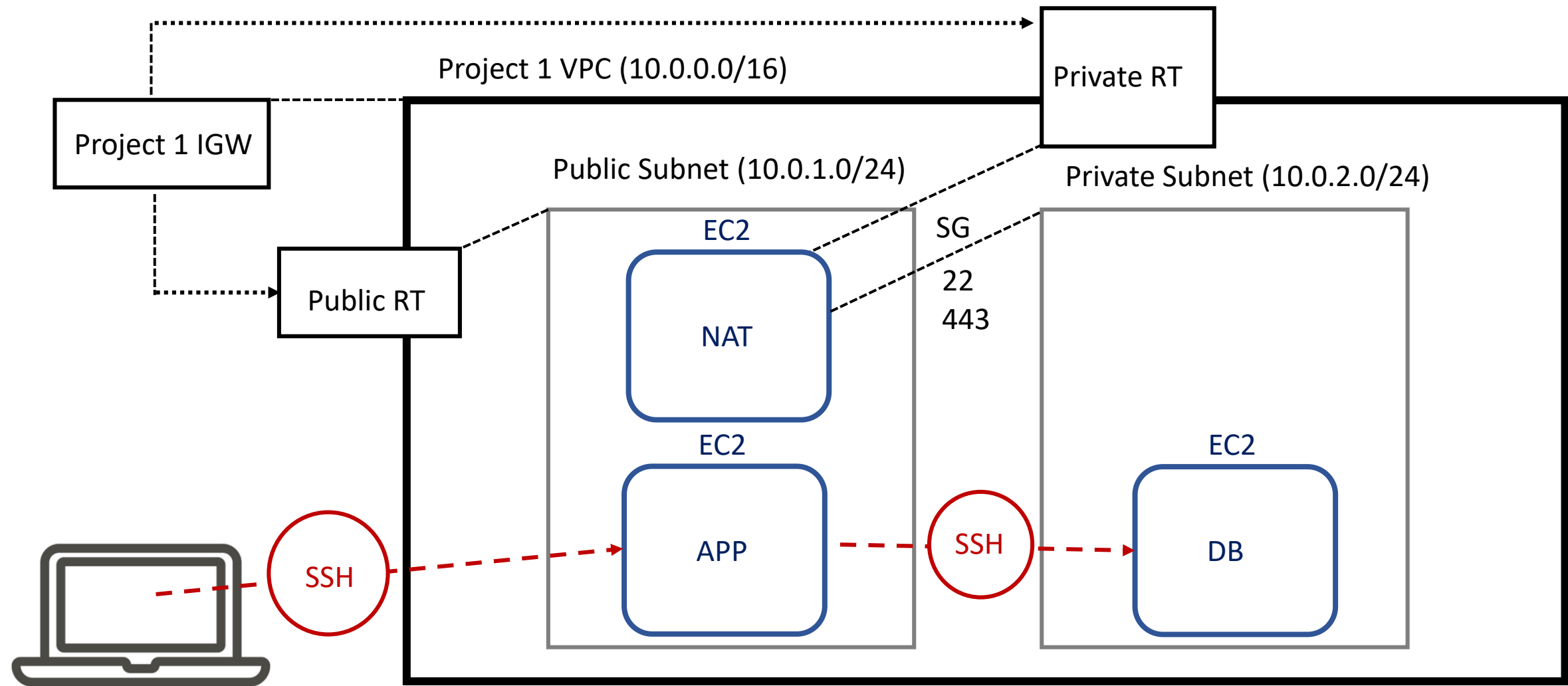



ARCHITECTURE




1) Create the custom VPC and enable DNS hostname



Services ▾

Resource Groups ▾

★

 vocstartsoft/user859235=dieg... ▾

N. Virginia ▾

Support ▾


[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

Project 1 VPC



IPv4 CIDR block*

10.0.0.0/16




IPv6 CIDR block

☒ No IPv6 CIDR Block


☐ Amazon provided IPv6 CIDR block

☐ IPv6 CIDR owned by me



Tenancy

Default



* Required

Cancel

Create

1) Create the custom VPC and enable DNS hostname

aws

Services

Resource Groups

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Create VPC

Actions

Filter by tags and attributes or search by keyword

<<

<

1 to 2 of 2

>

>>

| | Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | IPv6 CIDR (Network Border Group) | DHCP options set | Main Route table | Main Network ACL |
|-------------------------------------|---------------|-----------------------|-----------|---------------|-----------|----------------------------------|------------------|-----------------------|-----------------------|
| <input type="checkbox"/> | | vpc-a915fed4 | available | 172.31.0.0/16 | - | - | dopt-9a42d6e0 | rtb-679deb19 | acl-46d5873b |
| <input checked="" type="checkbox"/> | Project 1 VPC | vpc-01c777ccc03c4dc61 | available | 10.0.0.0/16 | - | - | dopt-9a42d6e0 | rtb-0a05ec85a0cea06c9 | acl-02cafd27eed166123 |

VPC: vpc-01c777ccc03c4dc61

Description

CIDR Blocks

Flow Logs

Tags

VPC ID

State

IPv4 CIDR

IPv6 CIDR

IPv6 Pool

Network ACL

DHCP options set

Route table

vpc-01c777ccc03c4dc61

available

10.0.0.0/16

-

-

acl-02cafd27eed166123

dopt-9a42d6e0

rtb-0a05ec85a0cea06c9

Tenancy

Default VPC

Classic link

IPv6 CIDR (Network Border Group)

DNS resolution

DNS hostnames

ClassicLink DNS Support

Owner

default

No

Disabled

-

Enabled

Disabled

Disabled

280157415142

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

1) Create the custom VPC and enable DNS hostname



The screenshot displays the AWS Management Console's VPC Dashboard. On the left, there's a navigation sidebar with categories like 'VIRTUAL PRIVATE CLOUD' (containing 'Your VPCs', Subnets, Route Tables, etc.) and 'SECURITY'. The main area shows a table of VPCs with columns for Name, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Main Route table, and Main Network ACL. A context menu is open over the first VPC, offering actions like 'Delete VPC', 'Edit CIDRs', and 'Add/Edit Tags'. Below the table, the details for VPC 'vpc-01c777ccc03c4dc61' are shown under the 'Description' tab, listing various configuration parameters.


