnet

[Subnets](#) > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

| Name tag | Private 1 | ? | | | | | | |
|-------------------|---|---------------|------|--------|---------------|-------------|------------|--|
| VPC* | vpc-00d5522b0b6c9e556 | ? | | | | | | |
| Availability Zone | us-west-1a | ? | | | | | | |
| VPC CIDRs | <table><thead><tr><th>CIDR</th><th>Status</th><th>Status Reason</th></tr></thead><tbody><tr><td>10.0.0.0/16</td><td>associated</td><td></td></tr></tbody></table> | | CIDR | Status | Status Reason | 10.0.0.0/16 | associated | |
| CIDR | Status | Status Reason | | | | | | |
| 10.0.0.0/16 | associated | | | | | | | |
| IPv4 CIDR block* | 10.0.3.0/24 | ? | | | | | | |

* Required

[Cancel](#) [Create](#)

A private subnet that will be used for the backend web server.

Subnets - Create subnet

[Subnets](#) > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

| Name tag | Private 2 | ? | | | | | | |
|-------------------|---|---------------|------|--------|---------------|-------------|------------|--|
| VPC* | vpc-00d5522b0b6c9e556 | ? | | | | | | |
| Availability Zone | us-west-1b | ? | | | | | | |
| VPC CIDRs | <table><thead><tr><th>CIDR</th><th>Status</th><th>Status Reason</th></tr></thead><tbody><tr><td>10.0.0.0/16</td><td>associated</td><td></td></tr></tbody></table> | | CIDR | Status | Status Reason | 10.0.0.0/16 | associated | |
| CIDR | Status | Status Reason | | | | | | |
| 10.0.0.0/16 | associated | | | | | | | |
| IPv4 CIDR block* | 10.0.4.0/24 | ? | | | | | | |

* Required

[Cancel](#) [Create](#)

The second and final private subnet.

VPC - Subnets

| Create subnet Actions | | | | | | | | | | | | |
|--|--------------------------|-----------|---------------------------------|----------------|----------------|------|-------------------|----------------------|---------------------------------|-----------------------|----------------|-------------|
| Filter by tags and attributes or search by keyword | | | | | | | | | | | | |
| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 | Availability Zone | Availability Zone ID | Route table | Network ACL | Default subnet | Auto-assign |
| Public 2 | subnet-0036ca5c8dddc34f | available | vpc-00e5522b0b5c9e556 My VPC | 10.0.2.0/24 | 251 | - | us-west-1b | usw1-az1 | rtb-024d574a4ee9a5389 Publ... | acl-0a44baaa0dec2a29 | No | Yes |
| Public 1 | subnet-01eabb989487eac0 | available | vpc-00e5522b0b5c9e556 My VPC | 10.0.1.0/24 | 250 | - | us-west-1a | usw1-az3 | rtb-024d574a4ee9a5389 Publ... | acl-0a44baaa0dec2a29 | No | Yes |
| Private 2 | subnet-020fce916aa5731b4 | available | vpc-00e5522b0b5c9e556 My VPC | 10.0.4.0/24 | 251 | - | us-west-1b | usw1-az1 | rtb-0aa03c16e0352a98f | acl-0a44baaa0dec2a29 | No | No |
| Private 1 | subnet-0a0b667f05498a670 | available | vpc-00e5522b0b5c9e556 My VPC | 10.0.3.0/24 | 251 | - | us-west-1a | usw1-az3 | rtb-0aa03c16e0352a98f | acl-0a44baaa0dec2a29 | No | No |
| 10.0.2.0 - us-west-1b | subnet-0f51a3cd8627a7772 | available | vpc-095246a87b82cc2c9 vpcdemo | 10.0.2.0/24 | 250 | - | us-west-1b | usw1-az1 | rtb-0546042692b2a08fa | acl-09a23e26a421217ac | No | No |
| 10.0.1.0 - us-west-1a | subnet-012a74242ca9f538d | available | vpc-095246a87b82cc2c9 vpcdemo | 10.0.1.0/24 | 250 | - | us-west-1a | usw1-az3 | rtb-00376893bdf9c74 nde... | acl-09a23e26a421217ac | No | Yes |
| | subnet-077cd1a3367eb6c3c | available | vpc-08b6681c2ed324117 VPC_1 | 172.30.1.0/24 | 251 | - | us-west-1b | usw1-az1 | rtb-0188dc0a317474d0 | acl-06273233a36b1dc04 | No | Yes |
| | subnet-02c109fc3a196d183 | available | vpc-08b6681c2ed324117 VPC_1 | 172.30.0.0/24 | 251 | - | us-west-1a | usw1-az3 | rtb-0188dc0a317474d0 | acl-06273233a36b1dc04 | No | Yes |
| | subnet-7991551f | available | vpc-56524731 default | 172.31.16.0/20 | 4091 | - | us-west-1b | usw1-az1 | rtb-305adb5e | acl-a3570c5 | Yes | Yes |
| | subnet-6dafbc36 | available | vpc-56524731 default | 172.31.0.0/20 | 4091 | - | us-west-1a | usw1-az3 | rtb-305adb5e | acl-a3570c5 | Yes | Yes |

