Creating a Virtual Private Cloud

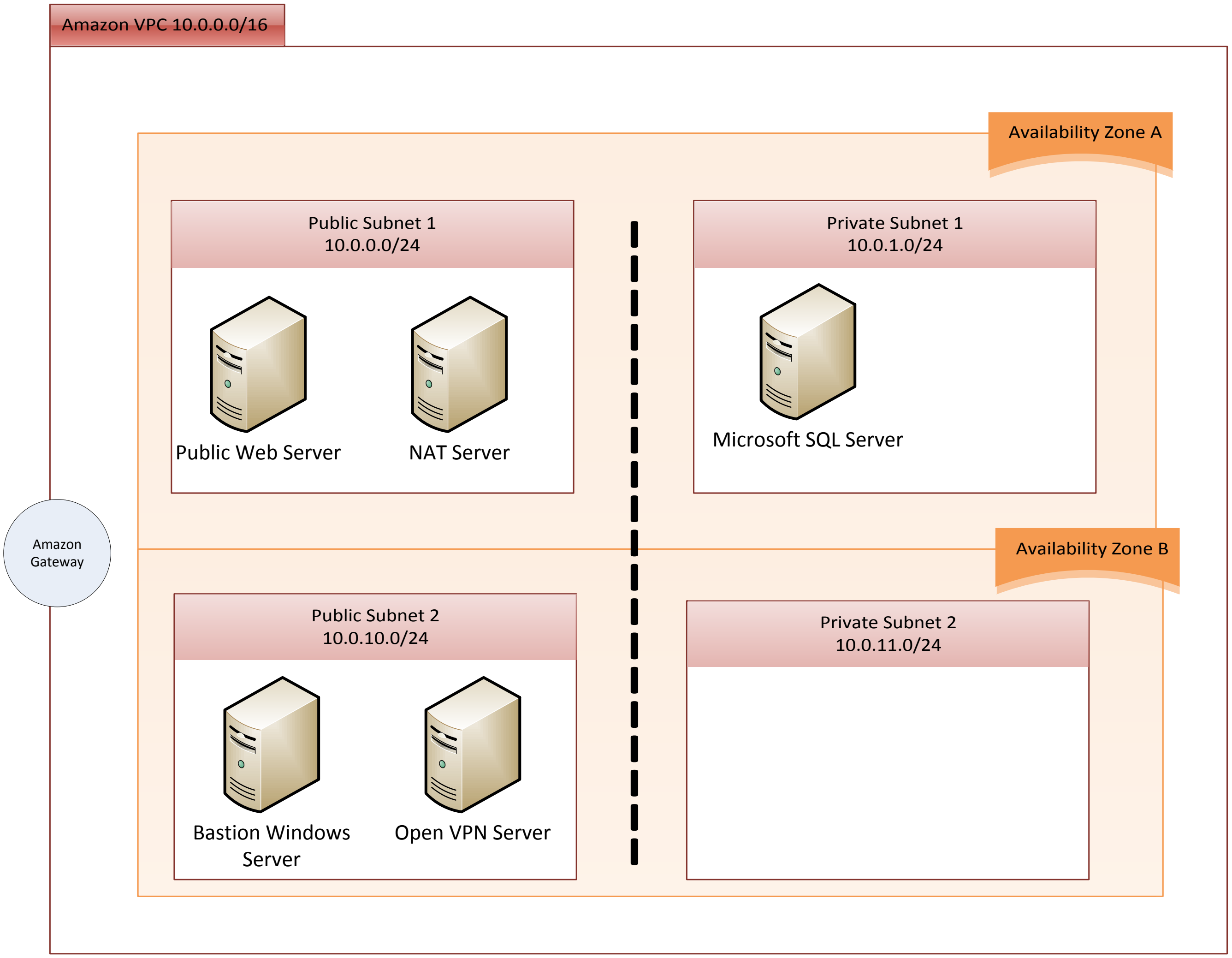
v. 3.0

TABLE OF CONTENTS

OVERVIEW

In this lab session, we are going to create a basic Amazon Virtual Private Cloud (VPC), and then extend what we created in order to produce a customized result. We'll do all of this with the AWS Management Console.

The diagram below is what we will build.

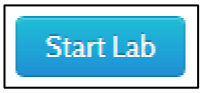


The overall VPC is designed to incorporate several basic features:

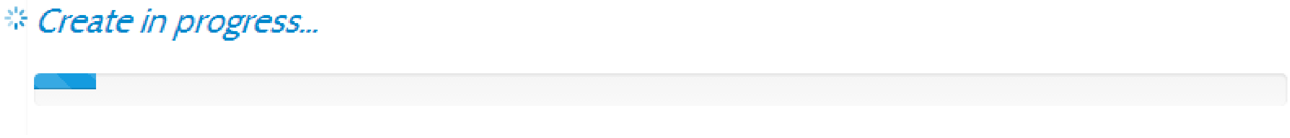
- It spans two Availability Zones (AZs), in order that later you can distribute applications across these zones in order to architect for application durability and availability.
- Within each Availability Zone (AZ) there are two subnets: one "public" subnet is connected directly to the Internet. The other "private" subnet is able to communicate with any other subnet within the VPC; however there is no access to them from the Internet. The dashed line demarcates this isolation.
- We'll walk through two alternatives to allowing access to servers that are in the private subnets.

START YOUR *QWIKLAB™*

1) Start your *qwikLAB™*
   Use the ‘Start Lab’ button to start your lab.
   (Hint: If you are prompted for a token, please use one you’ve been given or have purchased.)



   You will see the lab creation in progress.

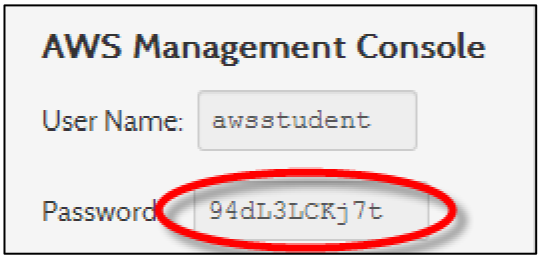


2) Note a few properties of the lab.

   a. **Duration -** The time the lab will run for before shutting itself down.
   b. **Setup Time -** The estimated lab creation time on starting the lab.
   c. **AWS Region** - The AWS Region the lab resources are being created in.

3) Copy the Password provided.

   a. Hint: selecting the value shown and using Ctrl+C works best

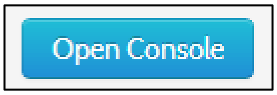


AWS Management Console

User Name: awsstudent

Password: 94dL3LCKj7t

4) Click the ‘Open Console’ button.

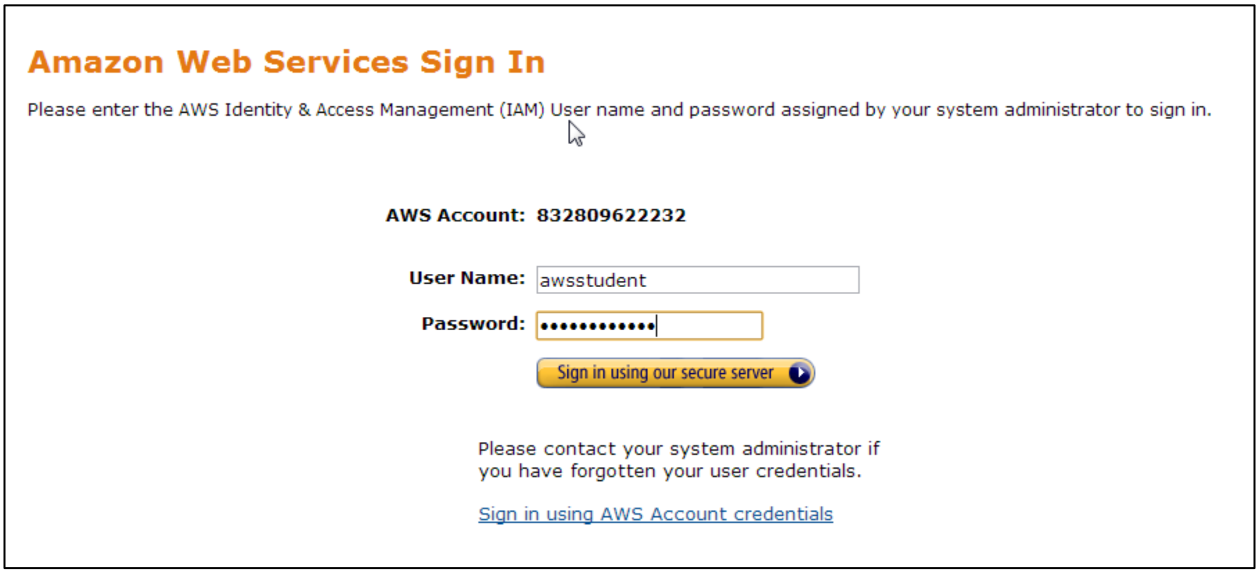


5) Login to the AWS Management Console

Enter the User Name ‘**awsstudent**’ and paste the password you copied from the lab details in *qwikLAB™* into the Password field.

Click on the ‘Sign in using our secure server’ button.

In this step you logged into the AWS Management Console using login credentials for a user provisioned via AWS Identity Access Management in an AWS account by *qwikLAB™*.



Amazon Web Services Sign In

Please enter the AWS Identity & Access Management (IAM) User name and password assigned by your system administrator to sign in.

AWS Account: 832809622232

User Name: awsstudent

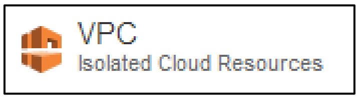
Password: ••••••••••••

Please contact your system administrator if you have forgotten your user credentials.

Sign in using AWS Account credentials

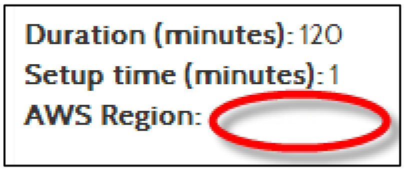
AWS MANAGEMENT CONSOLE

Once logged in, select "VPC" as from the service console.



CONFIRM YOUR AWS REGION

Note the AWS Region set for your lab in *qwikLAB*™

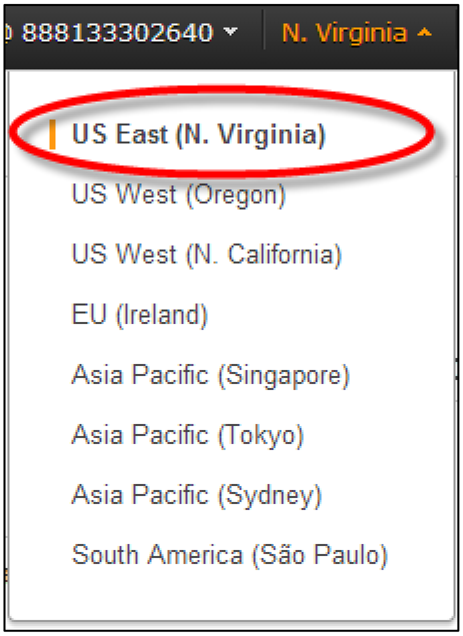


Duration (minutes): 120

Setup time (minutes): 1

AWS Region:

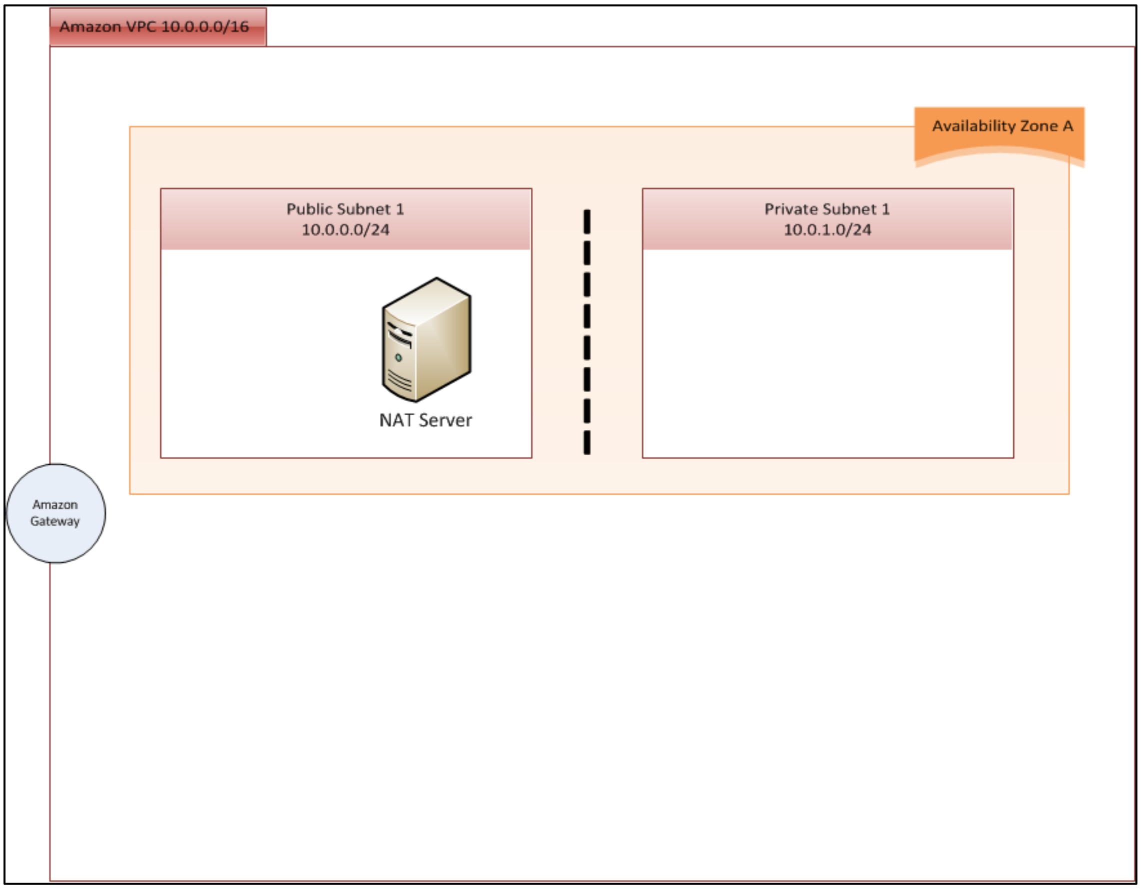
Select or confirm that the same AWS Region is already set in the AWS Management Console



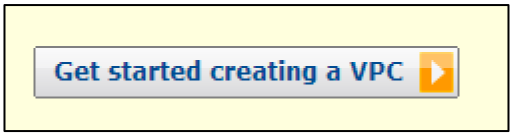
CREATE THE BASE VPC

We'll use a wizard to set up the initial VPC, and then we'll extend the result manually.

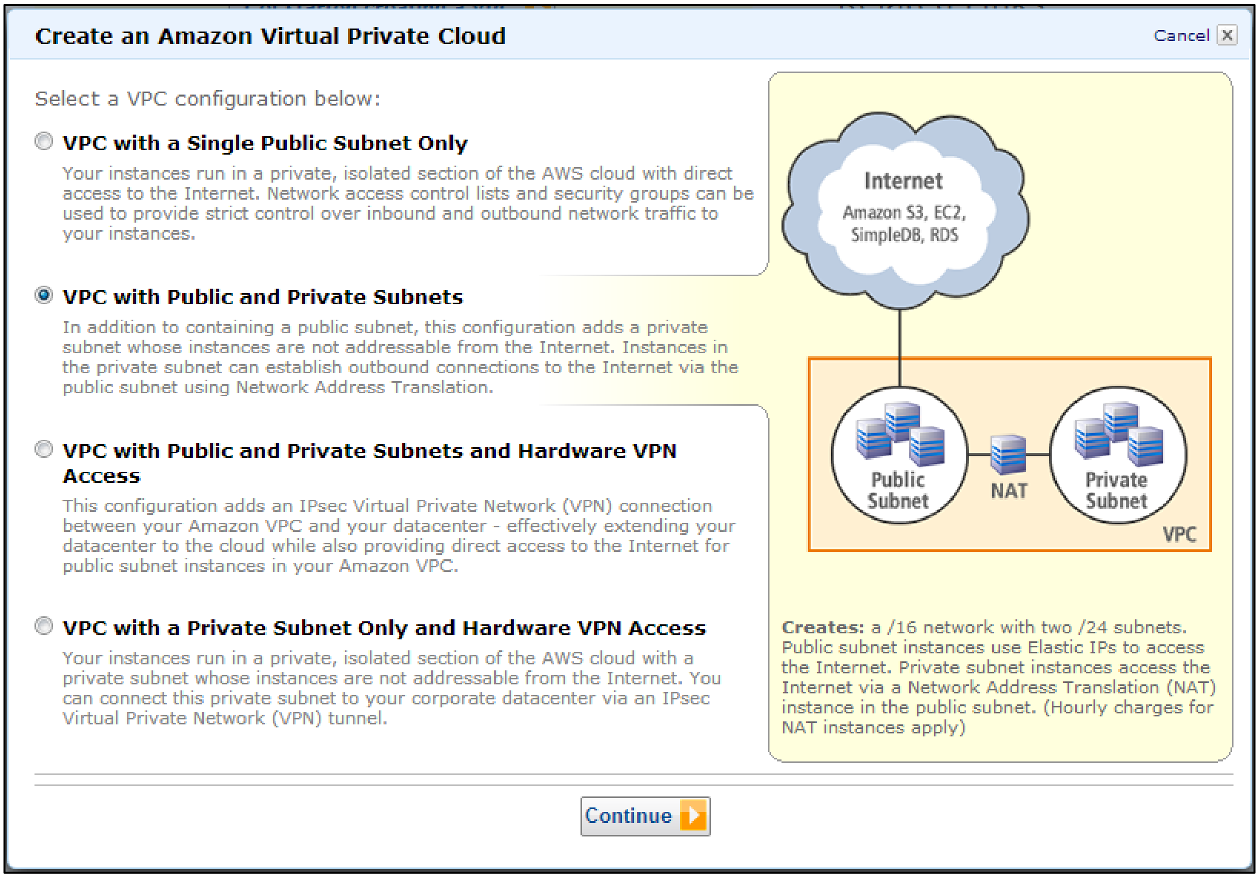
Initially we will create this:



We'll use the wizard to set up the initial network, which is fast and easy, but that won't teach you very much about VPC.



Choose the second option on the list and click Continue.



Create an Amazon Virtual Private Cloud

Select a VPC configuration below:

○ **VPC with a Single Public Subnet Only**

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

● **VPC with Public and Private Subnets**

In addition to containing a public subnet, this configuration adds a private subnet whose instances are not addressable from the Internet. Instances in the private subnet can establish outbound connections to the Internet via the public subnet using Network Address Translation.

○ **VPC with Public and Private Subnets and Hardware VPN Access**

This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your datacenter - effectively extending your datacenter to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.

○ **VPC with a Private Subnet Only and Hardware VPN Access**

Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate datacenter via an IPsec Virtual Private Network (VPN) tunnel.

Creates: a /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply)

This screen contains a lot of parameters. Depending on your professional background, the notation may appear different than what you are used to. This notation is commonly known as CIDR block notation, so, for example, 10.0.1.0/24 can also be expressed as 10.0.1.0 with a subnet mask of 255.255.255.0.

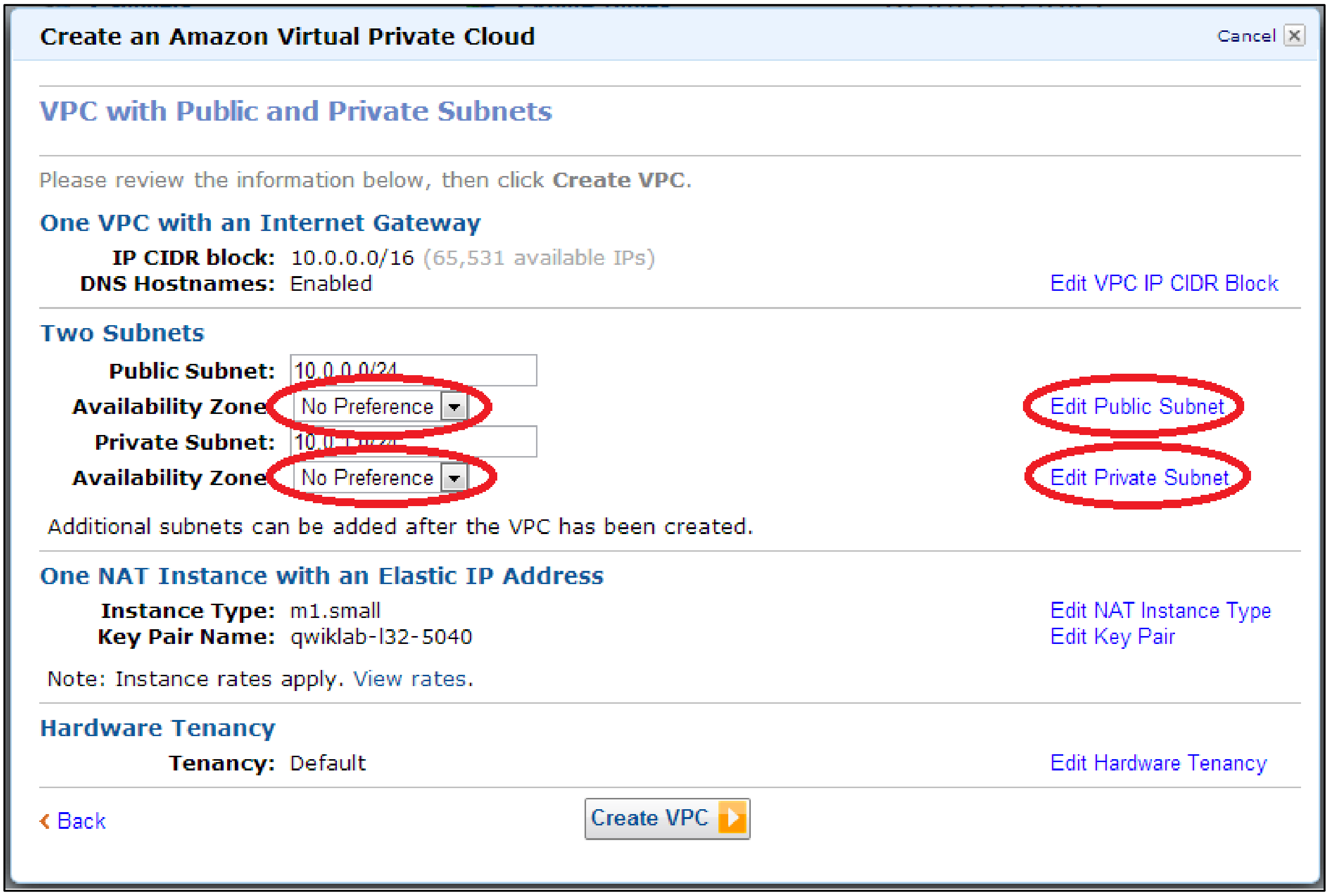
The VPC itself is a Class B network in the 10.0.0.0 space. If you are familiar with the IPv4 address space, this will be familiar as one of the non-routable address blocks.

The overall address space uses an IP CIDR block of 10.0.0.0/16, which is the equivalent of a subnet mask of 255.255.0.0 (a full Class B network).

We're going to leave most of this set to the default values, except for two settings.

Click on Edit Public Subnet. Select any Amazon EC2 Availability Zone.
Click on Edit Private Subnet. Select the same Availability Zone as you selected for the Public Subnet.

We want to make certain that the subnets are both in the same Amazon EC2 Availability Zone.



Create an Amazon Virtual Private Cloud

VPC with Public and Private Subnets

Please review the information below, then click **Create VPC**.

One VPC with an Internet Gateway

IP CIDR block: 10.0.0.0/16 (65,531 available IPs)
DNS Hostnames: Enabled

Two Subnets

Public Subnet: 10.0.0.0/24
Availability Zone No Preference
Private Subnet: 10.0.1.0/24
Availability Zone No Preference

Additional subnets can be added after the VPC has been created.