| Name | State | IPv4 CIDR | IPv6 CIDR | IPv6 CIDR (Network Border Group) | DHCP options set | Main Route table | Main Network ACL |
|---------|-----------|---------------|-----------|----------------------------------|------------------|-----------------------|-----------------------|
| Project | available | 172.31.0.0/16 | - | - | dopt-9a42d6e0 | rtb-679deb19 | acl-46d5873b |
| | available | 10.0.0.0/16 | - | - | dopt-9a42d6e0 | rtb-0a05ec85a0cea06c9 | acl-02cafd27eed166123 |

VPC: vpc-01c777ccc03c4dc61

| Description | | CIDR Blocks | | Flow Logs | | Tags | |
|-------------------------|-----------------------|--------------------|-----------------------|---|--------------|--------------------------------|----------|
| VPC ID | vpc-01c777ccc03c4dc61 | Tenancy | default | Default VPC | No | Classic link | Disabled |
| State | available | IPv4 CIDR | 10.0.0.0/16 | IPv6 CIDR (Network Border Group) | - | DNS resolution | Enabled |
| IPv4 CIDR | 10.0.0.0/16 | IPv6 Pool | - | DNS hostnames | Disabled | ClassicLink DNS Support | Disabled |
| IPv6 CIDR | - | Network ACL | acl-02cafd27eed166123 | Owner | 280157415142 | | |
| DHCP options set | dopt-9a42d6e0 | Route table | rtb-0a05ec85a0cea06c9 | | | | |

1) Create the custom VPC and enable DNS hostname

 Services ▾ Resource Groups ▾ 

 vocstartsoft/user859235=diag... ▾ N. Virginia ▾ Support ▾

[VPCs](#) > Edit DNS hostnames



Edit DNS hostnames

VPC ID vpc-01c777ccc03c4dc61

DNS hostnames ☒ enable

* Required

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

 Feedback  English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

2) Create the public and private subnet in the custom VPC

aws

Services ▾Resource Groups ▾★

vocstartsoft/user859235=dieg... ▾N. Virginia ▾Support ▾

[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 Subnet

VPC*

vpc-01c777ccc03c4dc61

Availability Zone

No preference

VPC CIDRs

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

IPv4 CIDR block*

10.0.1.0/24

* Required

Cancel

Create

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

2) Create the public and private subnet in the custom VPC

aws

Services ▾Resource Groups ▾★

vocstartsoft/user859235=dieg... ▾N. Virginia ▾Support ▾

[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 Subnet

VPC*

vpc-01c777ccc03c4dc61

Availability Zone

No preference

VPC CIDRs

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

IPv4 CIDR block*

10.0.2.0/24

* Required

Cancel

Create

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

2) Create the public and private subnet in the custom VPC

New VPC Experience
[Learn more](#)

VPC Dashboard

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- Carrier Gateways
- DHCP Options Sets
- Elastic IPs
- Managed Prefix Lists
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Create subnetActions

Filter by tags and attributes or search by keyword

| Name | Subnet ID | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 CIDR | Availability Zone | Availability Zone ID | Network Border Group | Route table |
|----------------|--------------------------|-----------|-----------------------------|----------------|----------------|-----------|-------------------|----------------------|----------------------|-----------------------|
| Public Subnet | subnet-06104cc3bacff4a82 | available | vpc-01c777ccc03c4dc61 ... | 10.0.1.0/24 | 251 | - | us-east-1f | use1-az5 | us-east-1 | rtb-0a05ec85a0cea06c9 |
| Private Subnet | subnet-076db1b17b707b636 | available | vpc-01c777ccc03c4dc61 ... | 10.0.2.0/24 | 251 | - | us-east-1f | use1-az5 | us-east-1 | rtb-0a05ec85a0cea06c9 |
| | subnet-555d8233 | available | vpc-a915fed4 | 172.31.0.0/20 | 4091 | - | us-east-1d | use1-az1 | us-east-1 | rtb-679det |
| | subnet-0e8d282f | available | vpc-a915fed4 | 172.31.80.0/20 | 4091 | - | us-east-1a | use1-az2 | us-east-1 | rtb-679det |
| | subnet-db6e0096 | available | vpc-a915fed4 | 172.31.16.0/20 | 4091 | - | us-east-1b | use1-az4 | us-east-1 | rtb-679det |
| | subnet-25f0602b | available | vpc-a915fed4 | 172.31.64.0/20 | 4091 | - | us-east-1f | use1-az5 | us-east-1 | rtb-679det |
| | subnet-0024c631 | available | vpc-a915fed4 | 172.31.48.0/20 | 4091 | - | us-east-1e | use1-az3 | us-east-1 | rtb-679det |
| | subnet-f5a873aa | available | vpc-a915fed4 | 172.31.32.0/20 | 4091 | - | us-east-1c | use1-az6 | us-east-1 | rtb-679det |

Subnet: subnet-06104cc3bacff4a82

DescriptionFlow LogsRoute TableNetwork ACLTagsSharing

Subnet ID

subnet-06104cc3bacff4a82

VPC

vpc-01c777ccc03c4dc61 | Project 1 VPC

Available IPv4 Addresses

251

Availability Zone

us-east-1f (use1-az5)

Route Table

rtb-0a05ec85a0cea06c9

Default subnet

No

Auto-assign customer-owned IPv4 address

No

Auto-assign IPv6 address

No

Owner

280157415142

State

available

IPv4 CIDR

10.0.1.0/24

IPv6 CIDR

-

Network Border Group

us-east-1

Network ACL

acl-02cafd27eed166123

Auto-assign public IPv4 address

No

Customer-owned IPv4 pool

-

Outpost ID

-

3) Turn on “Auto Assign Public IPv4 address for the public subnet”

New VPC Experience
[Learn more](#)

VPC Dashboard

Filter by VPC:
Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Create subnet