Subnets: subnet-0a0b667f05498a670, subnet-020fce916aa5731b4

Both private subnets have been created.

Security Groups - Create security group

Create security group info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name info

Database

Name cannot be edited after creation.

Description info

My Database Security Group

VPC info

vpc-00e5522b0b5c9e556 (My VPC)

Inbound rules

This security group has no inbound rules.

Add rule

Outbound rules

Type info

Protocol info

Port range info

Destination info

Description - optional info

Delete

All traffic

All

All

Custom

0.0.0.0/0

Add rule

Cancel Create security group

A new security group will allow MySQL traffic from the web server.

VPC - Edit inbound rules

VPC > Security Groups > sg-075a5772c10316ce - Database > Edit inbound rules

Edit inbound rules [info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [info](#)

Type [info](#)

Protocol [info](#)

Port range [info](#)

Source [info](#)

Description - optional [info](#)

MySQL/Aurora

TCP

3306

Custom

Q

Delete

Add rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause a brief interruption of traffic for a very brief period of time until the new rule can be created.

Cancel

Preview changes

Save rules

CIDR blocks

0.0.0.0/0

0.0.0.0/8

0.0.0.0/16

0.0.0.0/24

0.0.0.0/32

:/0

:/16

:/32

:/48

:/64

Security Groups

default | sg-0286085730c4d5657

Web server | sg-04b78c36f29b0f799

Database | sg-075a5772c10316ce

Prefix lists

com.amazonaws.us-west-2 | pl-6ba54002

com.amazonaws.us-west-2 | pl-6ba54007

This will allow the web server (as per defined by the security group) to communicate to the database.

Amazon RDS - Create DB subnet

Amazon RDS

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet details

Name
You won't be able to modify the name after your subnet group has been created.
My Subnet Group

Description
My Subnet Group

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.
My VPC (vpc-b0a5522b065c9c556)

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.
Choose an availability zone