One NAT Instance with an Elastic IP Address

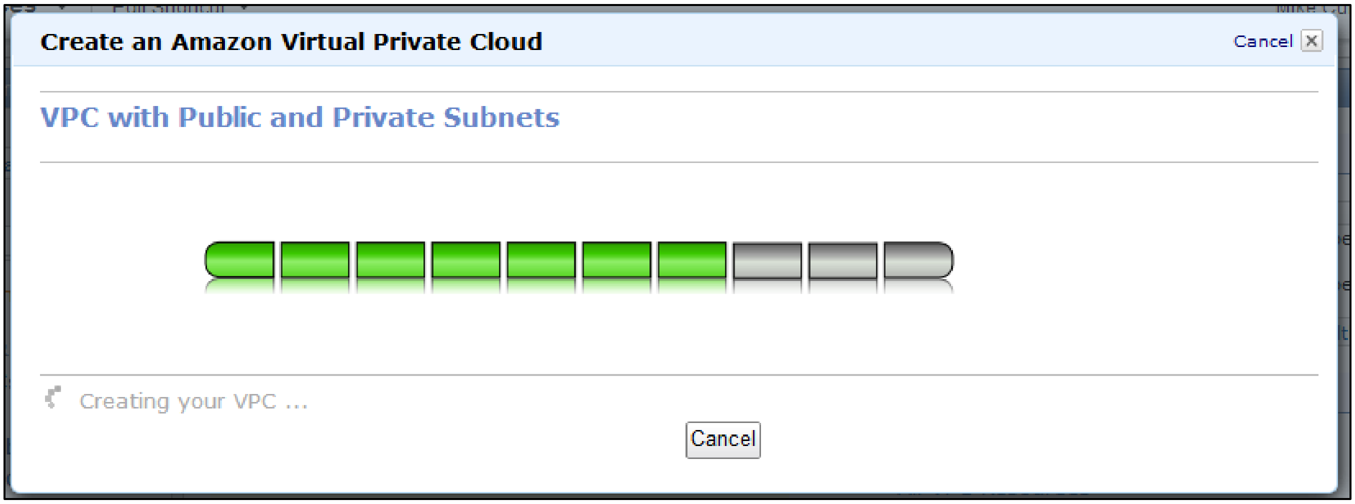
Instance Type: m1.small
Key Pair Name: qwiklab-l32-5040

Note: Instance rates apply. View rates.

Hardware Tenancy

Tenancy: Default

After you’ve selected one and the same Availability Zone for both the Public and Private Subnet, create the VPC by clicking on the Create VPC button.

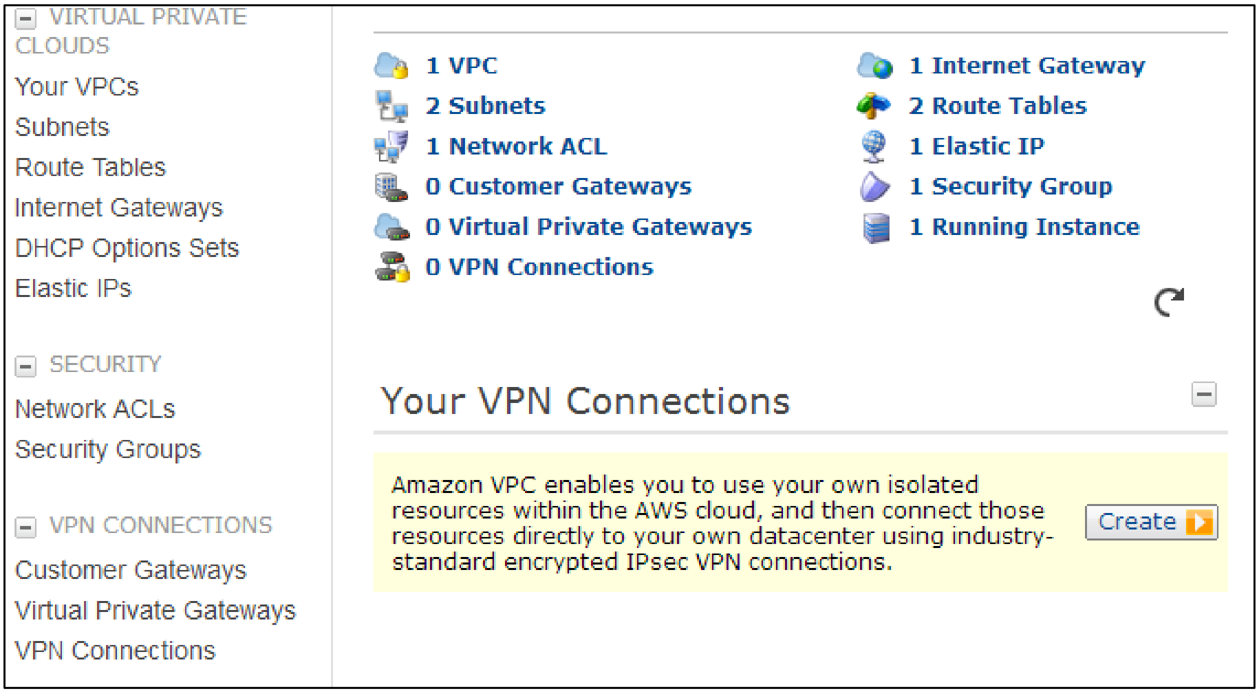


Create an Amazon Virtual Private Cloud

VPC with Public and Private Subnets

Creating your VPC ...

Once finished, you may close the dialog. Back on the VPC Dashboard, we can see the VPC, two subnets, and several other features such as network ACLs and route tables, etc. For the moment all that matters is that the network environment is ready to use.



1 VPC
2 Subnets
1 Network ACL
0 Customer Gateways
0 Virtual Private Gateways
0 VPN Connections
1 Internet Gateway
2 Route Tables
1 Elastic IP
1 Security Group
1 Running Instance

Your VPN Connections

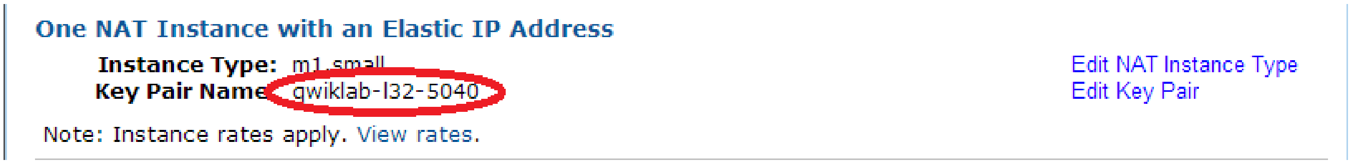
Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

Your VPC does, however, have an important specific: everything is in a single Availability Zone. In order to optimize application availability we need to distribute assets across zones, which means that we'll need to add another pair of subnets. We're going to wait to do that until later in this lab.

NAT SERVERS ARE FOR OUTBOUND REQUESTS

Note that there is already a running instance, which is the NAT server that the wizard created. The NAT server is an appliance in the sense that its only purpose is to allow servers in the Private subnet to communicate with the Internet in order to get updates, software packages, and so forth. It does not allow Internet clients to make connections to servers in the private subnet. Also note that it is assigned an *Elastic IP*, or NAT (Network Address Translation), address in order to facilitate Internet communication.

By default the instance type is an m1.small and the EC2 Key Pair Name associated with it is one that was generated for you by *qwikLAB*™.



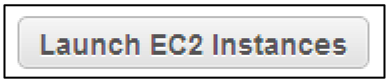
One NAT Instance with an Elastic IP Address

Instance Type: m1.small
Key Pair Name: qwiklab-l32-5040

Note: Instance rates apply. View rates.

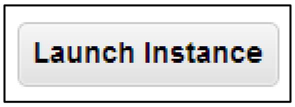
LAUNCH A WEB SERVER

Switch to the EC2 Service by clicking on Launch EC2 Instances.



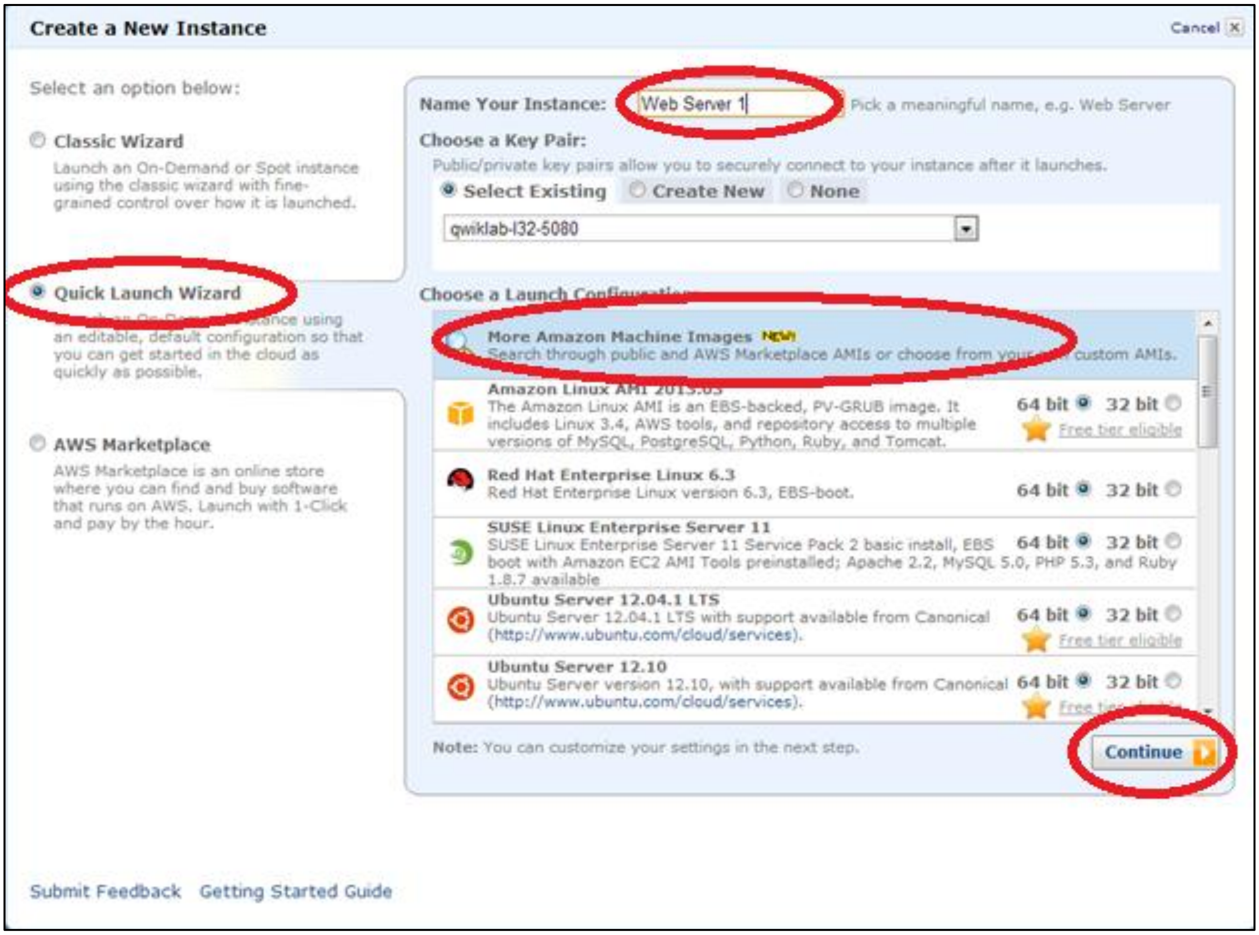
In this lab we're going to launch a BitNami web server as the front-end of our environment. The advantage of this particular AMI is that (a) it was created by a trusted partner, and (b) the Web server will respond to requests with it's default configuration.

Click Launch Instance.



Use the Quick-Launch Wizard, with the following additional choices:

- Name your Instance Web Server 1
- Click on More Amazon Machine Images, and then click Continue



Create a New Instance

Cancel ☒

Select an option below:

○ **Classic Wizard**
Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched.

● **Quick Launch Wizard**
Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible.

○ **AWS Marketplace**
AWS Marketplace is an online store where you can find and buy software that runs on AWS. Launch with 1-Click and pay by the hour.

Name Your Instance: Web Server 1 Pick a meaningful name, e.g. Web Server

Choose a Key Pair:
Public/private key pairs allow you to securely connect to your instance after it launches.
● Select Existing ○ Create New ○ None
qwiklab-l32-5080

Choose a Launch Configuration:

More Amazon Machine Images NEW
Search through public and AWS Marketplace AMIs or choose from your own custom AMIs.

Amazon Linux AMI 2013.03
The Amazon Linux AMI is an EBS-backed, PV-GRUB image. It includes Linux 3.4, AWS tools, and repository access to multiple versions of MySQL, PostgreSQL, Python, Ruby, and Tomcat.
64 bit ● 32 bit ○
Free tier eligible

Red Hat Enterprise Linux 6.3
Red Hat Enterprise Linux version 6.3, EBS-boot.
64 bit ● 32 bit ○

SUSE Linux Enterprise Server 11
SUSE Linux Enterprise Server 11 Service Pack 2 basic install, EBS boot with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, and Ruby 1.8.7 available
64 bit ● 32 bit ○

Ubuntu Server 12.04.1 LTS
Ubuntu Server 12.04.1 LTS with support available from Canonical (http://www.ubuntu.com/cloud/services).
64 bit ● 32 bit ○
Free tier eligible

Ubuntu Server 12.10
Ubuntu Server version 12.10, with support available from Canonical (http://www.ubuntu.com/cloud/services).
64 bit ● 32 bit ○
Free tier eligible

Note: You can customize your settings in the next step.

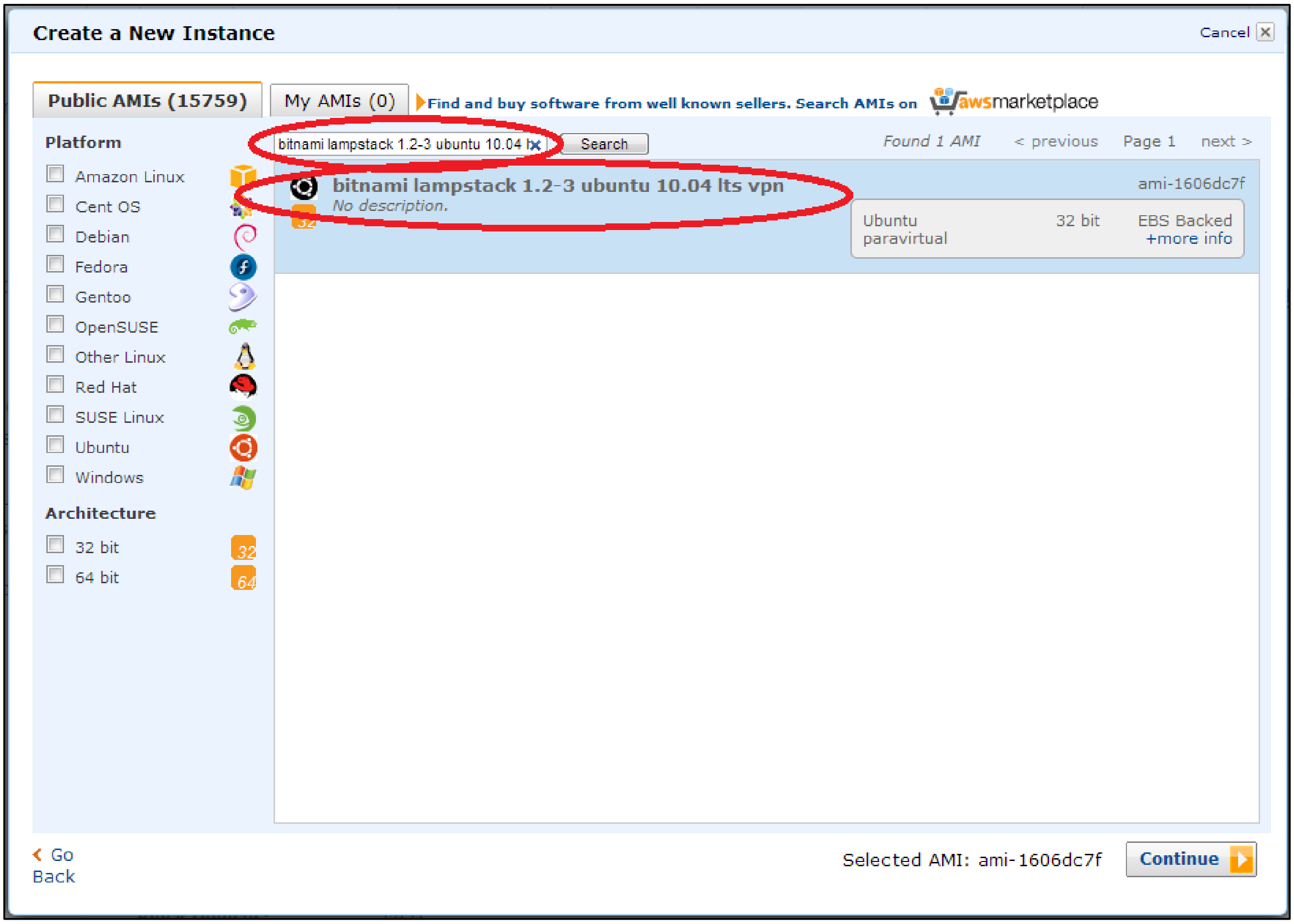
Continue

Submit Feedback Getting Started Guide

On the next screen, copy –paste the following into the search box. You won't even need to click on the search button, because the AMI will simply appear.

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn

Select the AMI by clicking on the search result, and then click on Continue



Create a New Instance

Search: bitnami lampstack 1.2-3 ubuntu 10.04 lt

Found 1 AMI

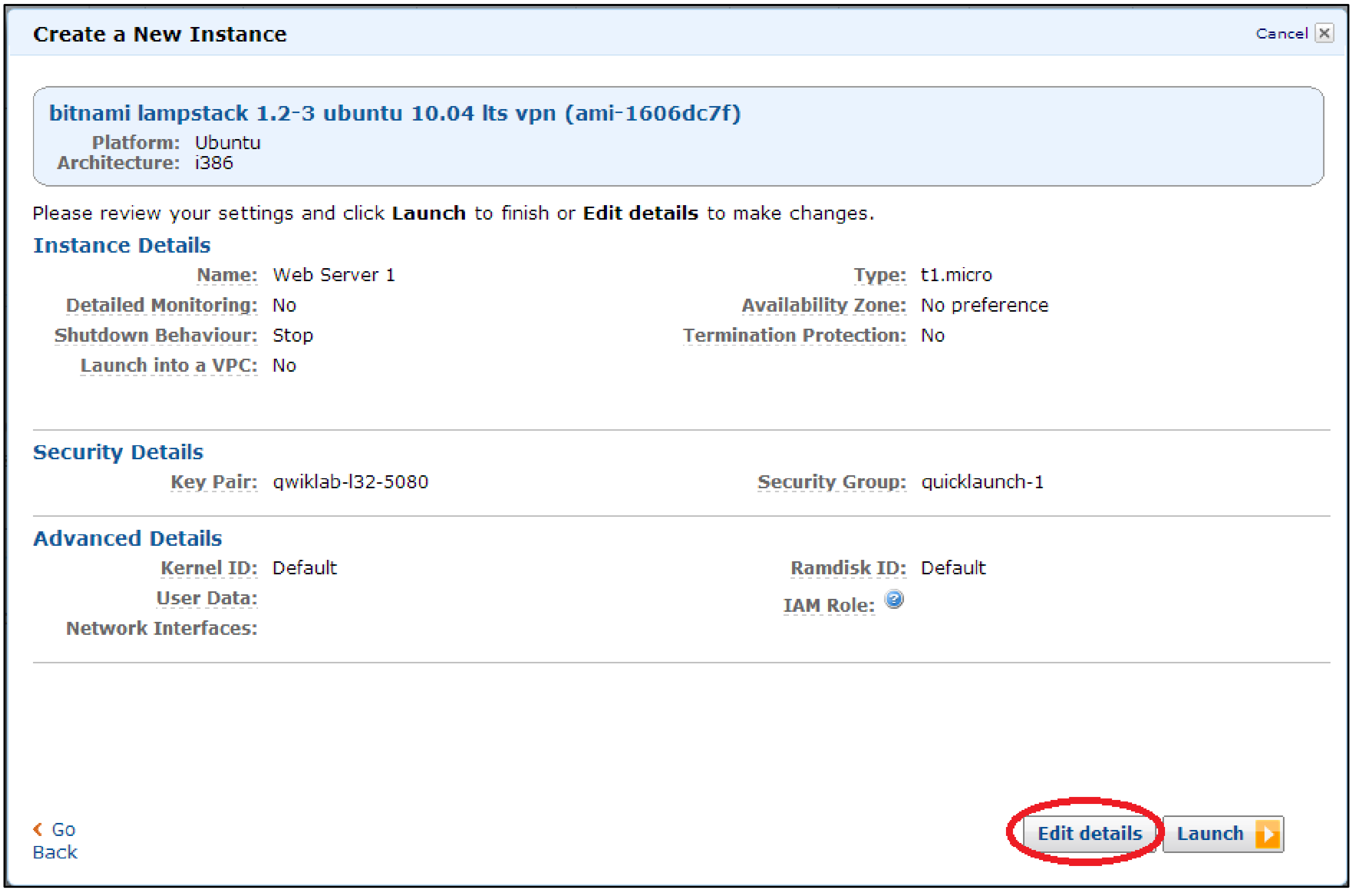
bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn — ami-1606dc7f

No description.

Ubuntu paravirtual | 32 bit | EBS Backed

Selected AMI: ami-1606dc7f

Next, Click Edit Details



Create a New Instance

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn (ami-1606dc7f)

Platform: Ubuntu
Architecture: i386

Please review your settings and click **Launch** to finish or **Edit details** to make changes.

Instance Details

Name:	Web Server 1	Type:	t1.micro
Detailed Monitoring:	No	Availability Zone:	No preference
Shutdown Behaviour:	Stop	Termination Protection:	No
Launch into a VPC:	No		

Security Details

Key Pair:	qwiklab-l32-5080	Security Group:	quicklaunch-1

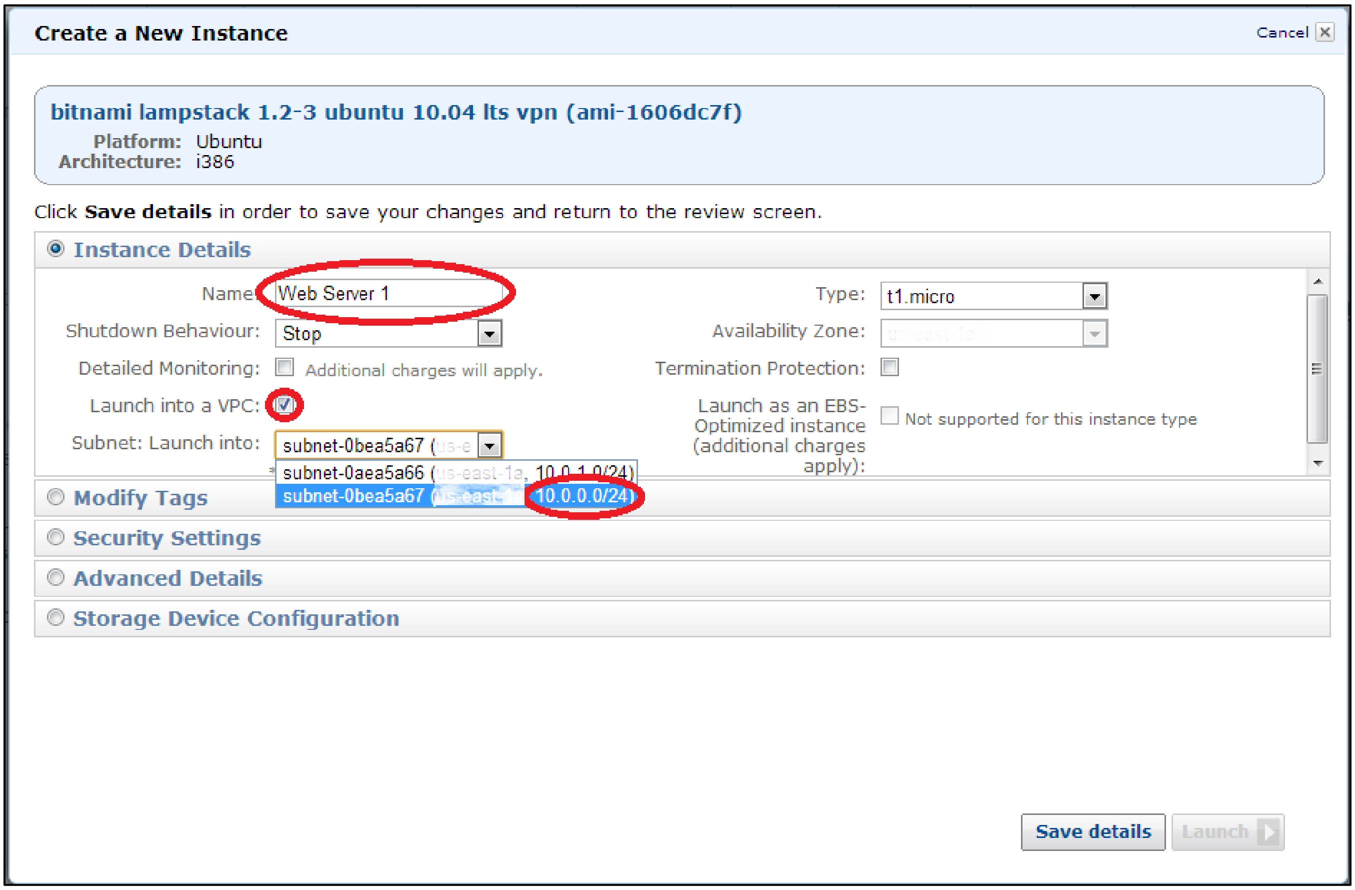
Advanced Details

Kernel ID:	Default	Ramdisk ID:	Default
User Data:		IAM Role:	
Network Interfaces:			

There are three important things to pay attention to on this screen:

- Enter the server name if for some reason it's blank
- Check "Launch into a VPC"
- Choose the public Subnet (10.0.0.0/24)

Do not click on "Save Details". Instead, click on Security Settings.