Actions

Filter by tags

| Name | State | VPC | IPv4 CIDR | Available IPv4 | IPv6 CIDR | Availability Zone | Availability Zone ID | Network Border Group | Route table |
|-----------------|-----------|---------------------------------------|----------------|----------------|-----------|-------------------|----------------------|----------------------|-----------------------|
| Public Subnet | available | vpc-01c777ccc03c4dc61 Project 1 VPC | 10.0.1.0/24 | 251 | - | us-east-1f | use1-az5 | us-east-1 | rtb-0a05ec85a0cea06c9 |
| Private Subnet | available | vpc-01c777ccc03c4dc61 Project 1 VPC | 10.0.2.0/24 | 251 | - | us-east-1f | use1-az5 | us-east-1 | rtb-0a05ec85a0cea06c9 |
| | available | vpc-a915fed4 | 172.31.0.0/20 | 4091 | - | us-east-1d | use1-az1 | us-east-1 | rtb-679det |
| | available | vpc-a915fed4 | 172.31.80.0/20 | 4091 | - | us-east-1a | use1-az2 | us-east-1 | rtb-679det |
| subnet-db6e0096 | available | vpc-a915fed4 | 172.31.16.0/20 | 4091 | - | us-east-1b | use1-az4 | us-east-1 | rtb-679det |
| subnet-25f0602b | available | vpc-a915fed4 | 172.31.64.0/20 | 4091 | - | us-east-1f | use1-az5 | us-east-1 | rtb-679det |
| subnet-0024c631 | available | vpc-a915fed4 | 172.31.48.0/20 | 4091 | - | us-east-1e | use1-az3 | us-east-1 | rtb-679det |
| subnet-f5a873aa | available | vpc-a915fed4 | 172.31.32.0/20 | 4091 | - | us-east-1c | use1-az6 | us-east-1 | rtb-679det |

Subnet: subnet-06104cc3bacff4a82

Description

Flow Logs

Route Table

Network ACL

Tags

Sharing

Subnet ID

subnet-06104cc3bacff4a82

State

available

VPC

vpc-01c777ccc03c4dc61 | Project 1 VPC

IPv4 CIDR

10.0.1.0/24

Available IPv4 Addresses

251

IPv6 CIDR

-

Availability Zone

us-east-1f (use1-az5)

Network Border Group

us-east-1

Route Table

rtb-0a05ec85a0cea06c9

Network ACL

acl-02cafd2eed166123

Default subnet

No

Auto-assign customer-owned IPv4 address

No

Customer-owned IPv4 pool

-

Auto-assign IPv6 address

No



Outpost ID


-

Owner

280157415142

3) Turn on “Auto Assign Public IPv4 address for the public subnet”

 Services ▾ Resource Groups ▾ 

 vocstartsoft/user859235=dieg... ▾ N. Virginia ▾ Support ▾


[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-06104cc3bacff4a82

Auto-assign IPv4 ☒



Enable auto-assign public IPv4 address 

Auto-assign Co-IP ☐

Enable auto-assign customer-owned IPv4 address 

* Required

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

 Feedback  English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

4) Create the Internet Gateway and attach it to the custom VPC

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

VPC

Internet gateways

Create internet gateway

Create internet gateway

Info

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.

Internet gateway settings

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Project 1 IGW

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

Q Name X

Q Project 1 IGW X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4) Create the Internet Gateway and attach it to the custom VPC

aws

Services

Resource Groups

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway

The following internet gateway was created: igw-049fb6d99d61eb5a1 . You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC > Internet gateways

Internet gateways (1/2)

Info

Refresh

Actions

Create internet gateway

Filter internet gateways

< 1 > Settings

| | Name | Internet gateway ID | State | VPC ID | Owner |
|-------------------------------------|---------------|-----------------------|----------|--------------|--------------|
| <input checked="" type="checkbox"/> | Project 1 IGW | igw-049fb6d99d61eb5a1 | Detached | - | 280157415142 |
| <input type="checkbox"/> | - | igw-d4bce2af | Attached | vpc-a915fed4 | 280157415142 |

igw-049fb6d99d61eb5a1 / Project 1 IGW

DetailsTags

Details

Internet gateway ID

igw-049fb6d99d61eb5a1

State

Detached

VPC ID

-

Owner

280157415142

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4) Create the Internet Gateway and attach it to the custom VPC

aws

Services

Resource Groups

vocstartsoft/user859235=diag...

N. Virginia

Support

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway

The following internet gateway was created: igw-049fb6d99d61eb5a1 . You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC

VPC > Internet gateways

Internet gateways (1/2)

Info

Filter internet gateways

| | Name | Internet gateway ID | State | VPC ID | Owner |
|-------------------------------------|---------------|-----------------------|----------|--------------|--------------|
| <input checked="" type="checkbox"/> | Project 1 IGW | igw-049fb6d99d61eb5a1 | Detached | - | 280157415142 |
| <input type="checkbox"/> | - | igw-d4bce2af | Attached | vpc-a915fed4 | 280157415142 |

Actions

View details

Attach to VPC

Detach from VVC

Manage tags

Delete internet gateway

Create internet gateway

igw-049fb6d99d61eb5a1 / Project 1 IGW

Details

Tags

Details

| | | | |
|---|----------|--------|--|
| Internet gateway ID | State | VPC ID | Owner |
| <input checked="" type="checkbox"/> igw-049fb6d99d61eb5a1 | Detached | - | <input checked="" type="checkbox"/> 280157415142 |