us-west-1a X us-west-1b X

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.
Select subnets

subnet-daf966705498a670 (10.0.1.0/24) X
subnet-020fce916aas731b4 (10.0.4.0/24) X

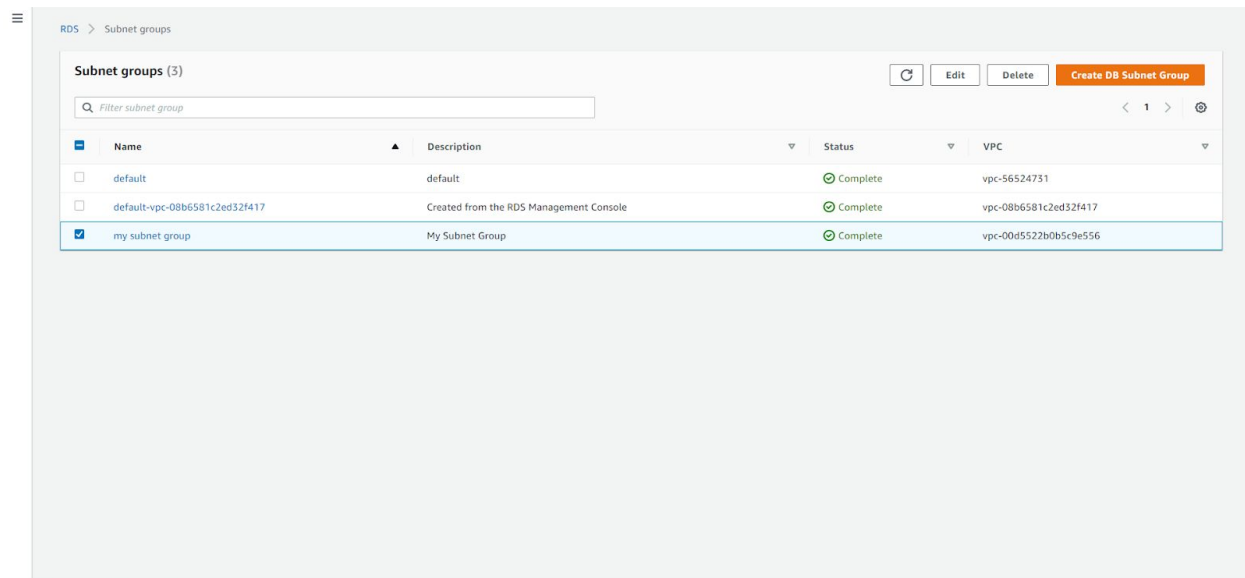
Subnets selected (2)

| Availability zone | Subnet ID | CIDR block |
|-------------------|--------------------------|-------------|
| us-west-1a | subnet-daf966705498a670 | 10.0.1.0/24 |
| us-west-1b | subnet-020fce916aas731b4 | 10.0.4.0/24 |

Cancel Create

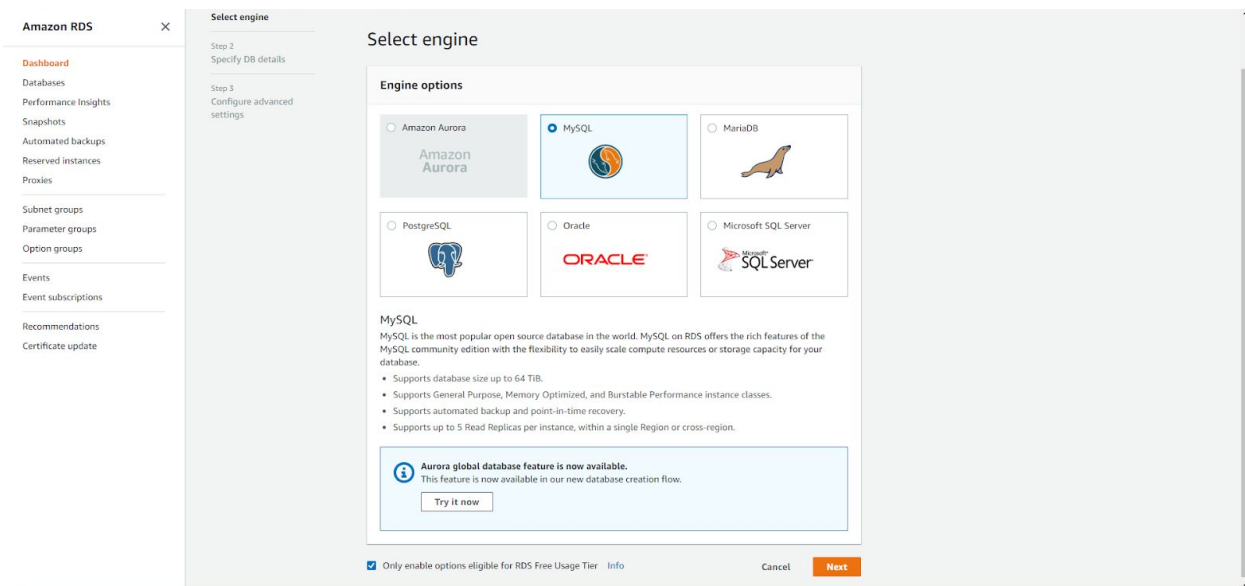
A DB subnet group is required for the Amazon RDS instances to work. Note that two AZ's are selected and required.