Create a New Instance

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn (ami-1606dc7f)
Platform: Ubuntu
Architecture: i386

Click **Save details** in order to save your changes and return to the review screen.

● Instance Details

Name: Web Server 1
Shutdown Behaviour: Stop
Detailed Monitoring: □ Additional charges will apply.
Launch into a VPC: ☑
Subnet: Launch into: subnet-0bea5a67 (us-e
subnet-0aea5a66 (us-east-1a, 10.0.1.0/24)
subnet-0bea5a67 (us-east-1a, 10.0.0.0/24)

Type: t1.micro
Availability Zone: us-east-1a
Termination Protection: □
Launch as an EBS-Optimized instance (additional charges apply): □ Not supported for this instance type

○ Modify Tags
○ Security Settings
○ Advanced Details
○ Storage Device Configuration

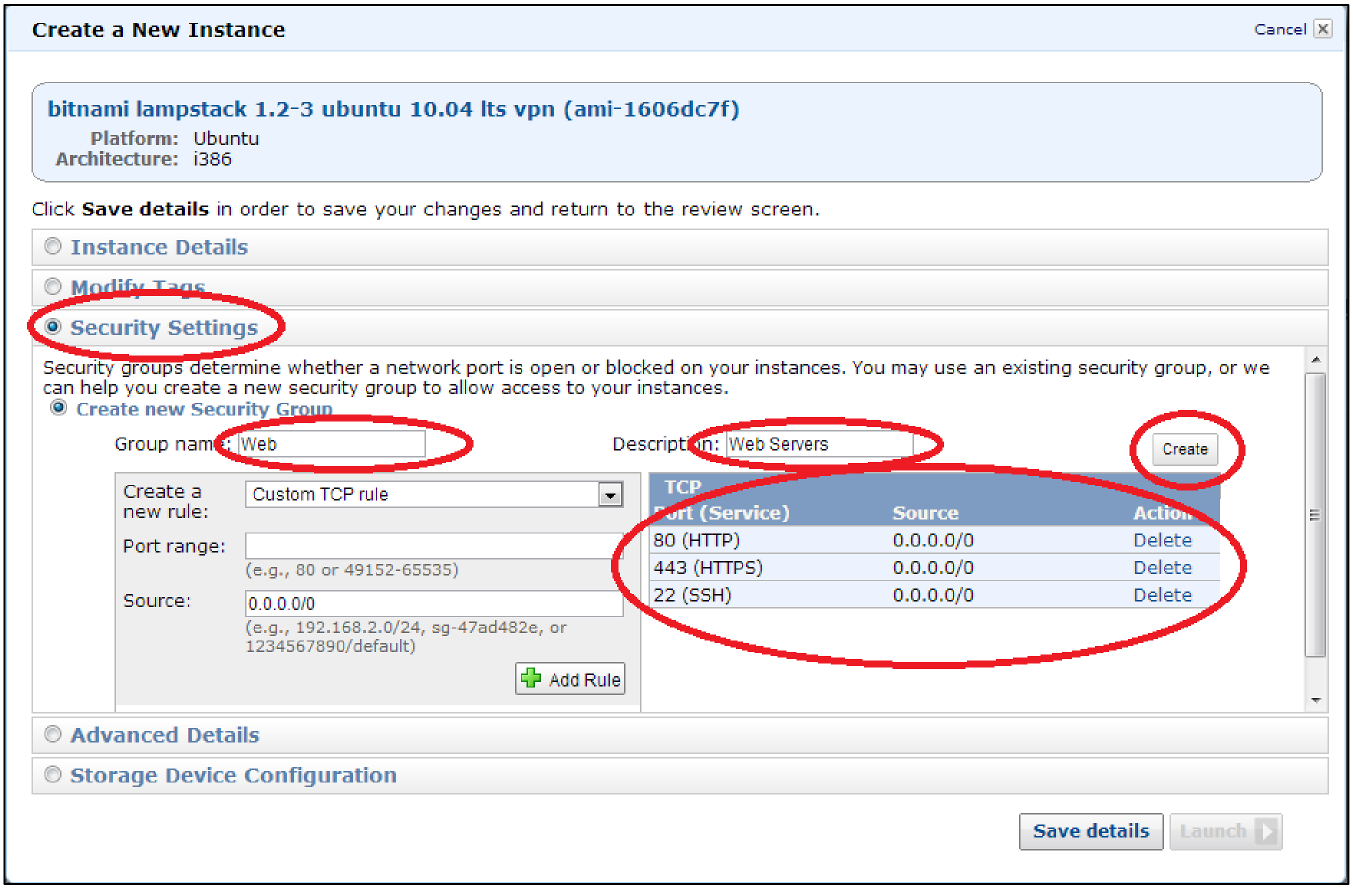
We recommend that you create a custom security group, based on role, instead of "selecting an existing Security Group, which is the default.

Create a new group named "Web", and then add a description.

Next, open inbound access for ports 22, 80, and 443. In real life you should restrict Port 22 access to just your own IP address range, or better yet only allow SSH from a bastion server.

You will need to add each rule, one at a time, which we do not illustrate here. You can choose SSH, HTTP, HTTPS from the dropdown and enter 0.0.0.0/0 in Source.

Click Create.



Create a New Instance

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn (ami-1606dc7f)

Platform: Ubuntu
Architecture: i386

Click **Save details** in order to save your changes and return to the review screen.

○ Instance Details

○ Modify Tags

● Security Settings

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances.

● Create new Security Group

Group name: Web
Description: Web Servers

Create a new rule: Custom TCP rule
Port range:
(e.g., 80 or 49152-65535)
Source: 0.0.0.0/0
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

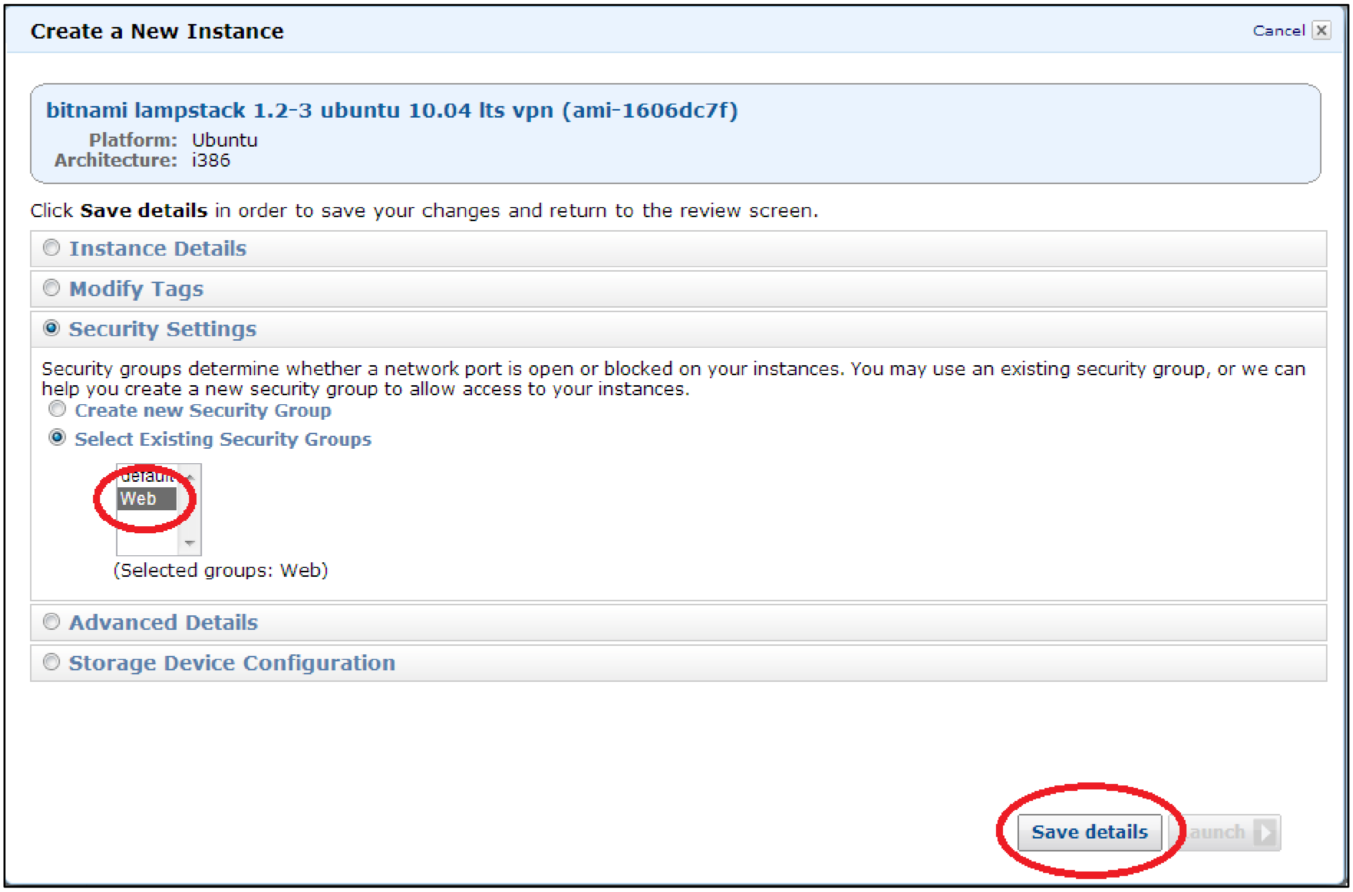
TCP

Port (Service)	Source	Action
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
22 (SSH)	0.0.0.0/0	Delete

○ Advanced Details

○ Storage Device Configuration

Make sure your just created Security Group is selected and click Save Details.



Create a New Instance

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn (ami-1606dc7f)
Platform: Ubuntu
Architecture: i386

Click **Save details** in order to save your changes and return to the review screen.

○ Instance Details

○ Modify Tags

● Security Settings

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances.

○ Create new Security Group

● Select Existing Security Groups

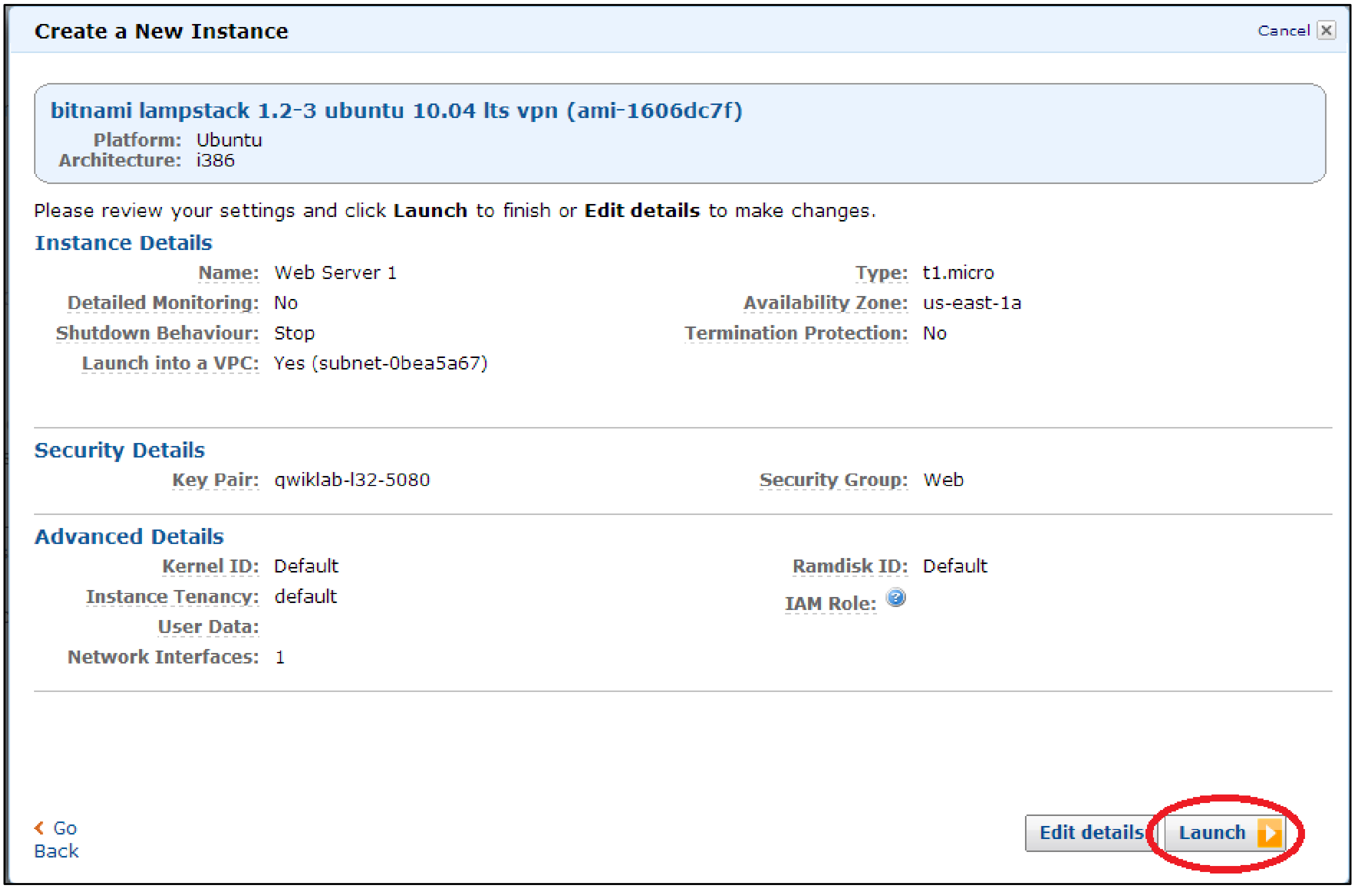
default
Web

(Selected groups: Web)

○ Advanced Details

○ Storage Device Configuration

Click Launch and then Close.



Create a New Instance

bitnami lampstack 1.2-3 ubuntu 10.04 lts vpn (ami-1606dc7f)
Platform: Ubuntu
Architecture: i386

Please review your settings and click **Launch** to finish or **Edit details** to make changes.

Instance Details

Name:	Web Server 1	Type:	t1.micro
Detailed Monitoring:	No	Availability Zone:	us-east-1a
Shutdown Behaviour:	Stop	Termination Protection:	No
Launch into a VPC:	Yes (subnet-0bea5a67)		

Security Details

Key Pair:	qwiklab-l32-5080	Security Group:	Web

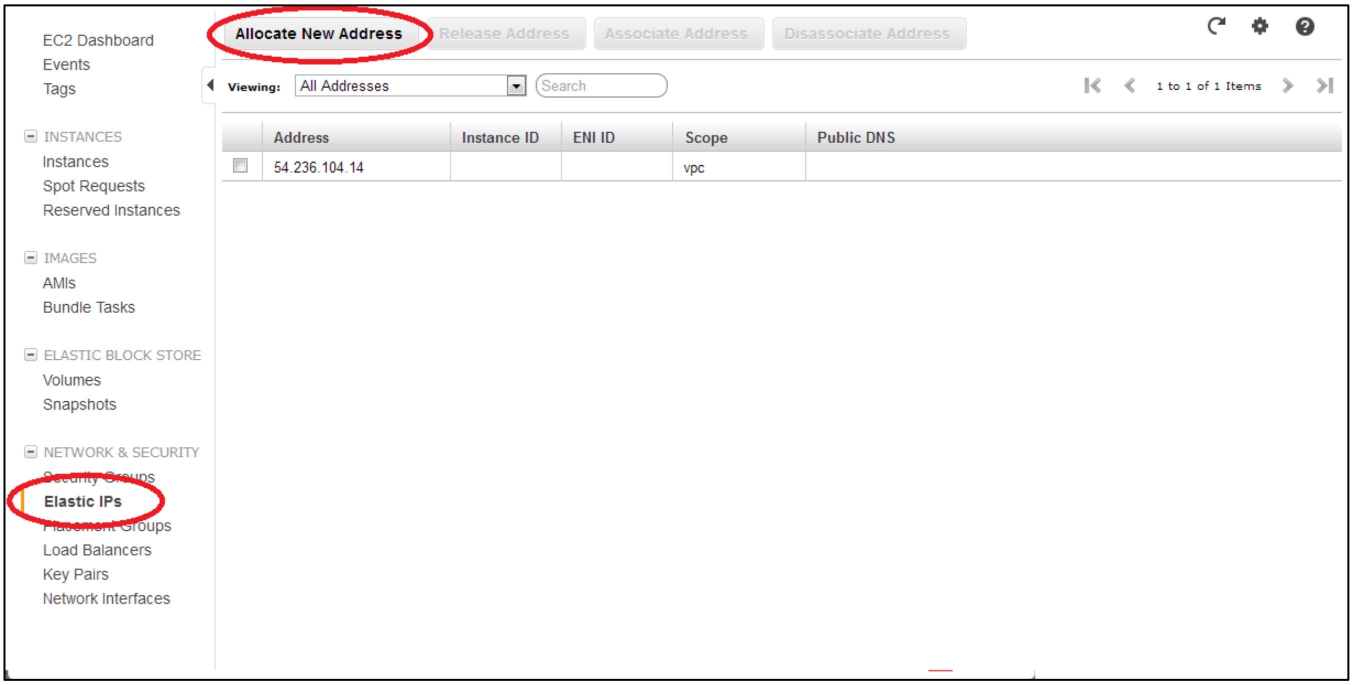
Advanced Details

Kernel ID:	Default	Ramdisk ID:	Default
Instance Tenancy:	default	IAM Role:	
User Data:			
Network Interfaces:	1		

CREATE AND ASSIGN AN ELASTIC IP ADDRESS

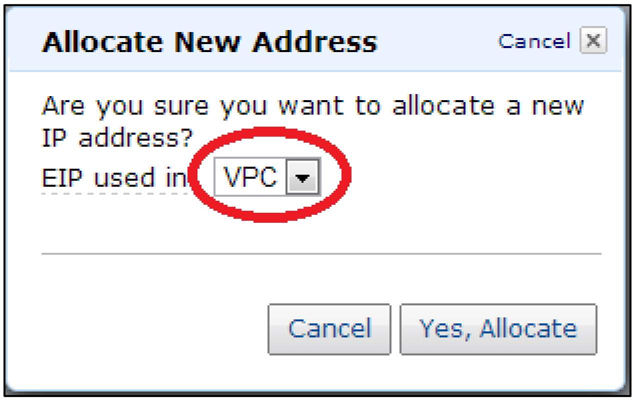
By default instances in the VPC do not have a public IP address. Because this Web server is meant to be public, we need to allocate an Elastic IP address (EIP) and associate it with the server.

In the *Elastic IPs* section of the EC2 Console, click on *Allocate New Address*, and make certain that you allocate one in the VPC.



Viewing: All Addresses

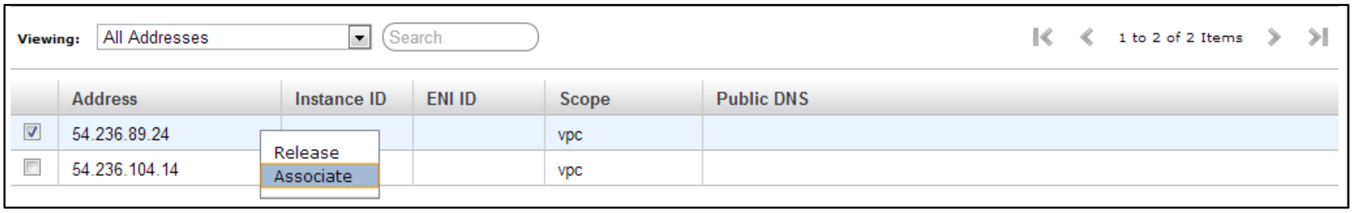
	Address	Instance ID	ENI ID	Scope	Public DNS
□	54.236.104.14			vpc	



Are you sure you want to allocate a new IP address?

EIP used in: VPC

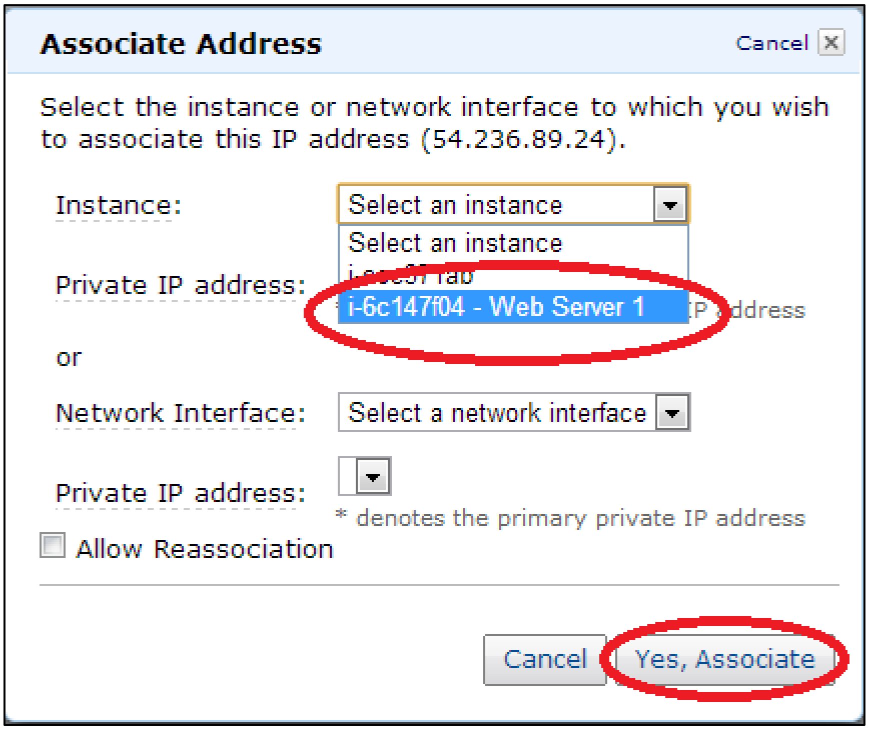
Right-click on the new address and click on Associate.



	Address	Instance ID	ENI ID	Scope	Public DNS
☑	54.236.89.24			vpc	
□	54.236.104.14			vpc	

Select your Web Server 1 Instance. Be certain that you select the appropriate server, because the options below are unlikely to remember what context you are working with.

Make note of this page. Later in the lab exercise you will be asked to do this again, except next time we will not provide screen shots.



Associate Address

Select the instance or network interface to which you wish to associate this IP address (54.236.89.24).