Feedback

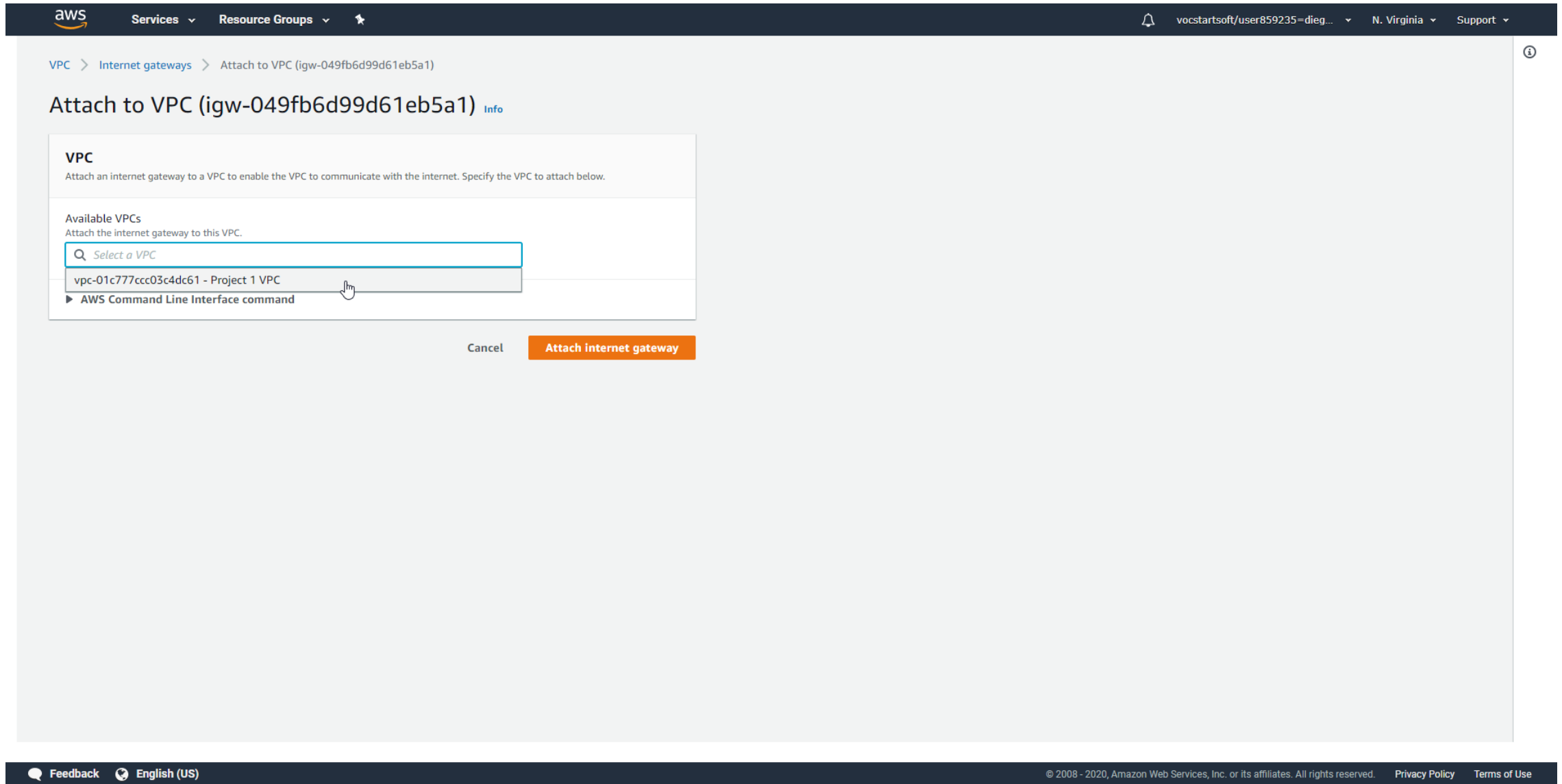
English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

4) Create the Internet Gateway and attach it to the custom VPC



4) Create the Internet Gateway and attach it to the custom VPC

Services

Resource Groups

🔔

vocstartsoft/user859235=diag...

N. Virginia

Support

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway

Internet gateway igw-049fb6d99d61eb5a1 successfully attached to vpc-01c777ccc03c4dc61

VPC > Internet gateways

Internet gateways (2)

Info

Filter internet gateways

Name

Internet gateway ID

State

VPC ID

Owner

Project 1 IGW

igw-049fb6d99d61eb5a1

Attached

vpc-01c777ccc03c4dc61 | Project 1 VPC

280157415142

-

igw-d4bce2af

Attached

vpc-a915fed4

280157415142


Select an internet gateway above


Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

5) Create the public route table and associate it with the public subnet

 Services ▾ Resource Groups ▾ ★


 vocstartsoft/user859235=dieg... ▾ N. Virginia ▾ Support ▾

[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

Public Route table 

VPC*

vpc-01c777ccc03c4dc61  

Key (128 characters maximum)

Value (256 characters maximum)


This resource currently has no tags



Add Tag

50 remaining (Up to 50 tags maximum)

* Required

Cancel

Create 

 Feedback  English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

[Privacy Policy](#)

[Terms of Use](#)

5) Create the public route table and associate it with the public subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

Route Tables

> Edit routes

Edit routes

| Destination | Target | Status | Propagated | |
|--|--|--------|------------|---|
| 10.0.0.0/16 | local | active | No | |
| <input type="text" value="0.0.0.0/0"/> | <input type="text" value="igw-049fb6d99d61eb5a1"/> | | No | ✕ |

Add route

igw-049fb6d99d61eb5a1

Project 1 IGW

* Required

Cancel

Save routes

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

5) Create the public route table and associate it with the public subnet

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Q

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Create route table

Actions

Filter by tags and attributes or search by keyword

<<

<

1 to 3 of 3

>

>>

| | Name | Route Table ID | Explicit subnet association | Edge associations | Main | VPC ID | Owner |
|-------------------------------------|----------------|-----------------------|-----------------------------|-------------------|------|----------------------------|--------------|
| <input checked="" type="checkbox"/> | Public Rout... | rtb-056c3e917489d5b3c | - | - | No | vpc-01c777ccc03c4dc61 ... | 280157415142 |
| <input type="checkbox"/> | | rtb-0a05ec85a0cea06c9 | - | - | Yes | vpc-01c777ccc03c4dc61 ... | 280157415142 |
| <input type="checkbox"/> | | rtb-679deb19 | - | - | Yes | vpc-a915fed4 | 280157415142 |

Route Table: rtb-056c3e917489d5b3c

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

Edit subnet associations

<<

<

None found

>

>>

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|-----------|-----------|-----------|
|-----------|-----------|-----------|

You do not have any subnet associations.

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

<<

<

1 to 2 of 2

>

>>

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|----------------------------|-------------|-----------|
| subnet-076db1b17b707b6... | 10.0.2.0/24 | - |
| subnet-06104cc3bacff4a8... | 10.0.1.0/24 | - |

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

5) Create the public route table and associate it with the public subnet

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

Route Tables

> Edit subnet associations

Edit subnet associations

Route table

rtb-056c3e917489d5b3c (Public Route table)

Associated subnets

subnet-06104cc3bacff4a82

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 type="checkbox"/> | subnet-076db1b17b707b636 Private S... | 10.0.2.0/24 | - | Main |
| <input checked="" type="checkbox"/> | subnet-06104cc3bacff4a82 Public Sub... | 10.0.1.0/24 | - | Main |

* Required

Cancel

Save

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

6) Navigate to EC2 and create the NAT instance in the public subnet

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

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)

Cancel and Exit

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 NAT

Search by Systems Manager parameter

Quick Start (0)

My AMIs (0)

AWS Marketplace (25)

Community AMIs (507)

Operating system

Architecture

Root device type

amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-ebs - ami-00a9d4a05375b2763