RDS - Subnet groups



The subnet group for RDS is created.

Amazon RDS - Select engine



Setting up the database instance as a MySQL engine type.

Amazon RDS - Specify DB details

Amazon RDS

Switch to the new database creation flow.

Share your feedback

Step 1: Select engine

Step 2: Specify DB details

Step 3: Configure advanced settings

Specify DB details

Instance specifications

Estimate your monthly costs for the DB instance using the [AWS Simple Monthly Calculator](#).

DB engine: MySQL Community Edition

License model: [Info](#)
general-public-license

DB engine version: [Info](#)
MySQL 5.7.26

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

Free tier
The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GiB of storage, allowing new AWS customers to gain hands-on experience with Amazon RDS. Learn more about the RDS Free Tier and the instance restrictions here.
☒ Only enable options eligible for RDS Free Usage Tier [Info](#)

DB instance class: [Info](#)
db.t2.micro — 1 vCPU, 1 GiB RAM

Multi-AZ deployment: [Info](#)
☒ Create replica in a different zone
Creates a replica in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freeze, and minimize latency during system backups.
☐ No

Storage type: [Info](#)

The Amazon RDS instance will be a t2.micro type.

Amazon RDS - Configure advanced settings

Amazon RDS

Switch to the new database creation flow.

Share your feedback

Step 1: Select engine

Step 2: Specify DB details

Step 3: Configure advanced settings

Configure advanced settings

Network & Security

Virtual Private Cloud (VPC): [Info](#)
VPC defines the virtual networking environment for this DB instance.
My VPC (vpc-00d522b0b5c9e556) [Info](#)

Only VPCs with a corresponding DB subnet group are listed.

Subnet group: [Info](#)
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.
my subnet group

Public accessibility: [Info](#)
☐ Yes
EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.
☒ No
DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.

Availability zone: [Info](#)
No preference

VPC security groups
Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.
☐ Create new VPC security group
☒ Choose existing VPC security groups
Choose VPC security groups

Database options

Database name: [Info](#)
myDB

The DB instance is assigned the “My VPC” VPC, “my subnet group” subnet group, and the “Database” security group. All of which have been created in the lab.

Amazon RDS - myDB

The screenshot shows the Amazon RDS console for an instance named 'mydb'. The instance is in the 'Available' state. The summary table shows the following details:

| DB identifier | CPU | Info | Class |
|---------------|------------------|-----------------|-------------|
| mydb | - | Available | db.t2.micro |
| Role | Current activity | Engine | Region & AZ |
| Instance | | MySQL Community | us-west-1a |

The 'Connectivity & security' tab is selected, showing the following details:

| Endpoint & port | Networking | Security |
|---|--|---|
| Endpoint: mydb.c0ps0y5roh4c.us-west-1.rds.amazonaws.com Port: 3306 | Availability zone: us-west-1a VPC: My VPC (vpc-00d5522b0b5c9e556) Subnet group: my-subnet-group Subnets: subnet-0a8b667f05498a670, subnet-020fce916aa5731b4 | VPC security groups: Database (sg-075a5772cf10316ce) (active) Public accessibility: No Certificate authority: rds-ca-2019 Certificate authority date: Aug 22nd, 2024 |

Below the connectivity details, there is a section for 'Security group rules (2)' with a search bar and a table with columns for Security group, Type, and Rule.

The Amazon RDS instance is now running, to connect to it the endpoint must be copied.