Instance: Select an instance

Private IP address:

or

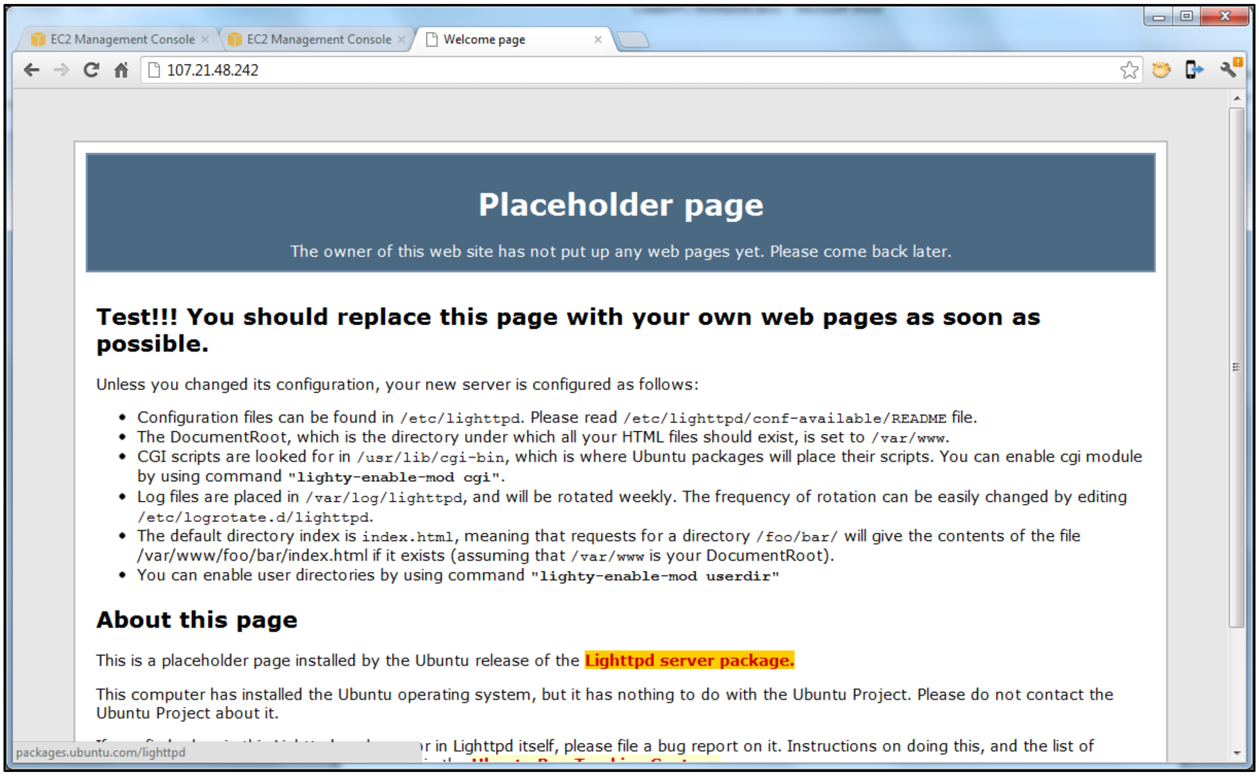
Network Interface: Select a network interface

Private IP address:

* denotes the primary private IP address

□ Allow Reassociation

Try connecting to the Web server from a browser connection by typing the IP address into the page. You will connect to a page similar to the one in this screen shot. We won't modify the Web site, and instead will focus on the network portion of this exercise.



Placeholder page

The owner of this web site has not put up any web pages yet. Please come back later.

Test!!! You should replace this page with your own web pages as soon as possible.

Unless you changed its configuration, your new server is configured as follows:

- Configuration files can be found in `/etc/lighttpd`. Please read `/etc/lighttpd/conf-available/README` file.
- The DocumentRoot, which is the directory under which all your HTML files should exist, is set to `/var/www`.
- CGI scripts are looked for in `/usr/lib/cgi-bin`, which is where Ubuntu packages will place their scripts. You can enable cgi module by using command **"lighty-enable-mod cgi"**.
- Log files are placed in `/var/log/lighttpd`, and will be rotated weekly. The frequency of rotation can be easily changed by editing `/etc/logrotate.d/lighttpd`.
- The default directory index is `index.html`, meaning that requests for a directory `/foo/bar/` will give the contents of the file /var/www/foo/bar/index.html if it exists (assuming that `/var/www` is your DocumentRoot).
- You can enable user directories by using command **"lighty-enable-mod userdir"**

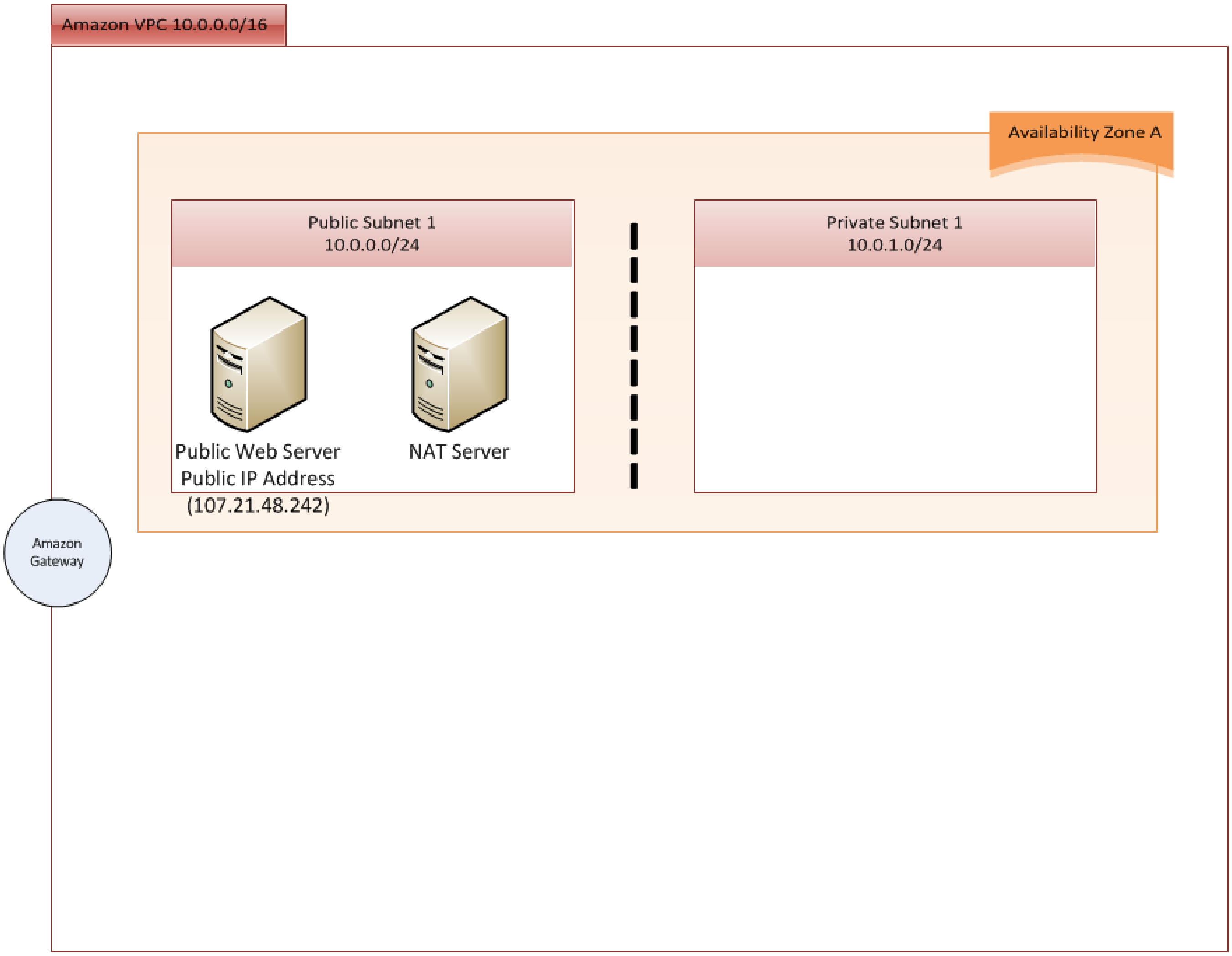
About this page

This is a placeholder page installed by the Ubuntu release of the **Lighttpd server package.**

This computer has installed the Ubuntu operating system, but it has nothing to do with the Ubuntu Project. Please do not contact the Ubuntu Project about it.

r in Lighttpd itself, please file a bug report on it. Instructions on doing this, and the list of

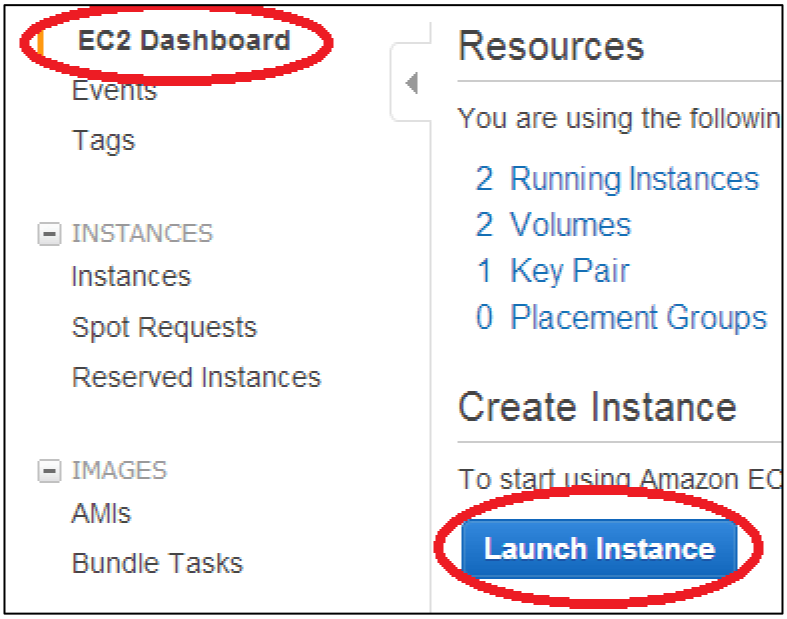
Here are the results so far:



LAUNCH A BACK-END WINDOWS SQL SERVER

Database security is a serious subject. We're going to place our database in a private subnet, tucked away from Internet traffic.

In the EC2 Dashboard part of the AWS Management Console, click on the "Launch Instance" button and choose the Quick Launch Wizard.



Resources

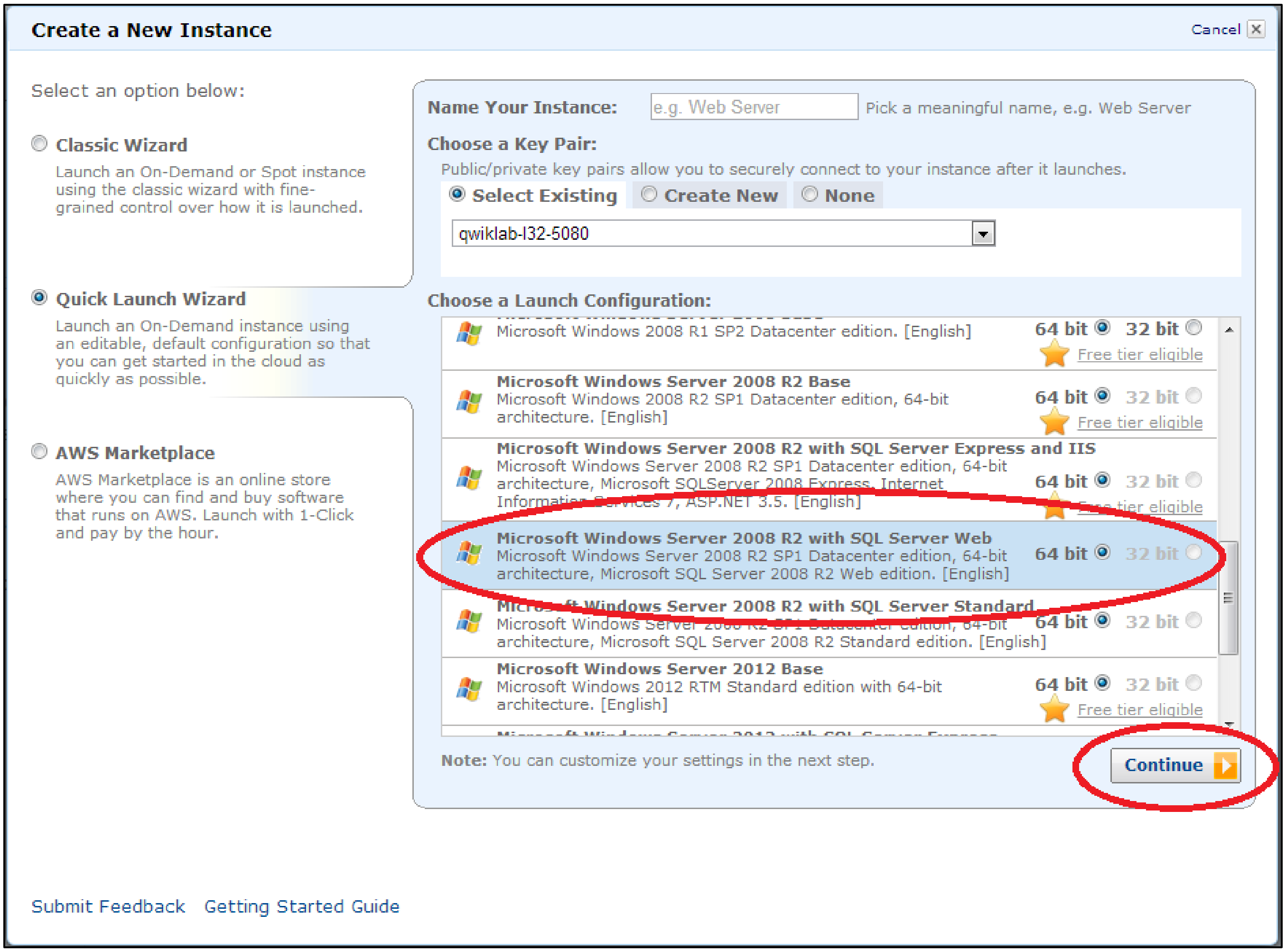
You are using the followin

2 Running Instances
2 Volumes
1 Key Pair
0 Placement Groups

Create Instance

To start using Amazon EC

Then select the Microsoft Windows Server 2008 R2 with SQL Server Web AMI. We won't actually use the database in this lab. Rather, our objective is to create a "pot of gold" in the sense that this server will be reachable via RDP under only a select set of conditions.



Create a New Instance

Select an option below:

○ **Classic Wizard**
Launch an On-Demand or Spot instance using the classic wizard with fine-grained control over how it is launched.

● **Quick Launch Wizard**
Launch an On-Demand instance using an editable, default configuration so that you can get started in the cloud as quickly as possible.

○ **AWS Marketplace**
AWS Marketplace is an online store where you can find and buy software that runs on AWS. Launch with 1-Click and pay by the hour.

Name Your Instance: e.g. Web Server Pick a meaningful name, e.g. Web Server

Choose a Key Pair:
Public/private key pairs allow you to securely connect to your instance after it launches.

● **Select Existing** ○ **Create New** ○ **None**

qwiklab-l32-5080

Choose a Launch Configuration:

Microsoft Windows 2008 R1 SP2 Datacenter edition. [English] — **64 bit** ● **32 bit** ○ Free tier eligible

Microsoft Windows Server 2008 R2 Base
Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English] — **64 bit** ● 32 bit ○ Free tier eligible

Microsoft Windows Server 2008 R2 with SQL Server Express and IIS
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQLServer 2008 Express, Internet Information Services 7, ASP.NET 3.5. [English] — **64 bit** ● 32 bit ○ Free tier eligible

Microsoft Windows Server 2008 R2 with SQL Server Web
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English] — **64 bit** ● 32 bit ○

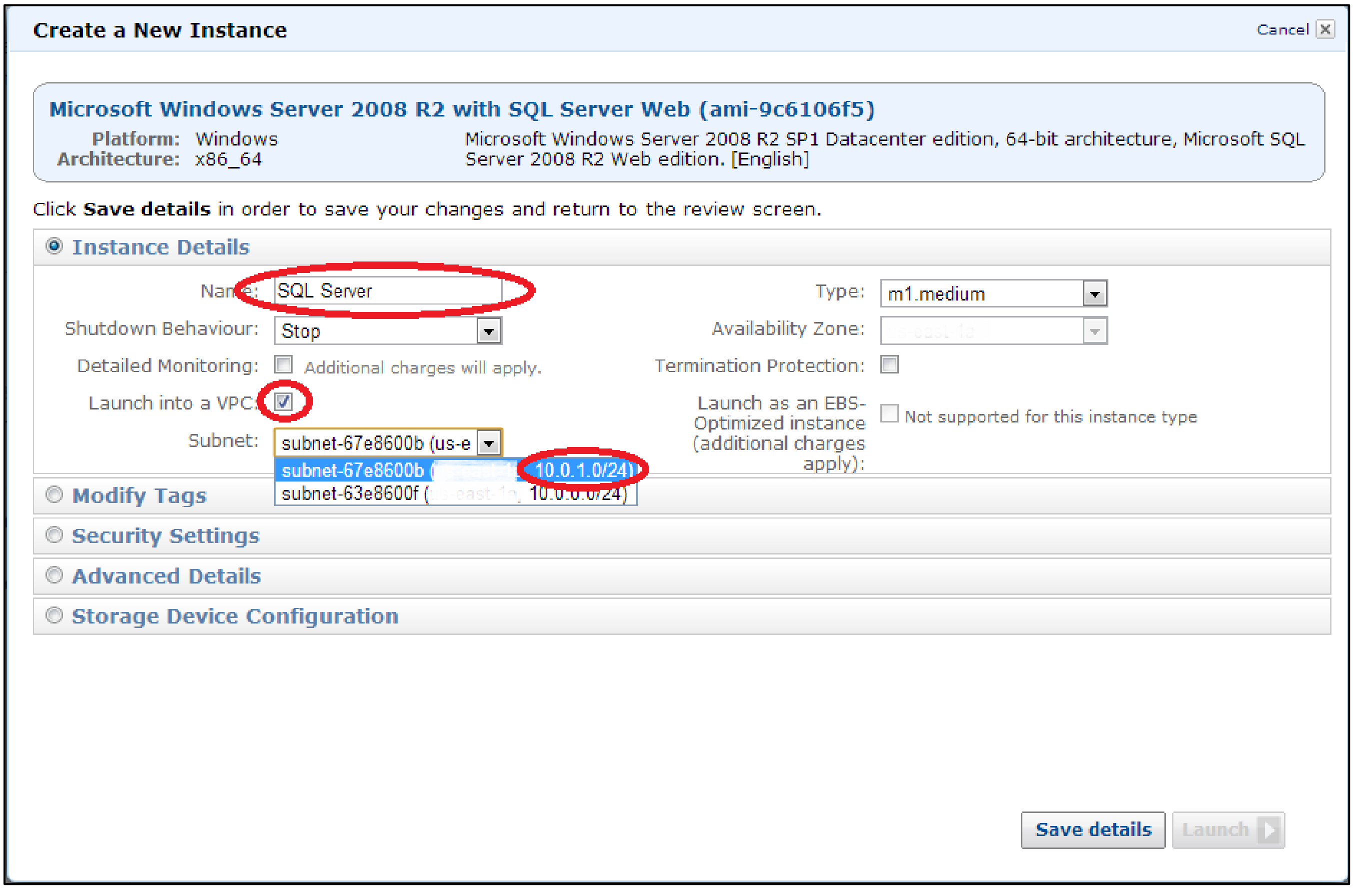
Microsoft Windows Server 2008 R2 with SQL Server Standard
Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Standard edition. [English] — **64 bit** ● 32 bit ○

Microsoft Windows Server 2012 Base
Microsoft Windows 2012 RTM Standard edition with 64-bit architecture. [English] — **64 bit** ● 32 bit ○ Free tier eligible

Note: You can customize your settings in the next step.

Edit the Instance Details.

1. Name the instance SQL Server.
2. Change the instance type to something larger than a t1.micro (we suggest an m1.medium).
3. Select Launch into a VPC
4. Choose 10.0.1.0 as the subnet. This subnet is not reachable directly from the Internet.



Create a New Instance

Microsoft Windows Server 2008 R2 with SQL Server Web (ami-9c6106f5)

Platform: Windows
Architecture: x86_64

Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English]

Click **Save details** in order to save your changes and return to the review screen.

● **Instance Details**

Name: SQL Server

Shutdown Behaviour: Stop

Detailed Monitoring: □ Additional charges will apply.

Launch into a VPC: ☑

Subnet: subnet-67e8600b (us-e

subnet-67e8600b ([redacted] 10.0.1.0/24)

subnet-63e8600f ([redacted] 10.0.0.0/24)

Type: m1.medium

Availability Zone: [redacted]

Termination Protection: □

Launch as an EBS-Optimized instance (additional charges apply): □ Not supported for this instance type

○ **Modify Tags**

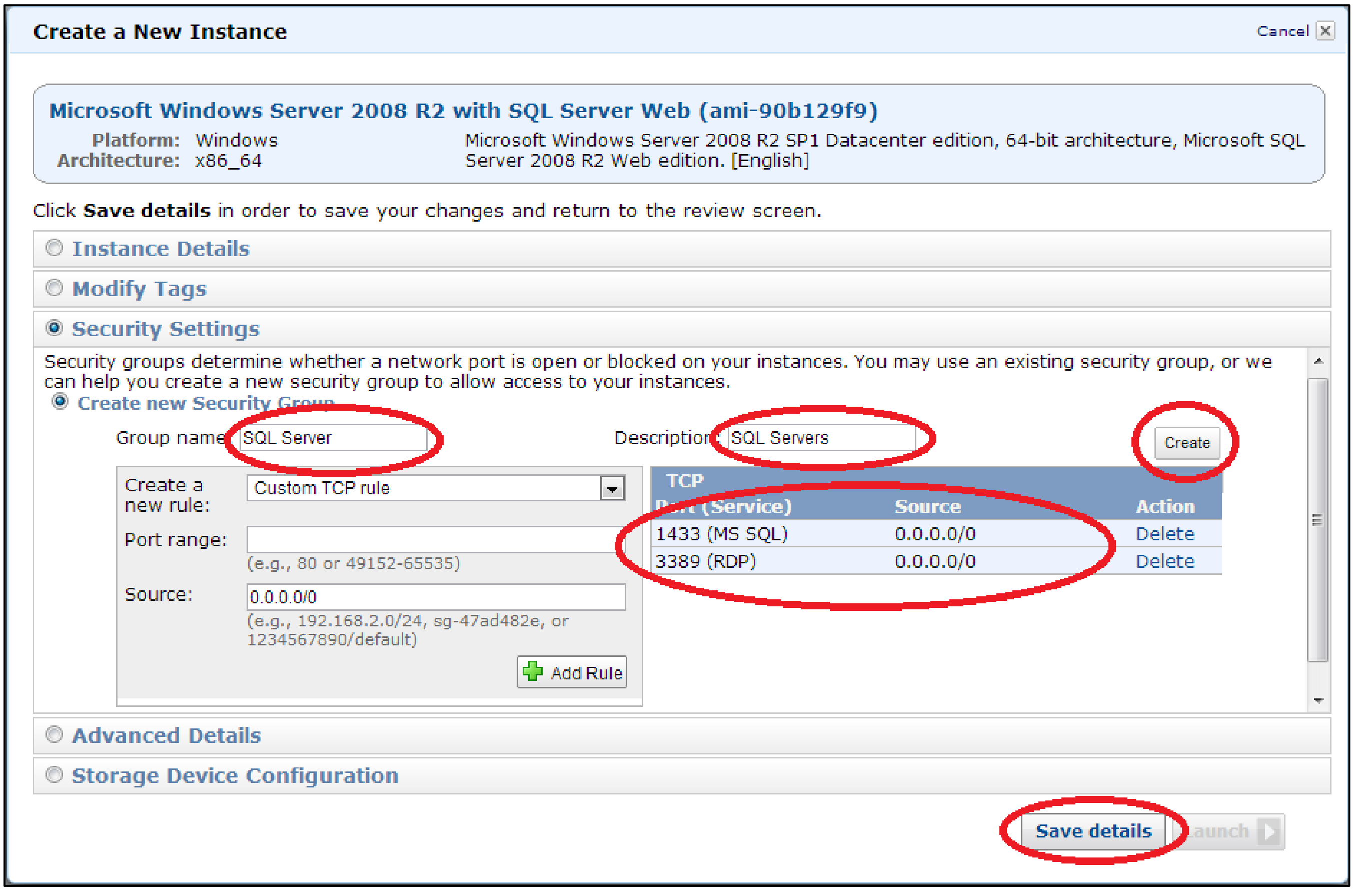
○ **Security Settings**

○ **Advanced Details**

○ **Storage Device Configuration**

Click on Security Settings and then Create new Security Group. Change the name of the security group to SQLServer (no spaces in names) and add a Description.