Amazon Linux AMI 2018.03.0.20181116 x86_64 VPC HVM ebs

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

amzn-ami-vpc-nat-hvm-2017.09.1.20180108-x86_64-ebs - ami-01623d7b

Amazon Linux AMI 2017.09.1.20180108 x86_64 VPC NAT HVM EBS

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

amzn-ami-vpc-nat-2018.03.0.20200716.0-x86_64-ebs - ami-01ef31f9f39c5aaed

Amazon Linux AMI 2018.03.0.20200716.0 x86_64 VPC HVM ebs

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

amzn-ami-vpc-nat-2018.03.0.20200514.0-x86_64-ebs - ami-02623b65d521fbd30

Amazon Linux AMI 2018.03.0.20200514.0 x86_64 VPC HVM ebs

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

amzn-ami-vpc-nat-2018.03.0.20190826-x86_64-ebs - ami-02cb555e324696ced

Amazon Linux AMI 2018.03.0.20190826 x86_64 VPC HVM ebs

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

amzn-ami-vpc-nat-2018.03.0.20200318.2-x86_64-ebs - ami-02f55863fb09f62b1

Amazon Linux AMI 2018.03.0.20200318.2 x86_64 VPC HVM ebs

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6) Navigate to EC2 and create the NAT instance in the public subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

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 ⓘ

1

Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ

☐ Request Spot instances

Network ⓘ

vpc-01c777ccc03c4dc61 | Project 1 VPC

Create new VPC

Subnet ⓘ

subnet-06104cc3bacff4a82 | Public Subnet | us-east-1

Create new subnet

Auto-assign Public IP ⓘ

Use subnet setting (Enable)

Placement group ⓘ

☐ Add instance to placement group

Capacity Reservation ⓘ

Open

IAM role ⓘ

None

Create new IAM role

Shutdown behavior ⓘ

Stop

Stop - Hibernate behavior ⓘ

☐ Enable hibernation as an additional stop behavior

Enable termination protection ⓘ

☐ Protect against accidental termination

Monitoring ⓘ

☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Tenancy ⓘ

Shared - Run a shared hardware instance

Additional charges will apply for dedicated tenancy.

Elastic Inference ⓘ

☐ Add an Elastic Inference accelerator

Additional charges apply.

T2/T3 Unlimited ⓘ

☐ Enable

Additional charges may apply

File systems ⓘ

Add file system

Create new file system

Cancel

Previous

Review and Launch

Next: Add Storage

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6) Navigate to EC2 and create the NAT instance in the public subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

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 name:

Description:

| Type | Protocol | Port Range | Source | Description |
|-------|----------|------------|--------------------|--|
| SSH | TCP | 22 | Custom 10.0.2.0/24 | Receive SSH traffic only from the private subnet |
| HTTP | TCP | 80 | Custom 10.0.2.0/24 | Receive HTTP traffic only from the private subnet |
| HTTPS | TCP | 443 | Custom 10.0.2.0/24 | Receive HTTPS traffic only from the private subnet |

Add Rule

Cancel

Previous

Review and Launch

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

6) Navigate to EC2 and create the NAT instance in the public subnet

aws

Services

Resource Groups

New EC2 Experience

Learn more

EC2 Dashboard

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

Name

Instance ID

Instance Type

Availability Zone

Instance State

Status Checks

Alarm Status

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

Key Name

Monitoring

Launch

i-0d2593c9adc51812f

t2.micro

us-east-1f

running

2/2 checks ...

None

ec2-3-237-31-83.comp...

3.237.31.83

-

NAT key pair

disabled

August

Instance: i-0d2593c9adc51812f

Public DNS: ec2-3-237-31-83.compute-1.amazonaws.com

Description

Status Checks

Monitoring

Tags

Instance ID

Instance state

Instance type

Finding

Private DNS

Private IPs

Secondary private IPs

VPC ID

Platform

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

Elastic IPs

Availability zone

Security groups

Scheduled events

AMI ID

Subnet ID

i-0d2593c9adc51812f

running

t2.micro

You may not have permission to access AWS Compute Optimizer.

ip-10-0-1-31.ec2.internal

10.0.1.31

vpc-01c777ccc03c4dc61 (Project 1 VPC)

Amazon Linux

ec2-3-237-31-83.compute-1.amazonaws.com

3.237.31.83

-

us-east-1f

NATSG. view inbound rules. view outbound rules

No scheduled events

amzn-ami-vpc-nat-hvm-2018.03.0.20181116-x86_64-eb3 (ami-00a9d4a05375b2763)

subnet-06104cc3bacff4a82 (Public Subnet)

Feedback

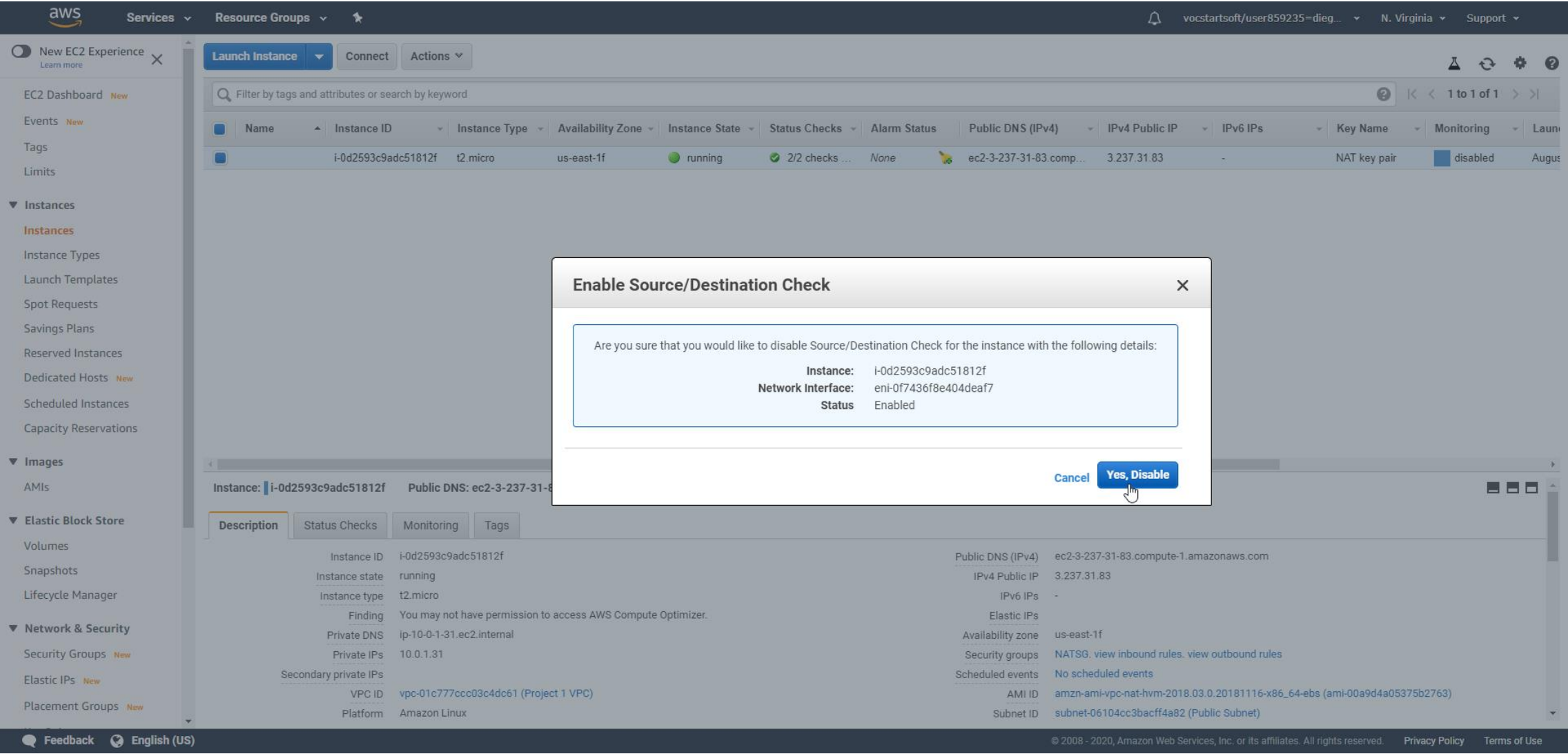
English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