Google Chrome

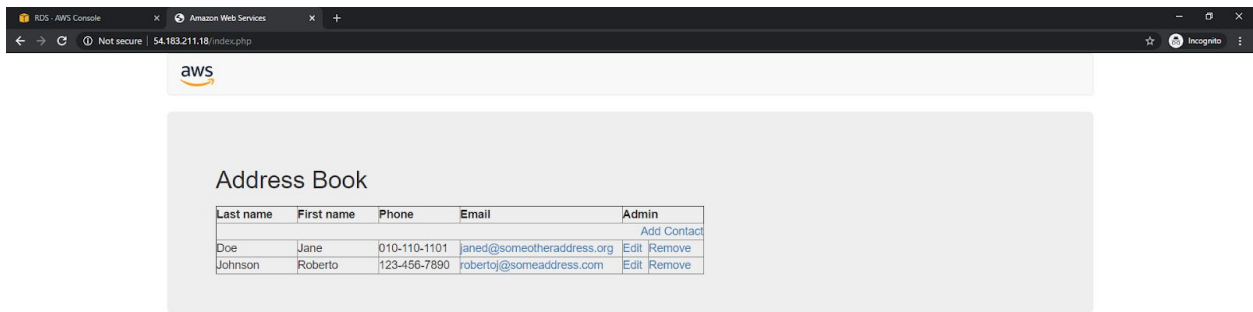
The screenshot shows a web browser window with the AWS logo at the top. Below the logo is a form for connecting to an RDS instance. The form contains the following fields:

- Endpoint: mydb.c0ps0y5roh4c.us-west-1.rds.amazonaws.com
- Database: mydb
- Username: admin
- Password: (masked with dots)

A 'Submit' button is located at the bottom of the form.

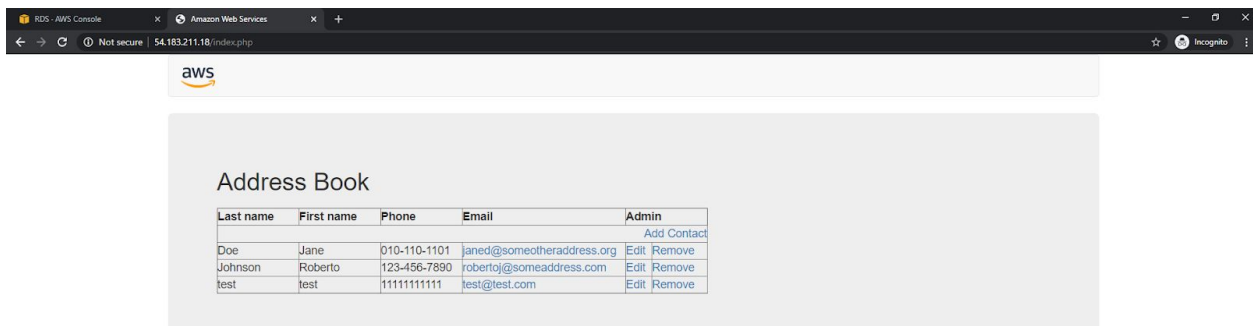
The RDS endpoint and credentials applied to the web server EC2 instance.

Google Chrome



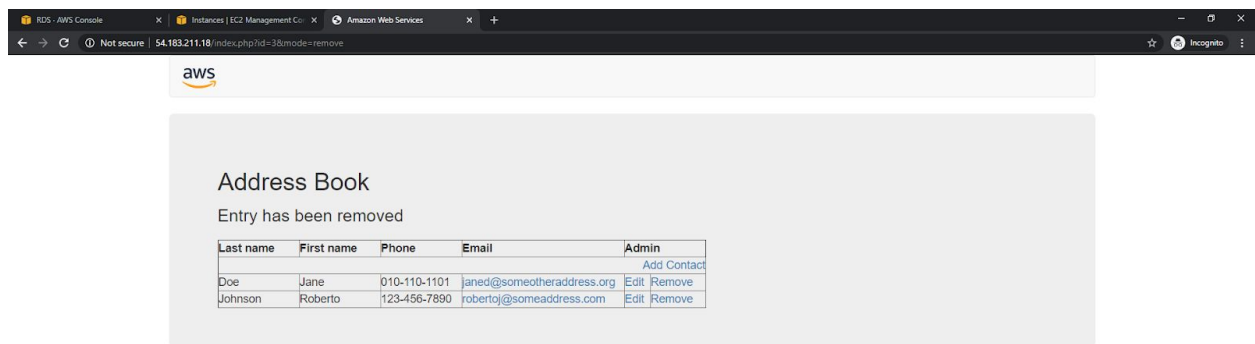
A successful connection to the Amazon RDS endpoint has been established.

Google Chrome



A test entry has been submitted and saved.

Google Chrome



The test entry has been successfully removed.