Note that the source IP address range says 0.0.0.0/0, which means "from anywhere". In fact, the routing restrictions translate this meaning into "from any host, as long as it is on one of the VPC subnets". We'll tighten this rule in a few minutes, once the Bastion Server is created.



Microsoft Windows Server 2008 R2 with SQL Server Web (ami-90b129f9)

Platform: Windows
Architecture: x86_64

Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English]

Click **Save details** in order to save your changes and return to the review screen.

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances.

● Create new Security Group

Group name: SQL Server

Description: SQL Servers

Create a new rule: Custom TCP rule

Port range:
(e.g., 80 or 49152-65535)

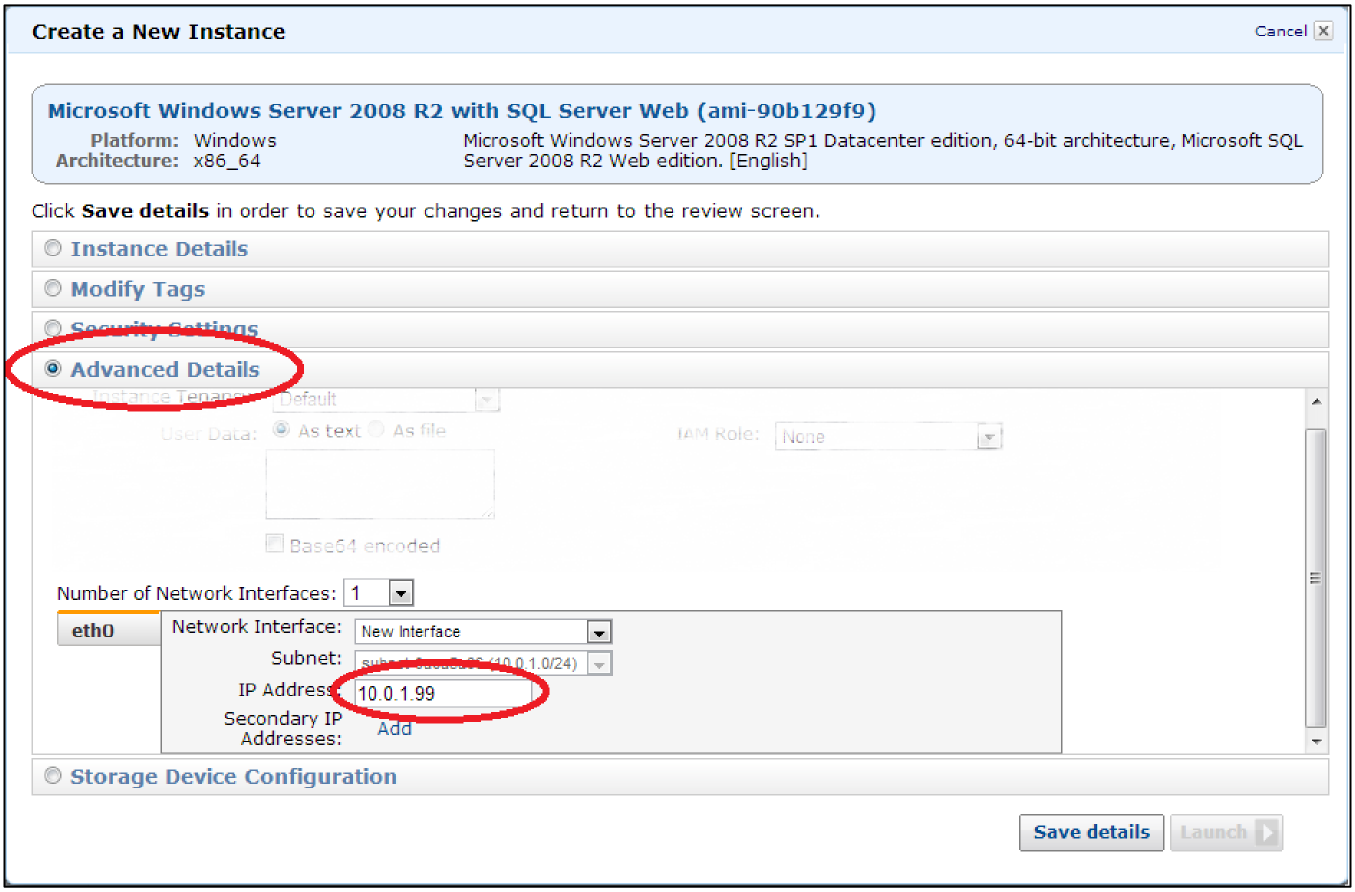
Source: 0.0.0.0/0
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

TCP Port (Service)	Source	Action
1433 (MS SQL)	0.0.0.0/0	Delete
3389 (RDP)	0.0.0.0/0	Delete

Select the just created SQLServer Security Group and click Save details. Do not click the Launch button.

Click Edit details again There will be additional options under Advanced Details.

In Advanced Details for the instance specify 10.0.1.99 as the address for this server.



Create a New Instance

Microsoft Windows Server 2008 R2 with SQL Server Web (ami-90b129f9)

Platform: Windows
Architecture: x86_64

Microsoft Windows Server 2008 R2 SP1 Datacenter edition, 64-bit architecture, Microsoft SQL Server 2008 R2 Web edition. [English]

Click **Save details** in order to save your changes and return to the review screen.

○ Instance Details
○ Modify Tags
○ Security Settings
● Advanced Details

Instance Tenancy: Default
User Data: ● As text ○ As file
□ Base64 encoded
IAM Role: None

Number of Network Interfaces: 1

eth0
Network Interface: New Interface
Subnet: subnet-[illegible] (10.0.1.0/24)
IP Address: 10.0.1.99
Secondary IP Addresses: Add

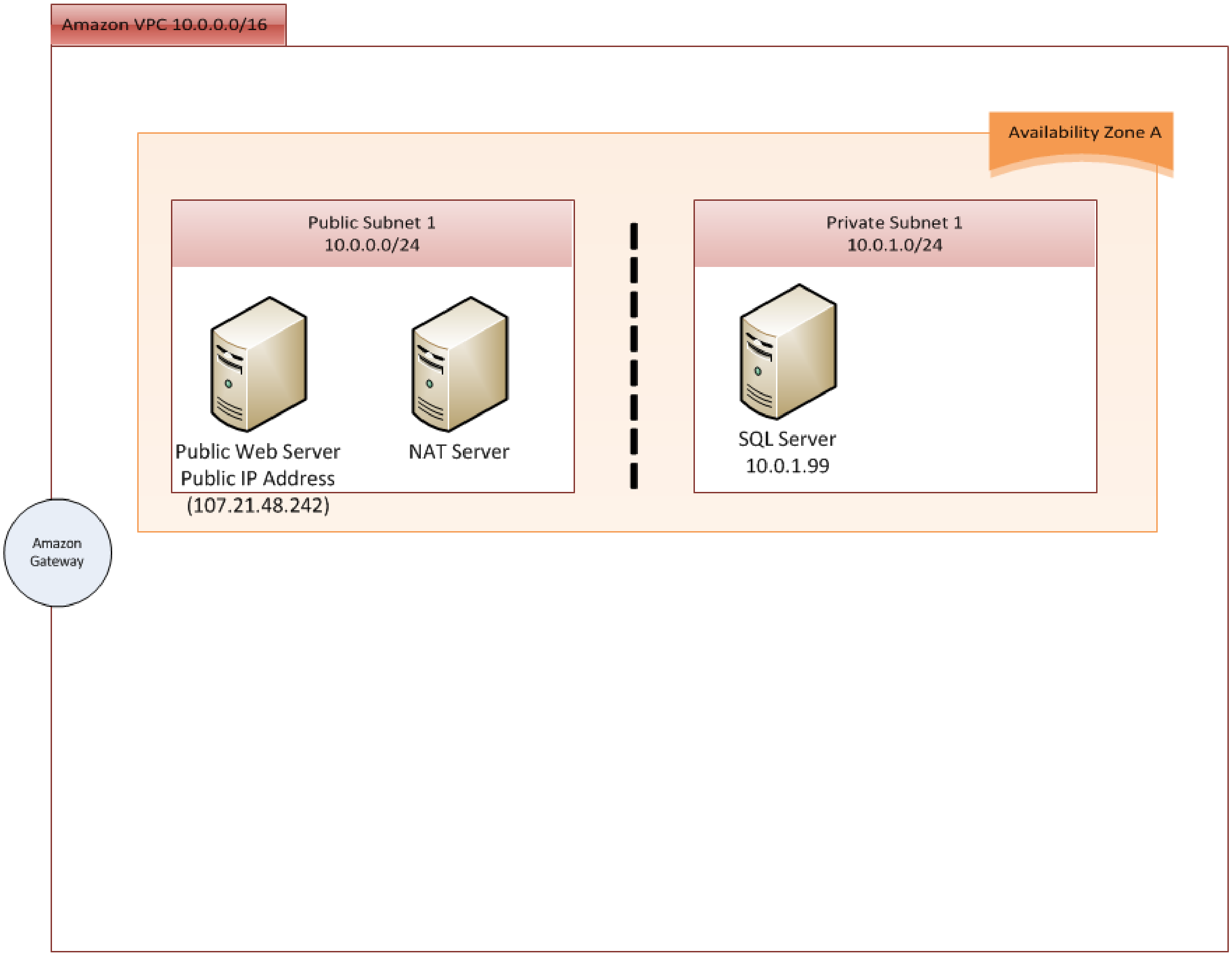
○ Storage Device Configuration

Click Save details and then Launch.

Our network now looks like the diagram below. It's still short of production ready, because the database is not set up to serve the Web server, and we still need a secure way to connect to and administer the SQL Server. However The NAT server stands ready to act as a router that allows the SQL Server to make outbound calls to the Internet in order to download Windows Updates, etc.

There is one other very important thing missing from our environment: a second Availability Zone with another Web server and a second database server in it. AWS provides you access to multiple Availability Zones (data centers) at no additional cost to you. A best practice is to mirror servers across two zones, and then use load balancing and other techniques in order to distribute traffic between them.

AWS considers multi-AZ deployments to be essential to your welfare, because data centers go offline from time to time. Our data centers are more reliable than typical Enterprise data centers; however the fact remains that outages happen. Note that if your application environment is in a single AZ, there is no SLA protection for you. **The EC2 SLA kicks in only if two or more Availbility Zones in an AWS Region go offline at the same time.**

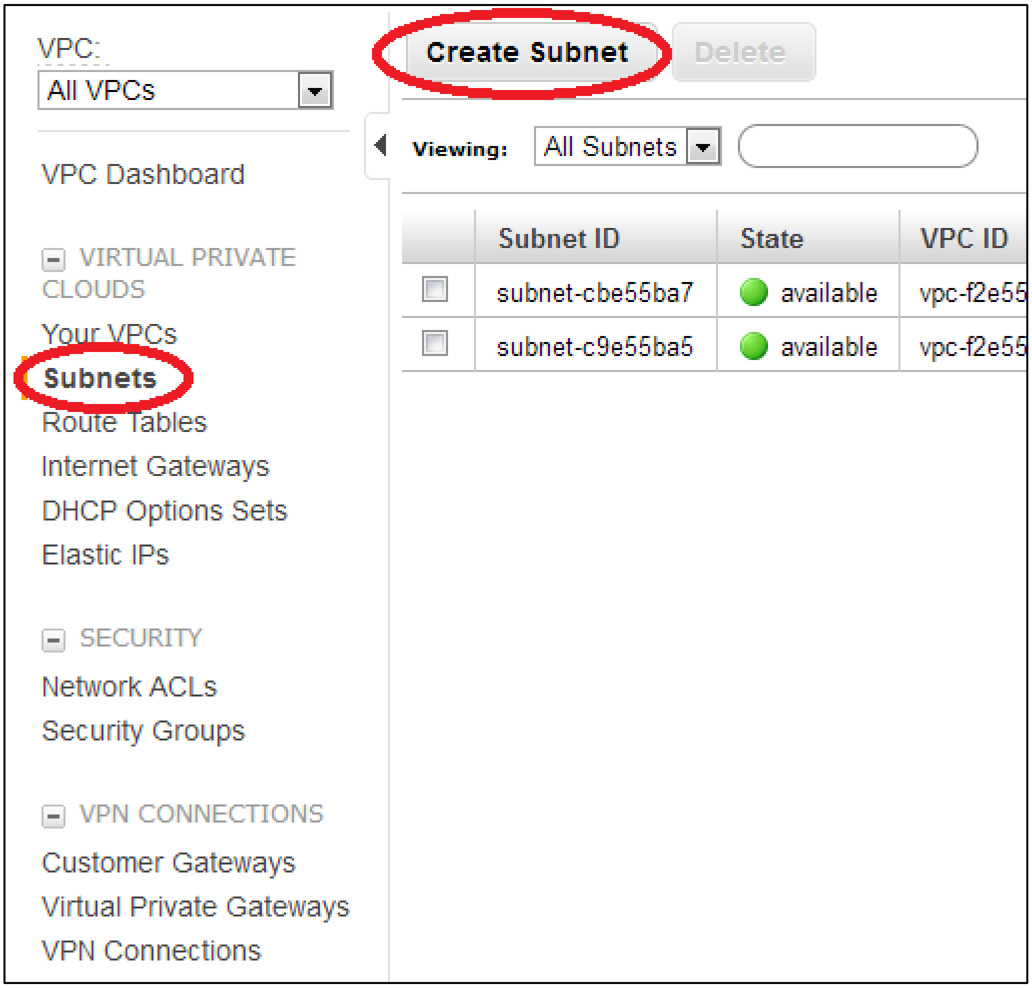


CREATE TWO MORE SUBNETS

We need to create a public subnet, and also a private subnet in another Availability Zone. Unlike the previous subnets, we'll create these without the assistance of a wizard. Along the way we'll learn a bit more about how they operate.

MANUALLY CREATE EACH SUBNET

Back in the VPC section of the management console, click "Create Subnet".

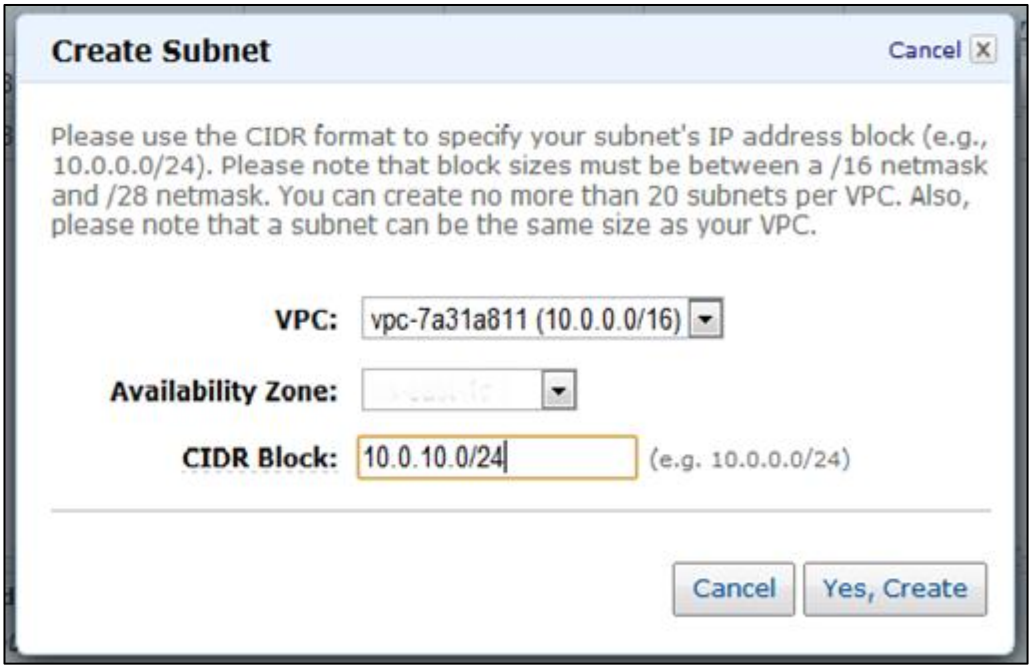


VPC: All VPCs

Viewing: All Subnets

	Subnet ID	State	VPC ID
□	subnet-cbe55ba7	● available	vpc-f2e55
□	subnet-c9e55ba5	● available	vpc-f2e55

To review, the original subnets were 10.0.0.0/24 (public), and 10.0.1.0/24 (private). Both were in the same Availability Zone. We will use 10.0.10.0/24 (public), and 10.0.11.0/24 (private) for these subnets. These will be in the same Availability Zone as each other but in a different Availability Zone from the first two you created.



Create Subnet

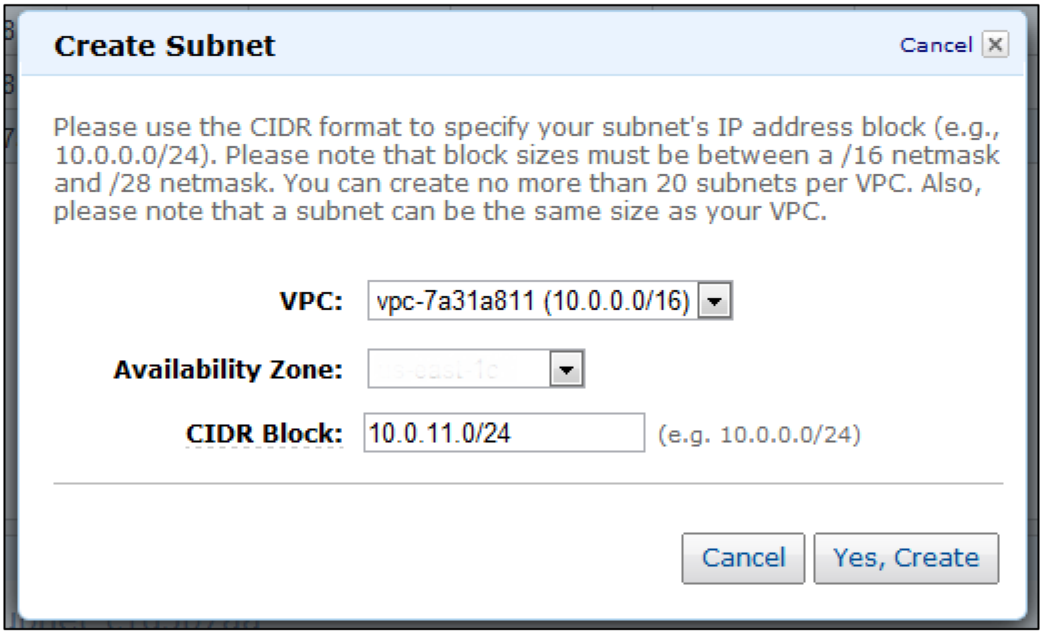
Please use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Please note that block sizes must be between a /16 netmask and /28 netmask. You can create no more than 20 subnets per VPC. Also, please note that a subnet can be the same size as your VPC.

VPC: vpc-7a31a811 (10.0.0.0/16)

Availability Zone: us-east-1c

CIDR Block: 10.0.10.0/24 (e.g. 10.0.0.0/24)

Repeat for 10.0.11.0/24



Create Subnet

Please use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Please note that block sizes must be between a /16 netmask and /28 netmask. You can create no more than 20 subnets per VPC. Also, please note that a subnet can be the same size as your VPC.

VPC: vpc-7a31a811 (10.0.0.0/16)

Availability Zone: us-east-1c

CIDR Block: 10.0.11.0/24 (e.g. 10.0.0.0/24)

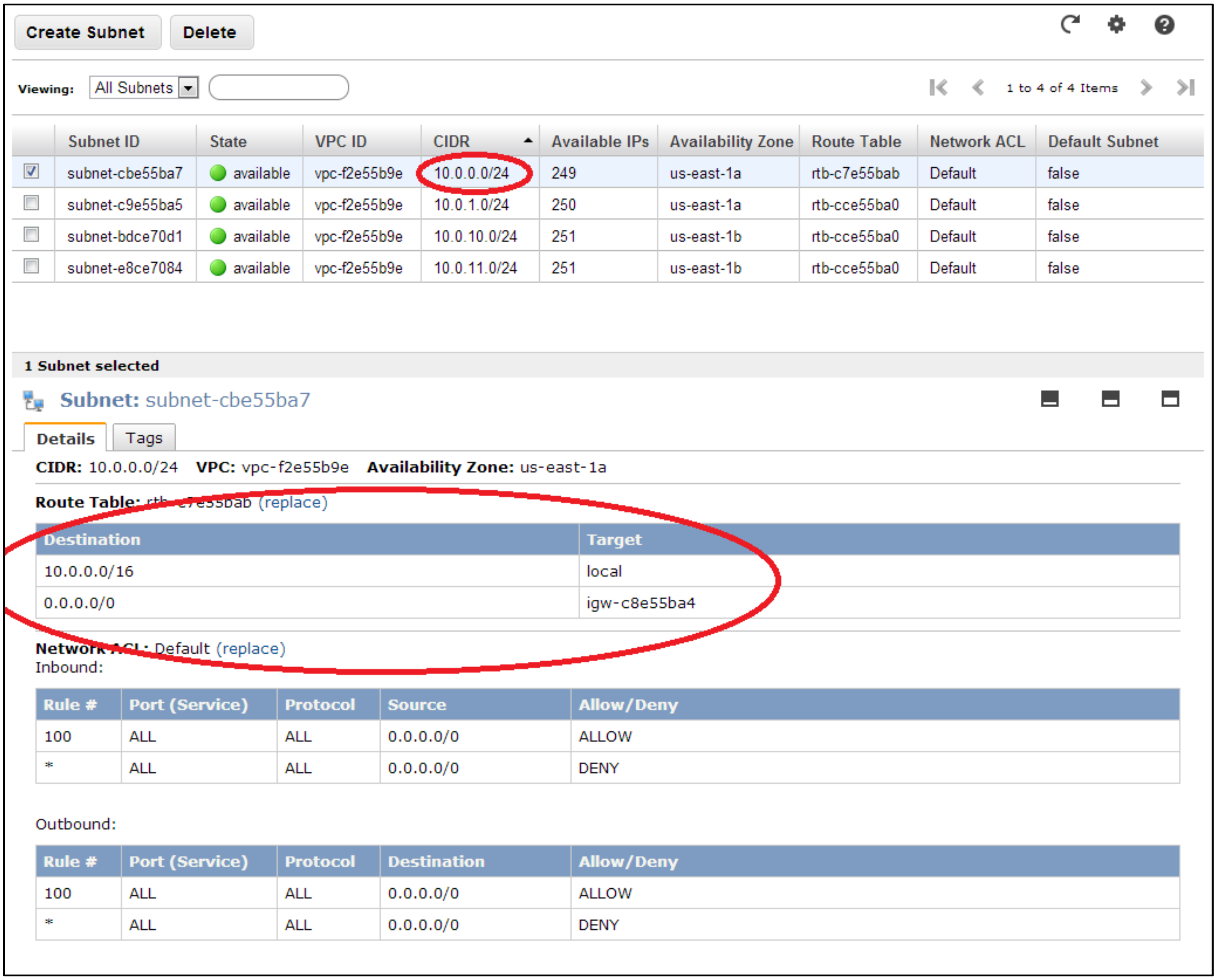
WHAT DETERMINES WHETHER A SUBNET IS PUBLIC OR PRIVATE?

Now we have two more subnets, but what makes them private or public? It's the routing rules.

Select 10.0.0.0/24, and note that there are two routing rules in the Route Table:

- Any machine in this subnet can communicate with any other machine in 10.0.0.0/16, which is the entire VPC In other words, communication between all subnets is wide open. Later in this lab we'll look at security groups as a mechanism to restrict traffic.
- Any traffic to/from the Internet (0.0.0.0/0) will be routed thru the Internet Gateway device. We have not looked at that device so far, but think of it as a router on the edge of our VPC. In fact, that's how its depicted in the network diagrams.

Scroll down and you will see some Network ACLs, which in theory could also control traffic. However the VPC supports a limited number of rules so we will use alternate controls that are even more granular.