6) Navigate to EC2 and create the NAT instance in the public subnet



7) Create the private route table pointing to the NAT instance and associate it with the private subnet

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

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

Private Route Table

VPC*

Filter by attributes

vpc-a915fed4

vpc-01c777ccc03c4dc61

Project 1 VPC

Add Tag

50 remaining

(Up to 50 tags maximum)

This resource currently has no tags

* Required

Cancel

Create

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

7) Create the private route table pointing to the NAT instance and associate it with the private subnet

aws

Services

Resource Groups

vocstartsoft/user859235=diag...

N. Virginia

Support

Route Tables

> Edit routes

Edit routes

| Destination | Target | Status | Propagated |
|--|--------------------------------|--------|------------|
| 10.0.0.0/16 | local | active | No |
| <input type="text" value="0.0.0.0/0"/> | <input type="text" value="i"/> | | No |

Add route

i-0d2593c9adc51812f

NAT instance

* Required

Cancel

Save routes

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

7) Create the private route table pointing to the NAT instance and associate it with the private subnet

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

New VPC Experience

Learn more

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Carrier Gateways

DHCP Options Sets

Elastic IPs

Managed Prefix Lists

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Create route table

Actions

Filter by tags and attributes or search by keyword

1 to 4 of 4

| | Name | Route Table ID | Explicit subnet association | Edge associations | Main | VPC ID | Owner |
|-------------------------------------|---------------------|-----------------------|-----------------------------|-------------------|------|----------------------------|--------------|
| <input type="checkbox"/> | | rtb-679deb19 | - | - | Yes | vpc-a915fed4 | 280157415142 |
| <input type="checkbox"/> | | rtb-0a05ec85a0cea06c9 | - | - | Yes | vpc-01c777ccc03c4dc61 ... | 280157415142 |
| <input checked="" type="checkbox"/> | Private Route Table | rtb-0d2b00bff3fd492b1 | - | - | No | vpc-01c777ccc03c4dc61 ... | 280157415142 |
| <input type="checkbox"/> | Public Route table | rtb-056c3e917489d5b3c | subnet-06104cc3bacff4a82 | - | No | vpc-01c777ccc03c4dc61 ... | 280157415142 |

Route Table: rtb-0d2b00bff3fd492b1

Summary

Routes

Subnet Associations

Edge Associations

Route Propagation

Tags

Edit subnet associations

None found

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|--|-----------|-----------|
| You do not have any subnet associations. | | |

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

1 to 1 of 1

| Subnet ID | IPv4 CIDR | IPv6 CIDR |
|---|-------------|-----------|
| subnet-076db1b17b707b636 Private Subnet | 10.0.2.0/24 | - |

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

7) Create the private route table pointing to the NAT instance and associate it with the private subnet

aws

Services ▾ Resource Groups ▾

vocstartsoft/user859235=dieg...

N. Virginia ▾

Support ▾

Route Tables > Edit subnet associations

Edit subnet associations

Route table rtb-0d2b00bff3fd492b1 (Private Route Table)

Associated subnets subnet-076db1b17b707b636

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-076db1b17b707b636 Private S... | 10.0.2.0/24 | - | Main |
| <input type="checkbox"/> | subnet-06104cc3bacff4a82 Public Sub... | 10.0.1.0/24 | - | rtb-056c3e917489d5b3c |

* Required

Cancel

Save

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

8) Create the Application Server in the public subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

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)

Cancel and Exit

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 Ubuntu

×

Search by Systems Manager parameter

Quick Start (8)

My AMIs (0)

AWS Marketplace (465)

Community AMIs (39059)

☐ Free tier only ⓘ

🔗

Free tier eligible

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type

ami-0bcc094591f354be2 (64-bit x86) / ami-0bc556e0c71e1b467 (64-bit Arm)

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)

☐ 64-bit (Arm)

🔗

Free tier eligible

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type

ami-05e16100b6f337dda (64-bit x86) / ami-0580fcddde65b4ace (64-bit Arm)

Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)

☐ 64-bit (Arm)

🔗

Deep Learning AMI (Ubuntu 18.04) Version 32.0

ami-0dc2264cd927ca9eb

MXNet-1.6.0, TensorFlow-2.3.0, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.6.0, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA support. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

🔗

Deep Learning AMI (Ubuntu 16.04) Version 32.0

ami-0eeaa365fa25d692a

MXNet-1.6.0, TensorFlow-2.3.0, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.6.0, EI, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

🔗

Deep Learning Base AMI (Ubuntu 18.04) Version 27.0

ami-0635dd49d5f046547

NVIDIA CUDA, cuDNN, NCCL, GPU Drivers, Intel MKL-DNN, Docker, NVIDIA-Docker & other system libraries to deploy your own custom deep learning environment. For a fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

🔗

Deep Learning Base AMI (Ubuntu 16.04) Version 27.0

ami-0139620c36763c6

Select

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

8) Create the Application Server in the public subnet

aws

Services

Resource Groups

vocstartsoft/user859235=diag...