☐	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
☑	subnet-cbe55ba7	● available	vpc-f2e55b9e	10.0.0.0/24	249	us-east-1a	rtb-c7e55bab	Default	false
☐	subnet-c9e55ba5	● available	vpc-f2e55b9e	10.0.1.0/24	250	us-east-1a	rtb-cce55ba0	Default	false
☐	subnet-bdce70d1	● available	vpc-f2e55b9e	10.0.10.0/24	251	us-east-1b	rtb-cce55ba0	Default	false
☐	subnet-e8ce7084	● available	vpc-f2e55b9e	10.0.11.0/24	251	us-east-1b	rtb-cce55ba0	Default	false

1 Subnet selected

Subnet: subnet-cbe55ba7

CIDR: 10.0.0.0/24 **VPC:** vpc-f2e55b9e **Availability Zone:** us-east-1a

Route Table: rtb-c7e55bab (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-c8e55ba4

Network ACL: Default (replace)

Inbound:

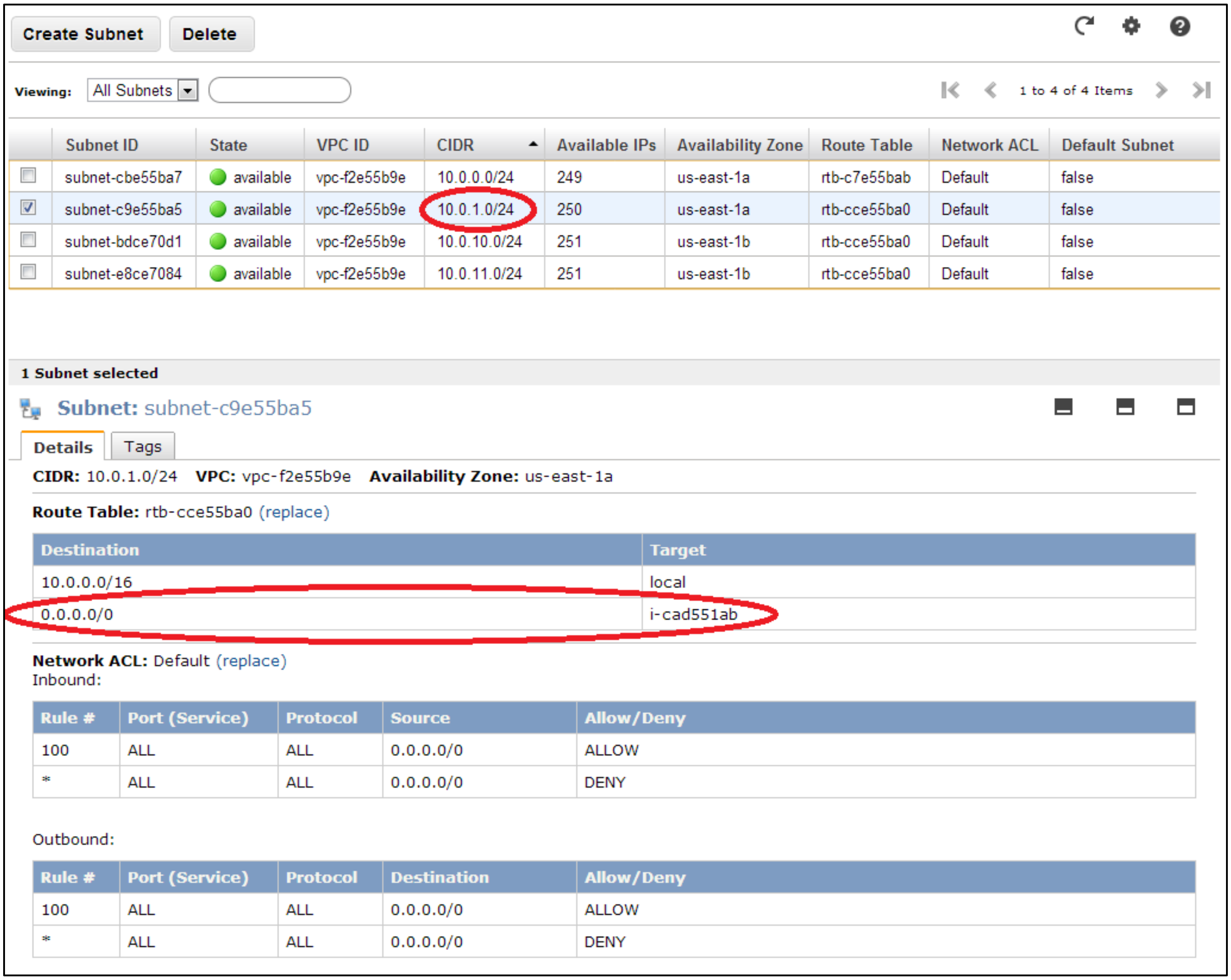
Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

In a similar manner 10.0.1.0/24 also has routing rules:

- Traffic bound for any other subnet in the VPC (10.0.0.0/16) is unrestricted.
- Traffic destined for the Internet will flow to the EC2 Instance, which is the Instance performing NAT. Note that the NAT will not route random requests from the Internet back into this subnet though. It will only route replies made in response to outbound requests from inside this subnet.



	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
☐	subnet-cbe55ba7	● available	vpc-f2e55b9e	10.0.0.0/24	249	us-east-1a	rtb-c7e55bab	Default	false
☑	subnet-c9e55ba5	● available	vpc-f2e55b9e	10.0.1.0/24	250	us-east-1a	rtb-cce55ba0	Default	false
☐	subnet-bdce70d1	● available	vpc-f2e55b9e	10.0.10.0/24	251	us-east-1b	rtb-cce55ba0	Default	false
☐	subnet-e8ce7084	● available	vpc-f2e55b9e	10.0.11.0/24	251	us-east-1b	rtb-cce55ba0	Default	false

1 Subnet selected

Subnet: subnet-c9e55ba5

Details Tags

CIDR: 10.0.1.0/24 **VPC:** vpc-f2e55b9e **Availability Zone:** us-east-1a

Route Table: rtb-cce55ba0 (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	i-cad551ab

Network ACL: Default (replace)
Inbound:

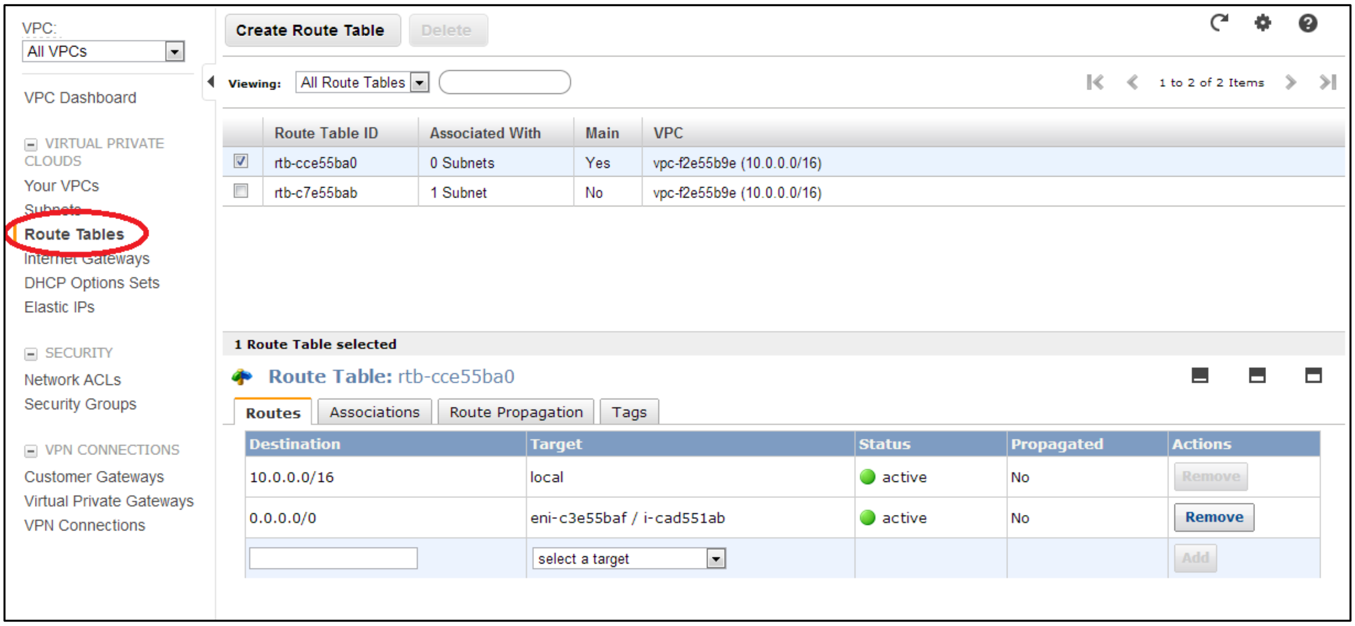
Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Let's switch over to the Route Tables view (route table from the left menu) and look at this from the other side. What's up? According to this view, only 1 subnet is associated with any routing rule at all, but we have a total of 4 subnets!

The Amazon VPC operates on a "safety first" principle. Note that one of the rule sets is marked "main". If a subnet is not explicitly associated with a routing ruleset, it uses the Main ruleset, which happens to be the ruleset that does not talk to the Internet. **So by default, no subnet is able to communicate with the Internet** (unless you switch the default.)



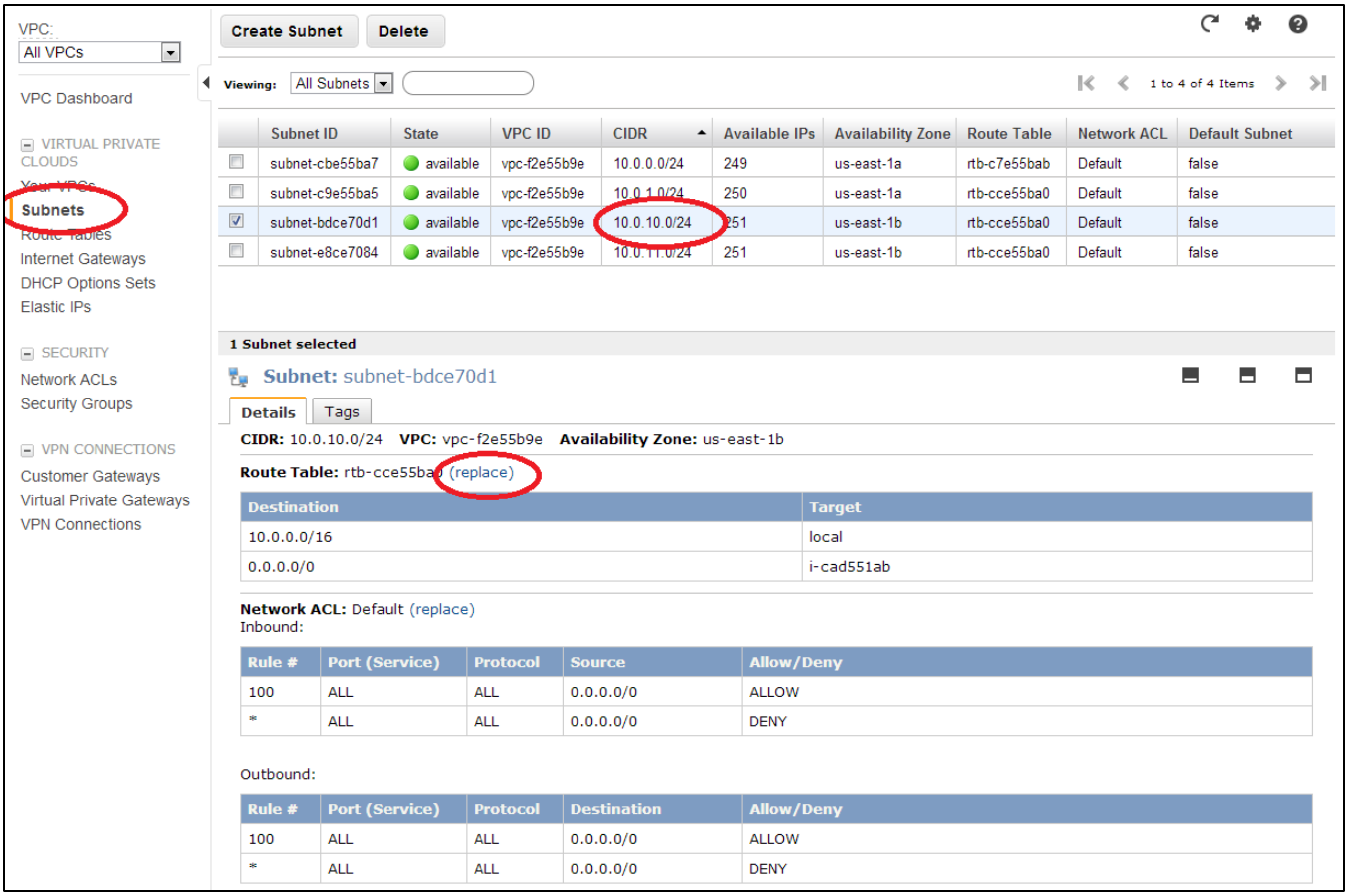
	Route Table ID	Associated With	Main	VPC
☑	rtb-cce55ba0	0 Subnets	Yes	vpc-f2e55b9e (10.0.0.0/16)
□	rtb-c7e55bab	1 Subnet	No	vpc-f2e55b9e (10.0.0.0/16)

1 Route Table selected

Route Table: rtb-cce55ba0

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	● active	No	Remove
0.0.0.0/0	eni-c3e55baf / i-cad551ab	● active	No	Remove
	select a target			Add

We need to associate the new public subnet (10.0.10.0/24) with the routing ruleset that routes bi-directionally to the Internet. Return to Subnets and Select the 10.0.10.0/24 subnet and replace the ruleset.



	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL	Default Subnet
☐	subnet-cbe55ba7	● available	vpc-f2e55b9e	10.0.0.0/24	249	us-east-1a	rtb-c7e55bab	Default	false
☐	subnet-c9e55ba5	● available	vpc-f2e55b9e	10.0.1.0/24	250	us-east-1a	rtb-cce55ba0	Default	false
☑	subnet-bdce70d1	● available	vpc-f2e55b9e	10.0.10.0/24	251	us-east-1b	rtb-cce55ba0	Default	false
☐	subnet-e8ce7084	● available	vpc-f2e55b9e	10.0.11.0/24	251	us-east-1b	rtb-cce55ba0	Default	false

1 Subnet selected

Subnet: subnet-bdce70d1

CIDR: 10.0.10.0/24 **VPC:** vpc-f2e55b9e **Availability Zone:** us-east-1b

Route Table: rtb-cce55ba0 (replace)

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	i-cad551ab

Network ACL: Default (replace)

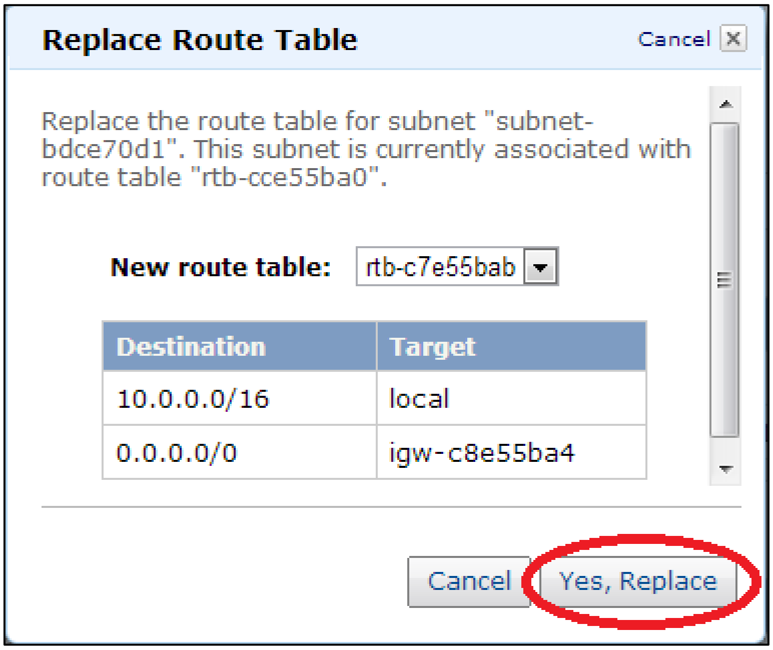
Inbound:

Rule #	Port (Service)	Protocol	Source	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

Outbound:

Rule #	Port (Service)	Protocol	Destination	Allow/Deny
100	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL	ALL	0.0.0.0/0	DENY

There is only one choice in the drop-down list because the console is smart enough to know that you don't want to replace the current routing rules with…..the current routing rules. Click Yes, Replace.

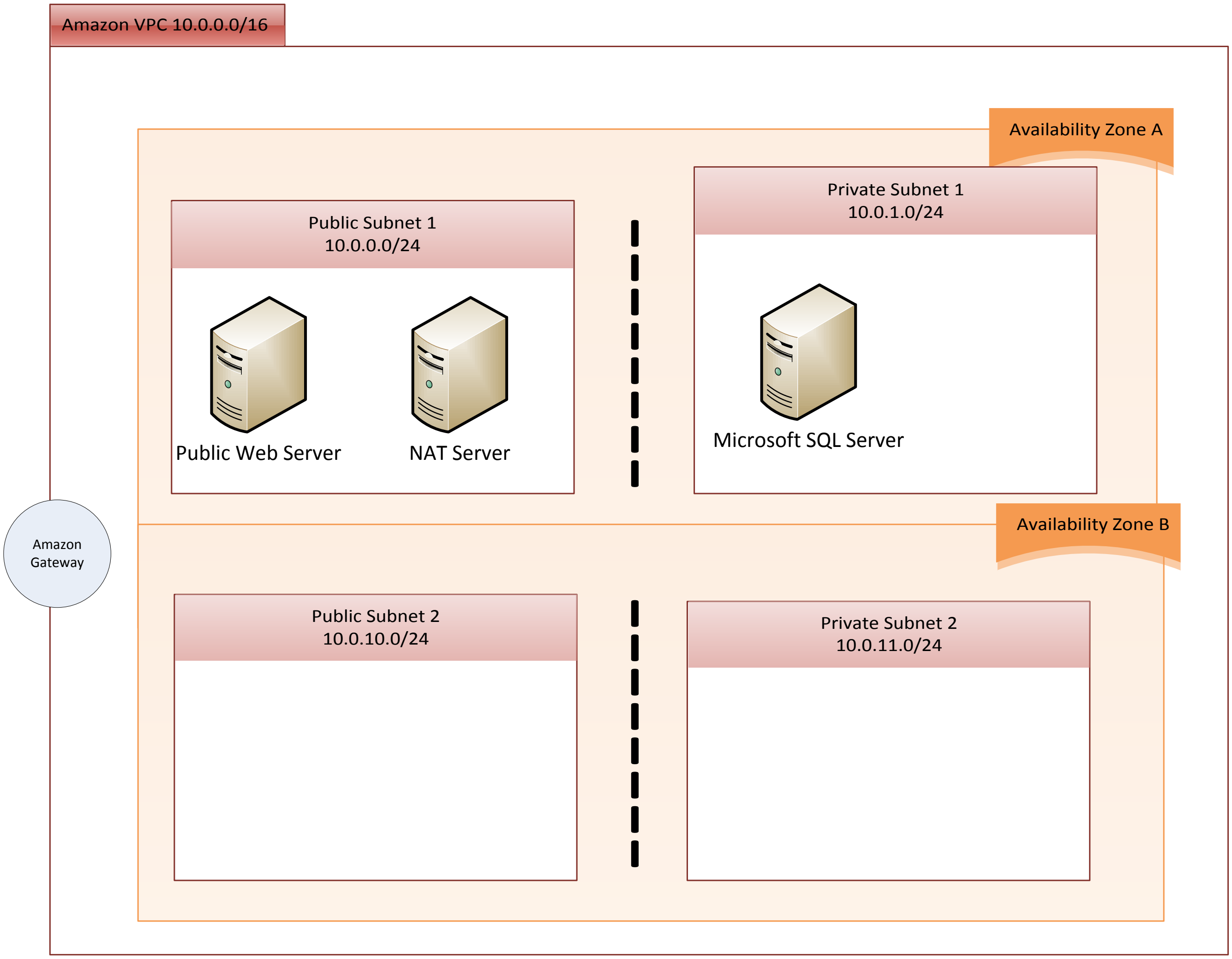


Replace the route table for subnet "subnet-bdce70d1". This subnet is currently associated with route table "rtb-cce55ba0".

New route table: rtb-c7e55bab

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-c8e55ba4

Here's the state of our VPC:



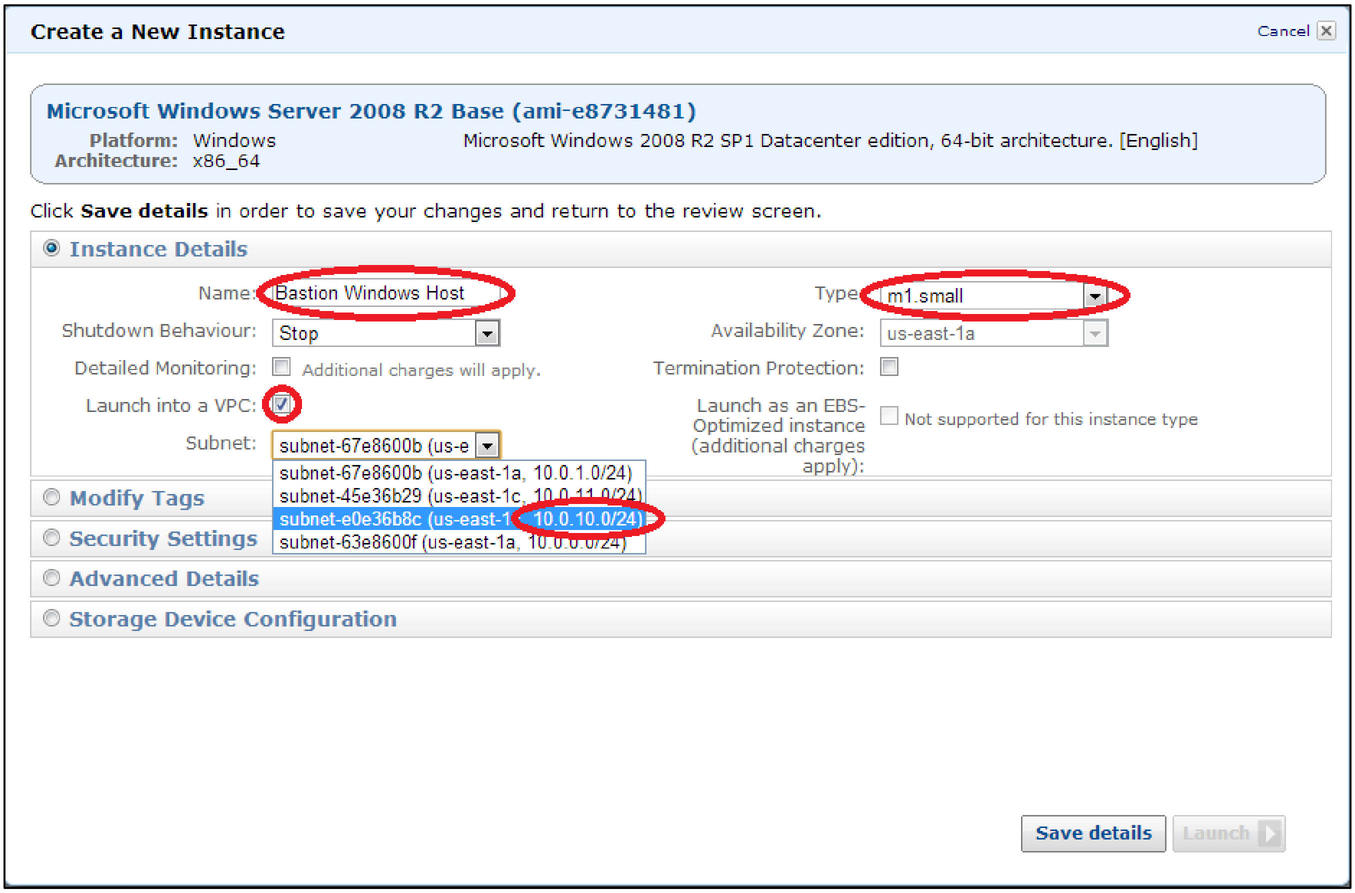
LAUNCH A BASTION WINDOWS HOST

Wikipedia's definition of a Bastion Host is "a special purpose computer on a network specifically designed and configured to withstand attacks. The computer generally hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers."

We're going to launch ours in the new public subnet, although the original public subnet would work just as well.