N. Virginia

Support

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

1

Launch into Auto Scaling Group

Purchasing option

☐ Request Spot instances

Network

vpc-01c777ccc03c4dc61 | Project 1 VPC

Create new VPC

Subnet

subnet-06104cc3bacff4a82 | Public Subnet | us-east-

Create new subnet

Auto-assign Public IP

Use subnet setting (Enable)

Placement group

☐ Add instance to placement group

Capacity Reservation

Open

IAM role

None

Create new IAM role

Shutdown behavior

Stop

Stop - Hibernate behavior

☐ Enable hibernation as an additional stop behavior

Enable termination protection

☐ Protect against accidental termination

Monitoring

☐ Enable CloudWatch detailed monitoring

Additional charges apply.

Tenancy

Shared - Run a shared hardware instance

Additional charges will apply for dedicated tenancy.

Elastic Inference

☐ Add an Elastic Inference accelerator

Additional charges apply.

T2/T3 Unlimited

☐ Enable

Additional charges may apply

File systems

Add file system

Create new file system

Cancel

Previous

Review and Launch

Next: Add storage

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

8) Create the Application Server in the public subnet

aws

Services

Resource Groups

vocstartsoft/user859235=diag...

N. Virginia

Support

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 name:

Description:

| Type | Protocol | Port Range | Source | Description |
|--------------|----------|------------|------------------------|----------------------------|
| SSH | TCP | 22 | Custom 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| Custom TCP F | TCP | 8065 | Custom 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |

Add Rule

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel

Previous

Review and Launch

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

9) Create the Database server in the private subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

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)

Cancel and Exit

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 Ubuntu

Search by Systems Manager parameter

Quick Start (8)

My AMIs (0)

AWS Marketplace (465)

Community AMIs (39059)

☐ Free tier only

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0bcc094591f354be2 (64-bit x86) / ami-0bc556e0c71e1b467 (64-bit Arm)

Free tier eligible

Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

64-bit (Arm)

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-05e16100b6f337dda (64-bit x86) / ami-0580fcddde65b4ace (64-bit Arm)

Free tier eligible

Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (<http://www.ubuntu.com/cloud/services>).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

64-bit (Arm)

Deep Learning AMI (Ubuntu 18.04) Version 32.0 - ami-0dc2264cd927ca9eb

MXNet-1.6.0, TensorFlow-2.3.0, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.6.0, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA support. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

Deep Learning AMI (Ubuntu 16.04) Version 32.0 - ami-0eeaa365fa25d692a

MXNet-1.6.0, TensorFlow-2.3.0, 2.1.0 & 1.15.3, PyTorch-1.4.0 & 1.6.0, EI, Neuron, & others. NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker, NVIDIA-Docker & EFA. For fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

Deep Learning Base AMI (Ubuntu 18.04) Version 27.0 - ami-0635dd49d5f046547

NVIDIA CUDA, cuDNN, NCCL, GPU Drivers, Intel MKL-DNN, Docker, NVIDIA-Docker & other system libraries to deploy your own custom deep learning environment. For a fully managed experience, check: <https://aws.amazon.com/sagemaker>

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

64-bit (x86)

Deep Learning Base AMI (Ubuntu 16.04) Version 27.0 - ami-0139620c36763c6

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

9) Create the Database server in the private subnet

aws

Services

Resource Groups

🔔

vocstartsoft/user859235=dieg...

N. Virginia

Support

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

1

Launch into Auto Scaling Group

Purchasing option

☐ Request Spot instances

Network

vpc-01c777ccc03c4dc61 | Project 1 VPC

Create new VPC

Subnet

subnet-076db1b17b707b636 | Private Subnet | us-east-1

Create new subnet

Auto-assign Public IP

Use subnet setting (Disable)

Placement group

☐ Add instance to placement group

Capacity Reservation

Open

IAM role

None

Create new IAM role

Shutdown behavior

Stop

Stop - Hibernate behavior

☐ Enable hibernation as an additional stop behavior

Enable termination protection

☐ Protect against accidental termination

Monitoring

☐ Enable CloudWatch detailed monitoring

Tenancy

Shared - Run a shared hardware instance

Elastic Inference

☐ Add an Elastic Inference accelerator

T2/T3 Unlimited

☐ Enable

251 IP Addresses available

Additional charges apply.

Additional charges will apply for dedicated tenancy.

Additional charges may apply.

Cancel

Previous

Review and Launch

Next: Add Storage

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Privacy Policy

Terms of Use

9) Create the Database server in the private subnet

aws

Services

Resource Groups

vocstartsoft/user859235=dieg...

N. Virginia

Support

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 name:

Description:

| Type | Protocol | Port Range | Source | Description |
|--------------|----------|------------|------------------------|----------------------------|
| SSH | TCP | 22 | Custom 0.0.0.0/0 | e.g. SSH for Admin Desktop |
| MySQL/Aurora | TCP | 3306 | Anywhere 0.0.0.0, ::/0 | e.g. SSH for Admin Desktop |

Add Rule

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel

Previous

Review and Launch

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

9) Create the Database server in the private subnet

aws

Services

Resource Groups

New EC2 Experience

Learn more

EC2 Dashboard

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

Elastic IPs

Placement Groups

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

1 to 3 of 3

| | Name | Instance ID | Instance Type | Availability Zone | Instance State | Status Checks | Alarm Status | Public DNS (IPv4) | IPv4 Public IP | IPv6 IPs | Key Name | Monitoring |
|--------------------------|--------------|---------------------|---------------|-------------------|----------------|----------------|--------------|----------------------------------|----------------|----------|-------------------|------------|
| <input type="checkbox"/> | NAT instance | i-0d2593c9adc51812f | t2.micro | us-east-1f | running | 2/2 checks ... | None | ec2-3-237-31-83.compute-1.ama... | 3.237.31.83 | - | NAT key pair | disabled |
| <input type="checkbox"/> | Application | i-0a9133ec576a33594 | t2.micro | us-east-1f | running | 2/2 checks ... | None | ec2-35-175-112-215.compute-1.... | 35.175.112.215 | - | Application ke... | disabled |
| <input type="checkbox"/> | Database | i-0ff6bdfb151fb964b | t2.micro | us-east-1f | running | 2/2 checks ... | None | | - | - | Database key ... | disabled |

Select an instance above

Feedback

English (US)

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

10) Copy the pem file for the Database Server to the Application Server to use it as a Bastion Host

```
MINGW64/c/Users/diego.bettega

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ pwd
/c/Users/diego.bettega

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ scp -i app_key_pair.pem app_key_pair.pem ubuntu@35.175.112.215:/home/ubuntu
load pubkey "app_key_pair.pem": invalid format
app_key_pair.pem                                     100% 1692    8.1KB/s   00:00

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$
```

11) Log into the application server and use it as a Bastion Host to log into the database server

```

MINGW64~/c/Users/diego.bettega

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ pwd
/c/Users/diego.bettega

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ scp -i app_key_pair.pem app_key_pair.pem ubuntu@35.175.112.215:/home/ubuntu
load pubkey "app_key_pair.pem": invalid format
app_key_pair.pem                                     100% 1692    8.1KB/s   00:00

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ ssh -i app_key_pair.pem ubuntu@35.175.112.215
load pubkey "app_key_pair.pem": invalid format
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.3.0-1032-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Aug 16 17:53:05 UTC 2020

System load:  0.0          Processes:      92
Usage of /:   29.1% of 7.69GB Users logged in:   0
Memory usage: 21%         IP address for eth0: 10.0.1.112
Swap usage:   0%

 * Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
   sudo snap install microk8s --channel=1.19/candidate --classic
   https://microk8s.io/ has docs and details.

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

2 packages can be updated.
2 updates are security updates.

Last login: Sat Aug 15 16:43:55 2020 from 86.6.240.100
ubuntu@ip-10-0-1-112:~$ ssh -i app_key_pair.pem ubuntu@ip-10-0-2-97.ec2.internal
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@                WARNING: UNPROTECTED PRIVATE KEY FILE!                @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'app_key_pair.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "app_key_pair.pem": bad permissions
ubuntu@ip-10-0-2-97.ec2.internal: Permission denied (publickey).
ubuntu@ip-10-0-1-112:~$
```

11) Log into the application server and use it as a Bastion Host to log into the database server

I was unable to proceed on point 12) & 13) because of this issue. I made a research on Google and I found this article:
<https://superuser.com/questions/1296024/windows-ssh-permissions-for-private-key-are-too-open>

I tried to execute the command before and/or after copying the pem file for the Database Server to the Application Server to use it as a Bastion Host, but I was unable to fix the issue.

14) Install the Mattermost application and run it using the provided commands in the brief

```
MINGW64/c/Users/diego.bettega

diego.bettega@LDNMBL-LW1046Q4 MINGW64 ~
$ ssh -i appkeypair.pem ubuntu@35.175.112.215
load pubkey "appkeypair.pem": invalid format
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.3.0-1032-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Aug 15 16:43:54 UTC 2020

System load:  0.05          Processes:           91
Usage of /:   24.0% of 7.69GB Users logged in:        0
Memory usage: 18%          IP address for eth0: 10.0.1.112
Swap usage:   0%

0 packages can be updated.
0 updates are security updates.

Last login: Sat Aug 15 16:42:38 2020 from 86.6.240.100
ubuntu@ip-10-0-1-112:~$ wget https://storage.googleapis.com/skl-training/aws-codelabs/mattermost/mattermost_install.sh
--2020-08-15 16:44:01-- https://storage.googleapis.com/skl-training/aws-codelabs/mattermost/mattermost_install.sh
Resolving storage.googleapis.com (storage.googleapis.com)... 172.217.13.80, 172.217.13.240, 172.217.15.112, ...
Connecting to storage.googleapis.com (storage.googleapis.com)|172.217.13.80|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 413 [application/x-shellscript]
Saving to: 'mattermost_install.sh.2'

mattermost_install.sh.2                100%[=====>] 413  --.-KB/s  in 0s

2020-08-15 16:44:01 (63.1 MB/s) - 'mattermost_install.sh.2' saved [413/413]

ubuntu@ip-10-0-1-112:~$ chmod 700 mattermost_install.sh
ubuntu@ip-10-0-1-112:~$ sudo ./mattermost_install.sh 10.0.2.97
```

I have executed only in a second time the last command to be able to get the screenshot

14) Install the Mattermost application and run it using the provided commands in the brief

```
ubuntu@ip-10-0-1-112:~$ sudo chown -R mattermost:mattermost /opt/mattermost
ubuntu@ip-10-0-1-112:~$ sudo chmod -R g+w /opt/mattermost
ubuntu@ip-10-0-1-112:~$ cd /opt/mattermost
ubuntu@ip-10-0-1-112:/opt/mattermost$
ubuntu@ip-10-0-1-112:/opt/mattermost$ sudo -u mattermost ./bin/mattermost
{"level":"info","ts":1597510069.8618348,"caller":"utils/i18n.go:83","msg":"Loaded system translations","for locale":"en","from locale":"/opt/mattermost/i18n/en.json"}
{"level":"info","ts":1597510069.862204,"caller":"app/server_app_adapters.go:58","msg":"Server is initializing..."}
{"level":"info","ts":1597510069.9152741,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510069.9187708,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510079.9218786,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510079.925595,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510089.9257905,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510089.9263866,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510099.9265764,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510099.9271402,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510109.9273207,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510109.9279685,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510119.928187,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510119.9289255,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510129.9291484,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510129.9638891,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510139.9642575,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510139.965001,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510149.9653194,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510149.9660778,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510159.9663715,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510159.9679573,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510169.9682837,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510169.968997,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510179.9693031,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510179.9700718,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510189.972414,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510189.9737692,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510199.974088,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510199.974978,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510209.9752665,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510209.9759793,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510219.9762917,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510219.9784834,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510229.9787874,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510229.9796424,"caller":"sqlstore/supplier.go:224","msg":"Failed to ping DB","error":"dial tcp 10.0.2.97:3306: connect: connection refused","retrying in seconds":10}
{"level":"info","ts":1597510239.9799516,"caller":"sqlstore/supplier.go:212","msg":"Pinging SQL","database":"master"}
{"level":"error","ts":1597510239.9807508,"caller":"sqlstore/supplier.go:220","msg":"Failed to ping DB, server will exit.","error":"dial tcp 10.0.2.97:3306: connect: connection refused"}
ubuntu@ip-10-0-1-112:/opt/mattermost$
```


15) Test the success of the implementation by visiting the public IP of the application server in your browser with the port 8065

I haven't been able to complete this step because of the issue I had at 11)