Back in the VPC Dashboard use the Launch EC2 Instances button to take you to the EC2 Instances section of the EC2 console. Click on Launch Instance and choose the **Windows Server 2008 R2 Base** AMI and name the Instance **Bastion Windows Host**.

Launch it into 10.0.10.0/24 as an m1.small instance.



Create a New Instance

Microsoft Windows Server 2008 R2 Base (ami-e8731481)

Platform: Windows
Architecture: x86_64

Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English]

Click **Save details** in order to save your changes and return to the review screen.

● **Instance Details**

Name: Bastion Windows Host
Shutdown Behaviour: Stop
Detailed Monitoring: □ Additional charges will apply.
Launch into a VPC: ☑
Subnet: subnet-67e8600b (us-e

subnet-67e8600b (us-east-1a, 10.0.1.0/24)
subnet-45e36b29 (us-east-1c, 10.0.11.0/24)
subnet-e0e36b8c (us-east-1 10.0.10.0/24)
subnet-63e8600f (us-east-1a, 10.0.0.0/24)

Type: m1.small
Availability Zone: us-east-1a
Termination Protection: □
Launch as an EBS-Optimized instance (additional charges apply): □ Not supported for this instance type

○ **Modify Tags**

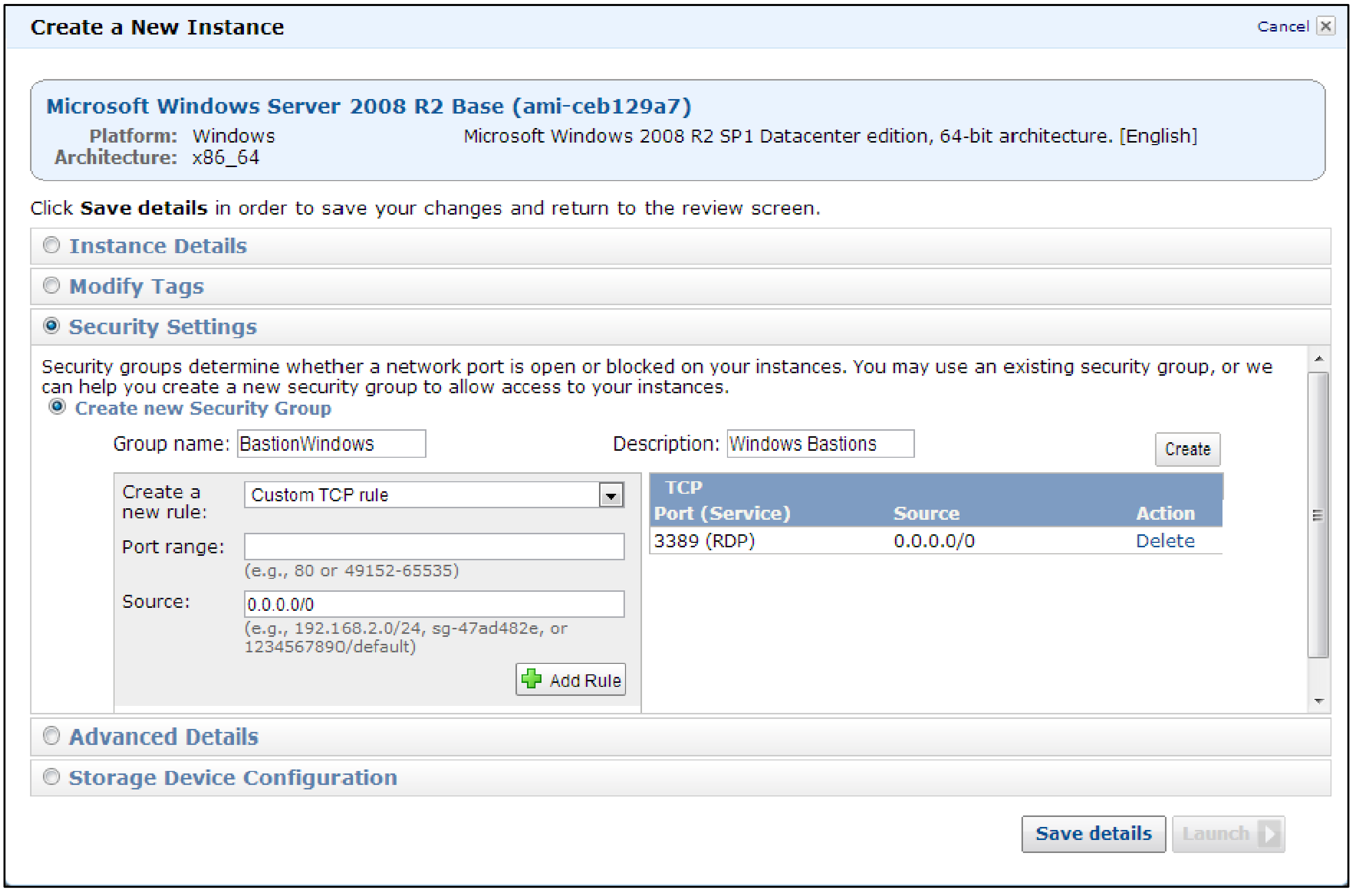
○ **Security Settings**

○ **Advanced Details**

○ **Storage Device Configuration**

There's no need to set a fixed IP address this time.

Create another new security group, named **BastionWindows**. We are only allowing access to port 3389, which is the Windows Remote Desktop Protocol (RDP). For this lab we are allowing access from any IP address on the Internet. In real life you will want to restrict access to the address ranges required for administration.



Create a New Instance

Microsoft Windows Server 2008 R2 Base (ami-ceb129a7)

Platform: Windows
Architecture: x86_64

Microsoft Windows 2008 R2 SP1 Datacenter edition, 64-bit architecture. [English]

Click **Save details** in order to save your changes and return to the review screen.

○ Instance Details

○ Modify Tags

● Security Settings

Security groups determine whether a network port is open or blocked on your instances. You may use an existing security group, or we can help you create a new security group to allow access to your instances.

● Create new Security Group

Group name: BastionWindows

Description: Windows Bastions

Create a new rule: Custom TCP rule

Port range:

(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0

(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

TCP Port (Service)	Source	Action
3389 (RDP)	0.0.0.0/0	Delete

○ Advanced Details

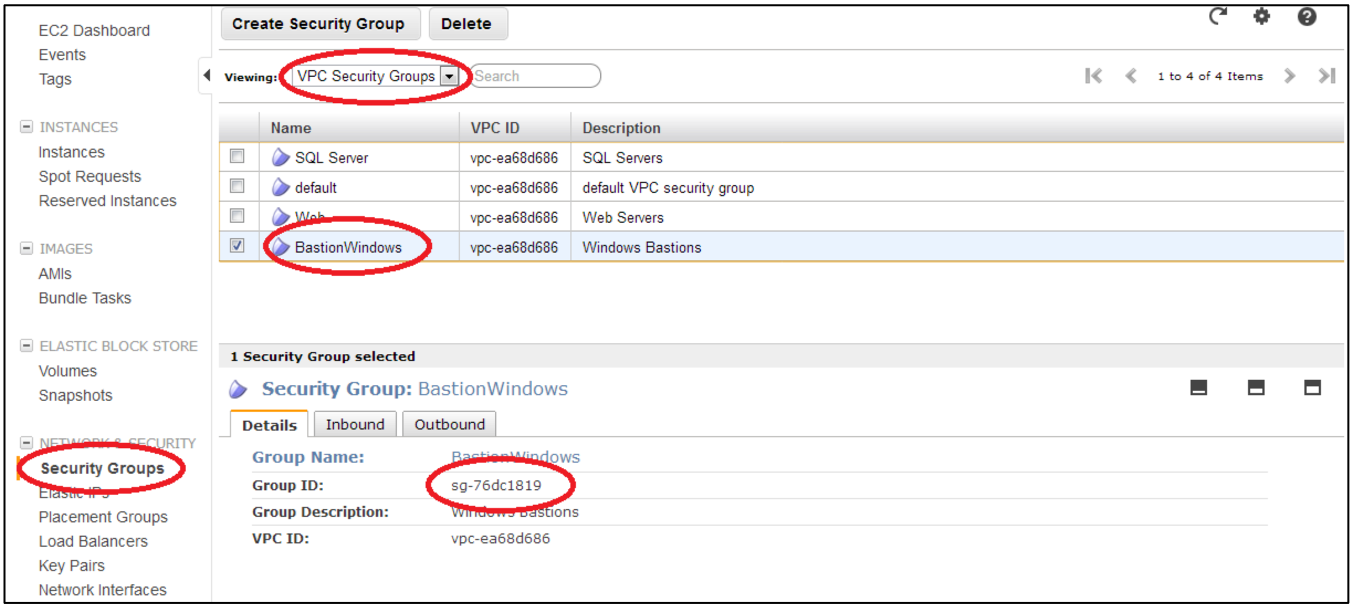
○ Storage Device Configuration

Review your options and launch the Instance.

Now that this new BastionWindows security group exists, let's change the rules for our database server so that the only traffic that it accepts is from the Bastion security group.

Return to VPC / Security Groups. Select "VPC Security Groups" from the drop-down list.

The first step is to make note of the BastionWindows Security Group ID, because you will need it in a moment. You can paste it to notepad or into the clipboard.



Viewing: VPC Security Groups

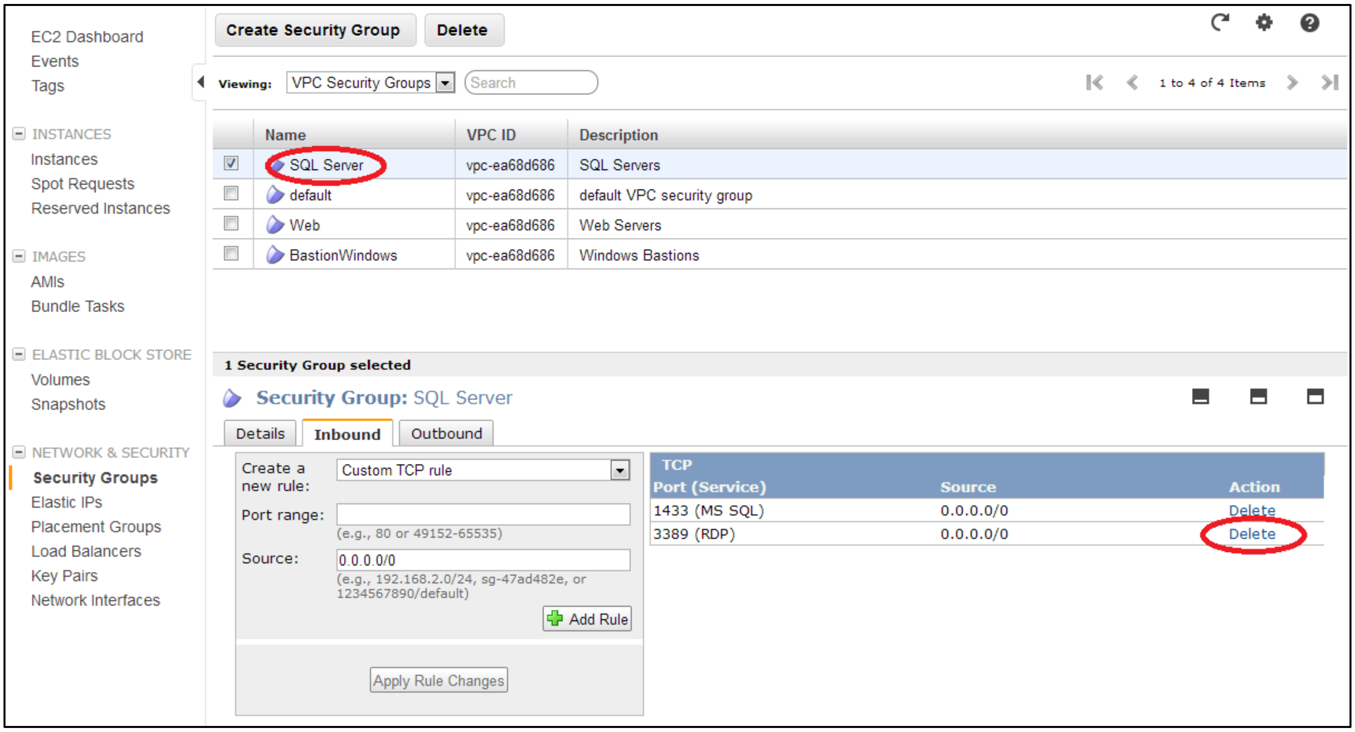
	Name	VPC ID	Description
□	SQL Server	vpc-ea68d686	SQL Servers
□	default	vpc-ea68d686	default VPC security group
□	Web	vpc-ea68d686	Web Servers
☑	BastionWindows	vpc-ea68d686	Windows Bastions

1 Security Group selected

Security Group: BastionWindows

Group Name: BastionWindows
Group ID: sg-76dc1819
Group Description: Windows Bastions
VPC ID: vpc-ea68d686

Next, delete the existing RDP rule out of the SQLServer security group.



Viewing: VPC Security Groups

	Name	VPC ID	Description
☑	SQL Server	vpc-ea68d686	SQL Servers
□	default	vpc-ea68d686	default VPC security group
□	Web	vpc-ea68d686	Web Servers
□	BastionWindows	vpc-ea68d686	Windows Bastions

1 Security Group selected

Security Group: SQL Server

Create a new rule: Custom TCP rule

Port range:

(e.g., 80 or 49152-65535)

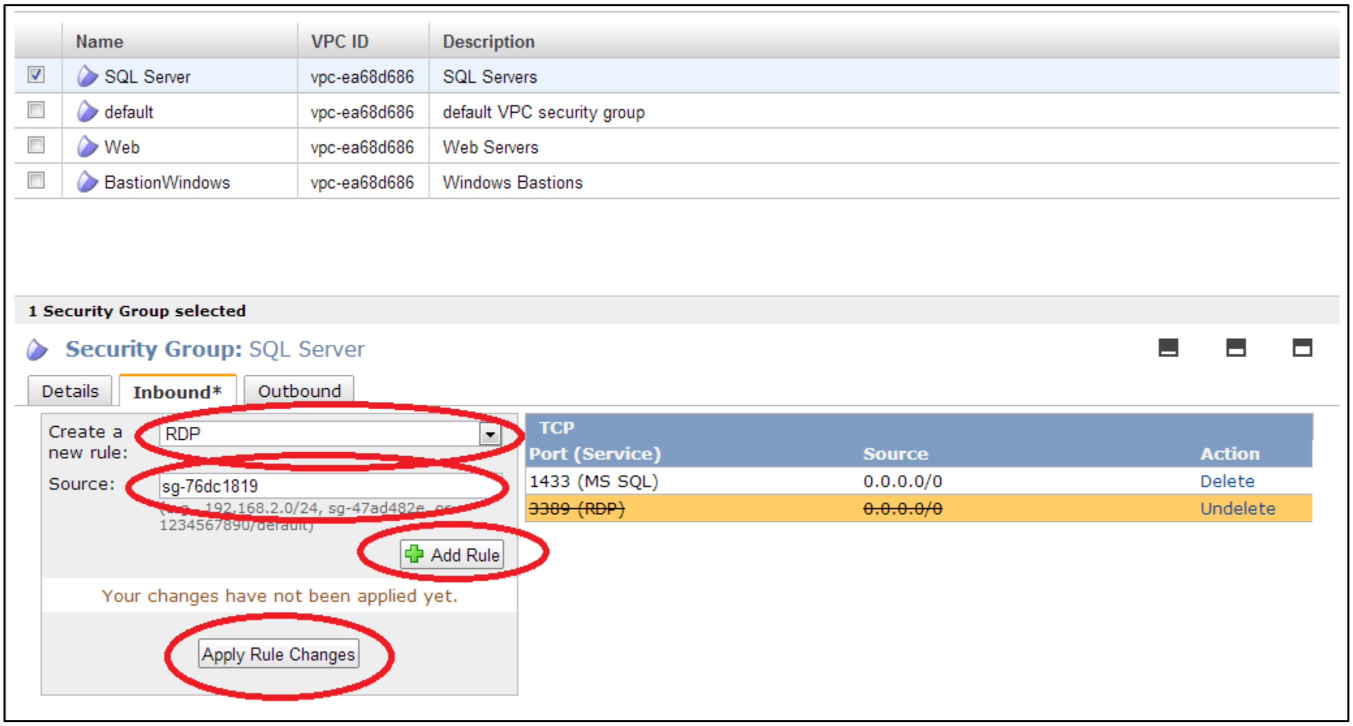
Source: 0.0.0.0/0

(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

TCP Port (Service)	Source	Action
1433 (MS SQL)	0.0.0.0/0	Delete
3389 (RDP)	0.0.0.0/0	Delete

Then add a new rule for RDP that is restricted to the BastionWindows security Group. Use the Security Group ID you pasted into notepad or the clipboard as the source. This rule illustrates another, powerful, way to use security groups.

Don't forget to apply these rule changes by clicking Apply Rule Changes.



	Name	VPC ID	Description
☑	SQL Server	vpc-ea68d686	SQL Servers
□	default	vpc-ea68d686	default VPC security group
□	Web	vpc-ea68d686	Web Servers
□	BastionWindows	vpc-ea68d686	Windows Bastions

1 Security Group selected

Security Group: SQL Server

Create a new rule: RDP

Source: sg-76dc1819

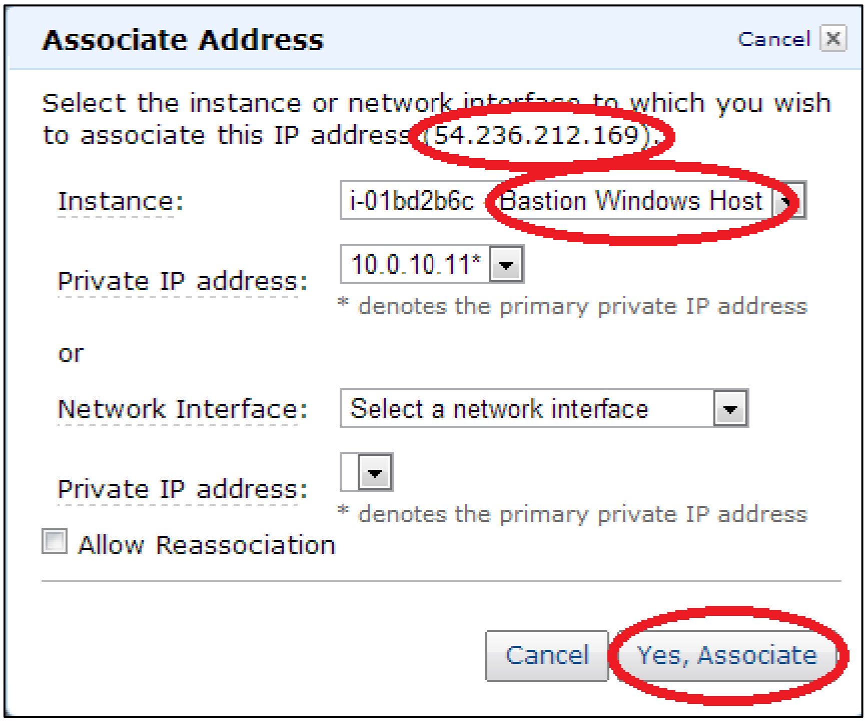
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

Your changes have not been applied yet.

TCP Port (Service)	Source	Action
1433 (MS SQL)	0.0.0.0/0	Delete
~~3389 (RDP)~~	~~0.0.0.0/0~~	Undelete

In order to use the Bastion server, you will need a public IP address.

Once assigned, the address will appear as part of the details for the Bastion host.



Associate Address

Select the instance or network interface to which you wish to associate this IP address (54.236.212.169):

Instance: i-01bd2b6c (Bastion Windows Host)

Private IP address: 10.0.10.11*

* denotes the primary private IP address

or

Network Interface: Select a network interface

Private IP address:

* denotes the primary private IP address

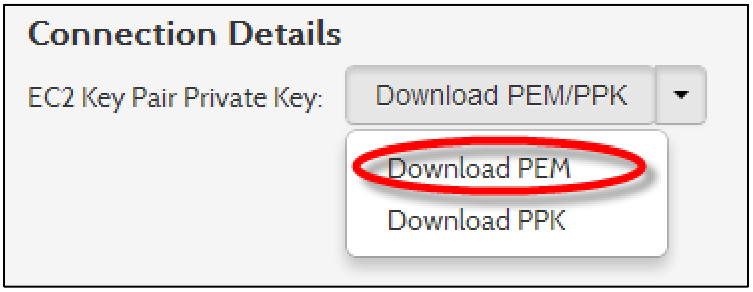
□ Allow Reassociation

Note the public IP address that you allocated and associated is the one you will use to connect to the Instance via RDP in the next section.

GET THE PASSWORD FOR YOUR WINDOWS INSTANCE

Go back to your lab in *qwikLAB*™.

Download the *qwikLAB*™ provided EC2 Key Pair private key file in the PEM format by clicking on Download PEM option in the “Download PEM/PPK” drop-down.

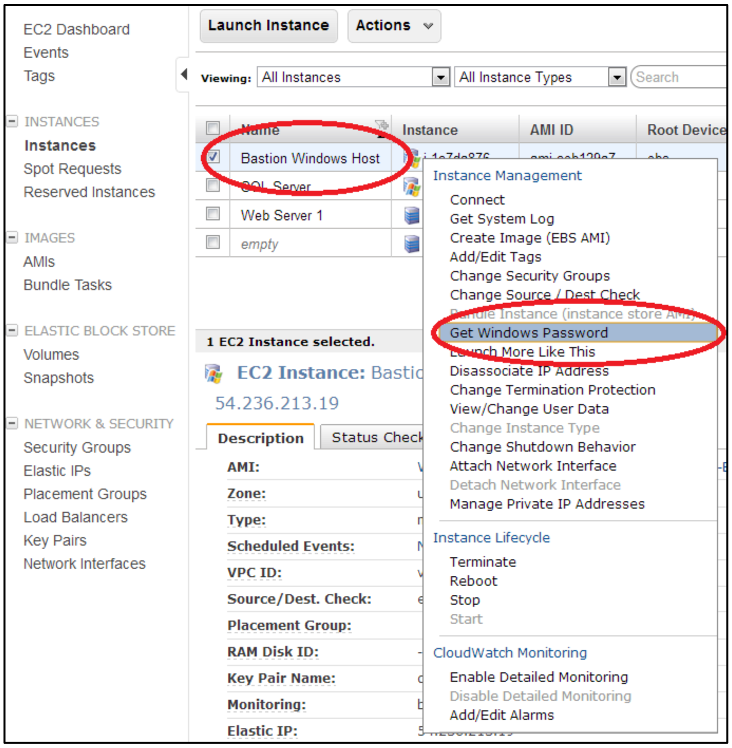


Save the file to your computer’s Downloads folder or directory or some other folder or directory of your choice.

Go back to the AWS Management Console.

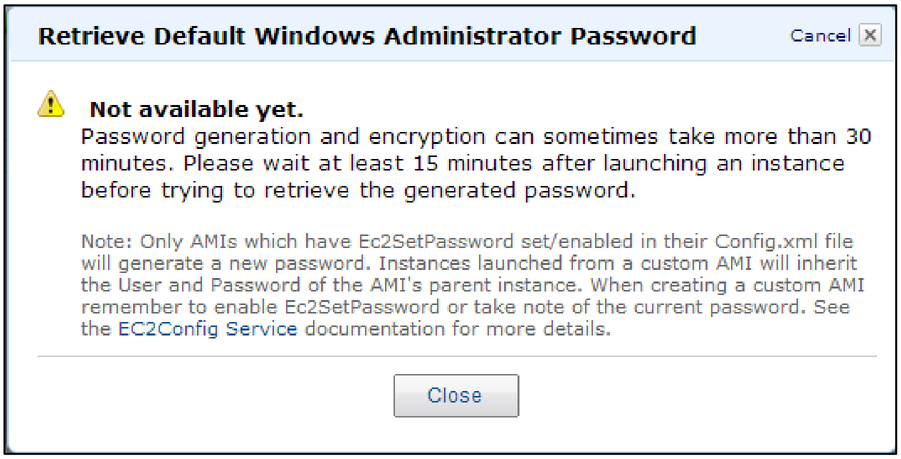
Locate the Bastion Host instance in the EC2 section. Right-click on the Instance in the AWS Management Console.

Click Get Windows Password.


EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Load Balancers
Key Pairs
Network Interfaces
Launch Instance
Actions
Viewing: All Instances
All Instance Types
Search
Name
Instance
AMI ID
Root Device
Bastion Windows Host
SQL Server
Web Server 1
empty
1 EC2 Instance selected.
EC2 Instance: Bastic
54.236.213.19
Description
Status Check
AMI:
Zone:
Type:
Scheduled Events:
VPC ID:
Source/Dest. Check:
Placement Group:
RAM Disk ID:
Key Pair Name:
Monitoring:
Elastic IP:
Instance Management
Connect
Get System Log
Create Image (EBS AMI)
Add/Edit Tags
Change Security Groups
Change Source / Dest Check
Bundle Instance (instance store AMI)
Get Windows Password
Launch More Like This
Disassociate IP Address
Change Termination Protection
View/Change User Data
Change Instance Type
Change Shutdown Behavior
Attach Network Interface
Detach Network Interface
Manage Private IP Addresses
Instance Lifecycle
Terminate
Reboot
Stop
Start
CloudWatch Monitoring
Enable Detailed Monitoring
Disable Detailed Monitoring
Add/Edit Alarms

Click on Choose File and navigate to your Downloads folder (or another place you choose) and select the EC2 Key Pair private key file that you downloaded from *qwikLAB™*.

If the Instance is still starting up you'll see a message the password is not available yet. Close the message and wait awhile and try again if you do see it. If you see it it's because you're working fast!

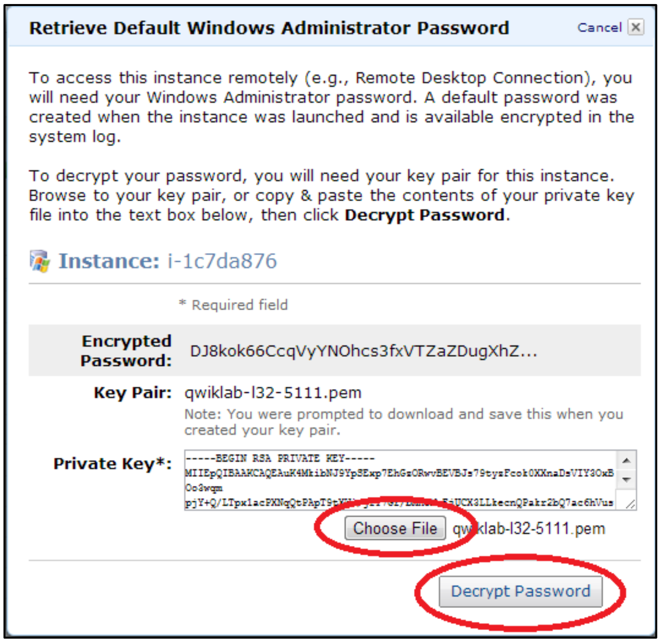


Retrieve Default Windows Administrator Password

Not available yet.
Password generation and encryption can sometimes take more than 30 minutes. Please wait at least 15 minutes after launching an instance before trying to retrieve the generated password.

Note: Only AMIs which have Ec2SetPassword set/enabled in their Config.xml file will generate a new password. Instances launched from a custom AMI will inherit the User and Password of the AMI's parent instance. When creating a custom AMI remember to enable Ec2SetPassword or take note of the current password. See the EC2Config Service documentation for more details.

Click Decrypt Password.



Retrieve Default Windows Administrator Password

To access this instance remotely (e.g., Remote Desktop Connection), you will need your Windows Administrator password. A default password was created when the instance was launched and is available encrypted in the system log.

To decrypt your password, you will need your key pair for this instance. Browse to your key pair, or copy & paste the contents of your private key file into the text box below, then click **Decrypt Password**.

Instance: i-1c7da876

* Required field

Encrypted Password: DJ8kok66CcqVyYNOhcs3fxVTZaZDugXhZ...

Key Pair: qwiklab-l32-5111.pem
Note: You were prompted to download and save this when you created your key pair.

Private Key*:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAuK4MkibNJ9YpSExp7EhGzORwvBEVBJs79tyzFcok0XXnaDsVIY3OxB
Oo3wqm
pjY+Q/LTpx1acPXNqQtPApT9t[illegible]FjUCX3LLkecnQPakr2bQ7ac6hVus
```

qwiklab-l32-5111.pem

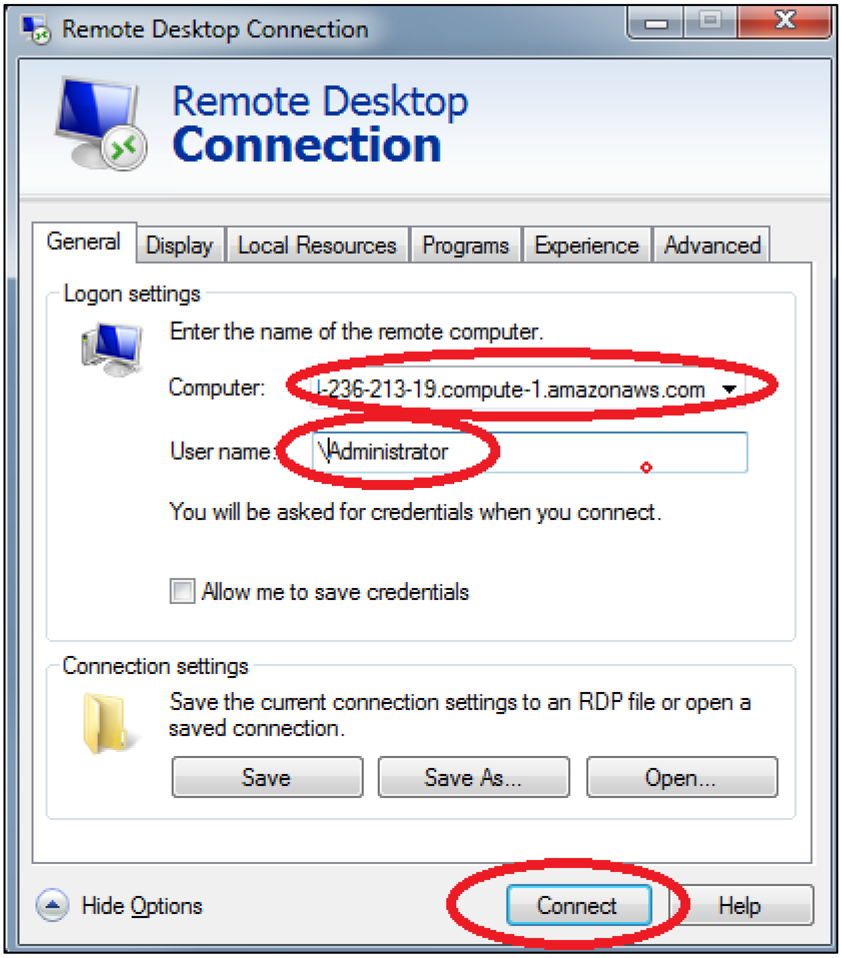
Make a note of the Computer, User, and Decrypted Password. You might copy-paste them to a text file on your computer.

CONNECT TO THE BASTION SERVER (WINDOWS)

(Hint: Go to the section Connect to the Bastion Server (OS X) or (Linux) if you are using one of those where you will run a Remote Desktop Protocol (RDP) client.)

On your local computer Start -> Run, and then type in MSTSC to start the local RDP client. Click Show Options. Enter the Computer and Username you noted and then Connect.

You'll be signing in as another account - Administrator, and may need to specify the user name as "\Administrator" (with a leading backslash) in order to differentiate from the Administrator user on your local computer.



Logon settings

Enter the name of the remote computer.

Computer: -236-213-19.compute-1.amazonaws.com

User name: \Administrator

You will be asked for credentials when you connect.

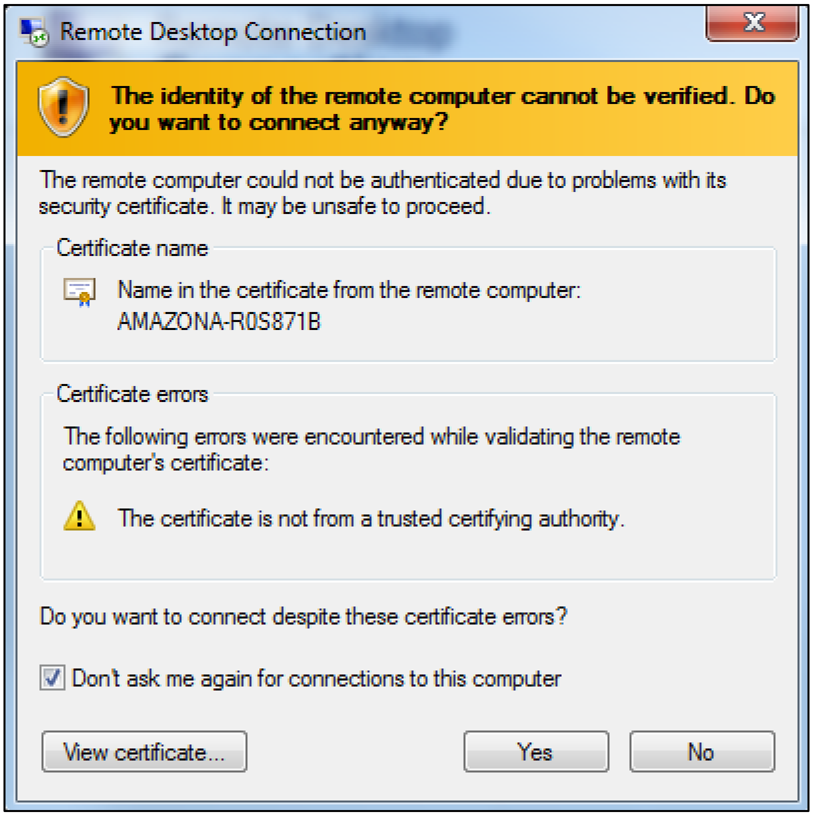
□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

When prompted, enter the Password you noted.

Click Yes when you see a certificate verification message similar to this one:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
AMAZONA-R0S871B

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

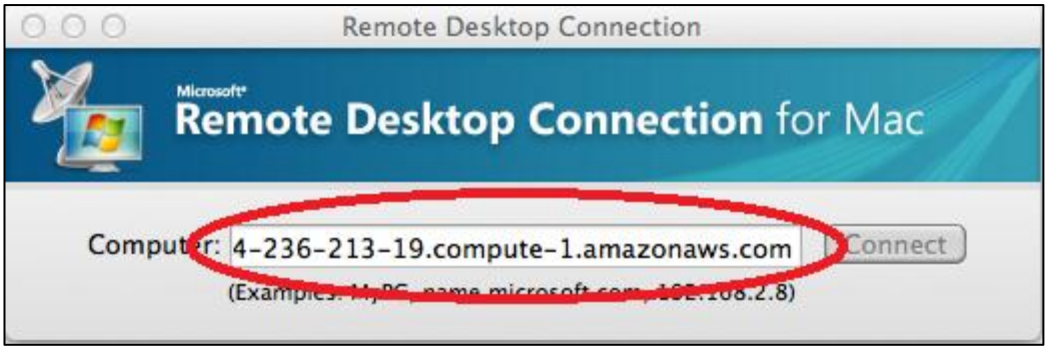
Do you want to connect despite these certificate errors?

☑ Don't ask me again for connections to this computer

CONNECT TO THE BASTION SERVER (OS X)

(Hint: Go to the section Connect to the Bastion Server (Windows) or (Linux) if you are using one of those where you will run a Remote Desktop Protocol (RDP) client.)

Open the Remote Desktop Connection for Mac application. Enter the Bastion Host Computer DNS hostname you noted or copied down above and click Connect.

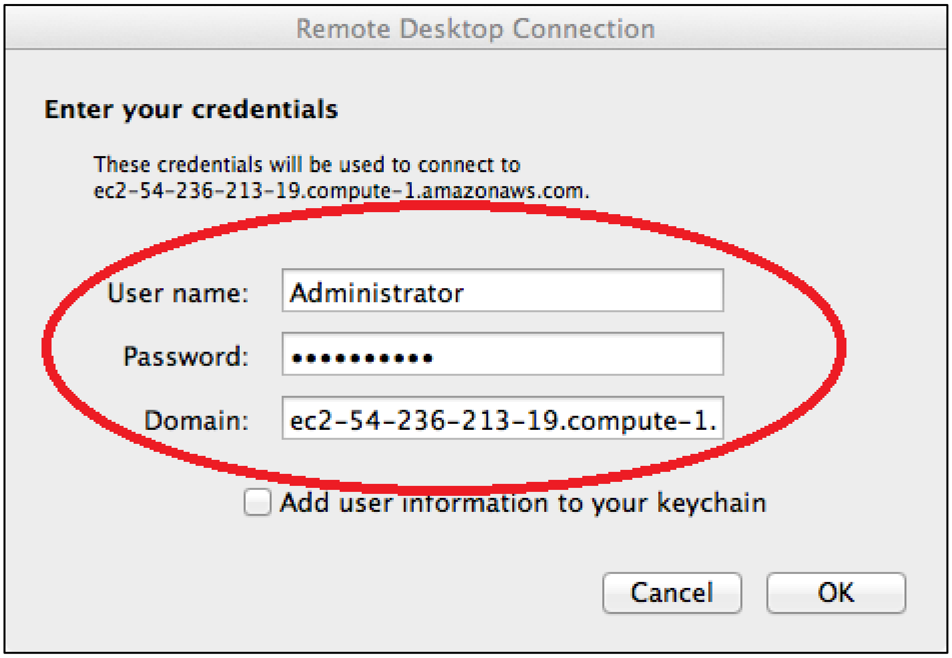


Remote Desktop Connection

Microsoft Remote Desktop Connection for Mac

Computer: 4-236-213-19.compute-1.amazonaws.com

When prompted, enter the Username and Password you noted. The Domain will auto-populate with the EC2 Instance DNS and you can ignore it. Click OK.



Enter your credentials

These credentials will be used to connect to ec2-54-236-213-19.compute-1.amazonaws.com.

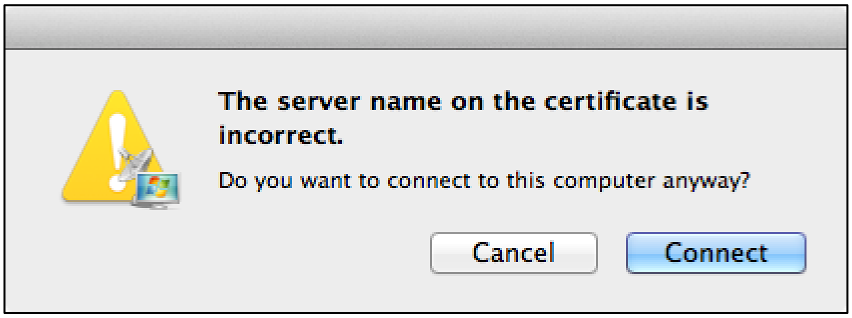
User name: Administrator

Password: ••••••••••

Domain: ec2-54-236-213-19.compute-1.

□ Add user information to your keychain

Click Yes when you see a certificate verification message similar to this one:



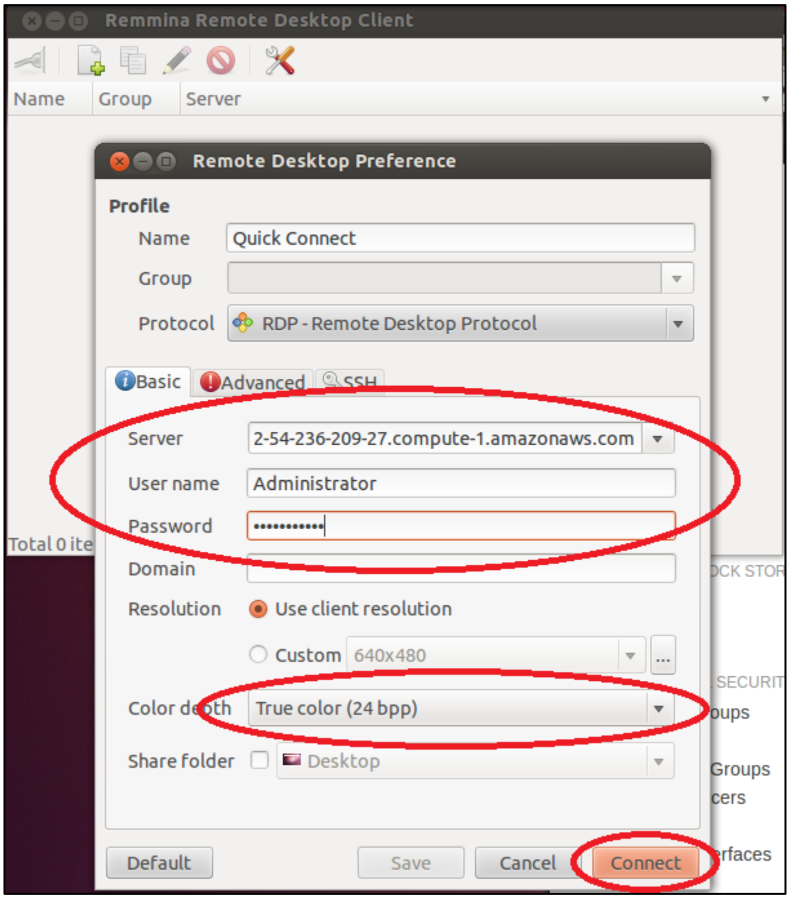
The server name on the certificate is incorrect.

Do you want to connect to this computer anyway?

CONNECT TO THE BASTION SERVER (LINUX)

(Hint: Go to the section Connect to the Bastion Server (Windows) or (OS X) if you are using one of those where you will run a Remote Desktop Protocol (RDP) client.)

Open the Remmina Remote Desktop Client. Enter the Bastion Host Computer DNS hostname you noted or copied down above in Server. Enter the Username and Password. Optionally, set Color depth to something that your bandwidth supports (in this example 'True color (24 bpp)') for a nicer remote desktop. Click Connect.



Remmina Remote Desktop Client

Remote Desktop Preference

Profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 2-54-236-209-27.compute-1.amazonaws.com

User name: Administrator

Password: •••••••••••

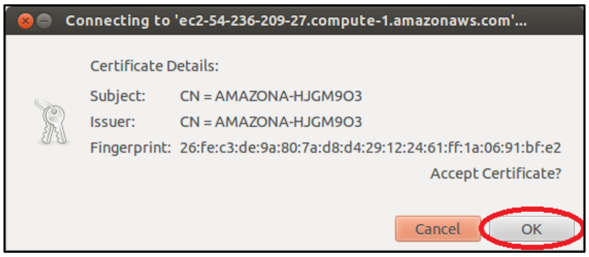
Domain:

Resolution: ● Use client resolution ○ Custom 640x480

Color depth: True color (24 bpp)

Share folder: □ Desktop

Click OK when prompted to accept the remote certificate.



Connecting to 'ec2-54-236-209-27.compute-1.amazonaws.com'...

Certificate Details:

Subject: CN = AMAZONA-HJGM9O3

Issuer: CN = AMAZONA-HJGM9O3

Fingerprint: 26:fe:c3:de:9a:80:7a:d8:d4:29:12:24:61:ff:1a:06:91:bf:e2

Accept Certificate?

LOG IN TO THE DATABASE SERVER

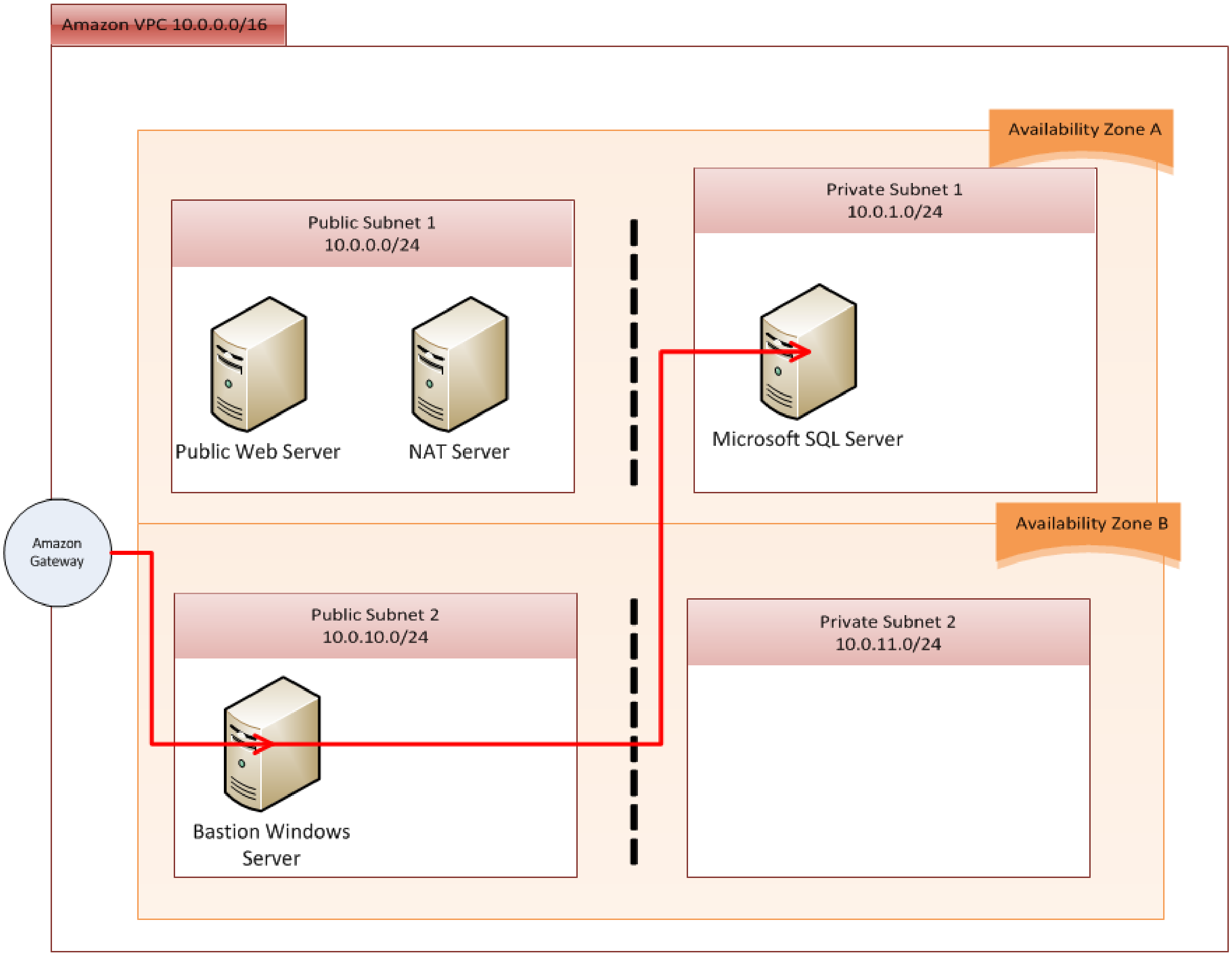
Now that we have logged in to the Bastion Host, repeat the process to log in to the SQL Server Instance from Windows.

Hint: use the above 'Connect to the Bastion Server (Windows)' even if you're using OS X or Linux yourself as you'll be running the RDP client from the remote Windows Bastion Host.

Connect to 10.0.1.99 via RDP in the remote Windows Bastion Host. You will need to repeat the process to retrieve the password for the SQL Server.

Here's our environment, now that all these pieces are in place. The line from the gateway device to the SQL Server illustrates traffic flow from the edge of the VPC network, through the Bastion Host, and to the SQL Server.

You might wonder why we created the Private Subnet 2 (10.0.11/0/24) subnet. It is because you would best deploy a slave, replica SQL Server Instance for the SQL Server in Private Subnet 1 (10.0.1.0/24).



CONCLUSION

Amazon networking is secure by default, and as you just learned there are multiple ways to safely connect to servers that are kept in private subnets.

In order to ensure that your network is secure, pay attention to which subnet you place servers in. Bastion hosts and VPN tunnels each have an advantage.

Bastion hosts are good if you need to log in to manage servers, especially if only a few people need to perform this activity.

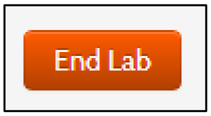
If you want the VPC to act as a virtual extension to your corporate network, then a VPN might make more sense.

Finally, we learned how Security Group rules can be either very precise, or quite loose. Make certain that your Security Groups are as restrictive as possible, but not so restrictive that there are unintended side effects.

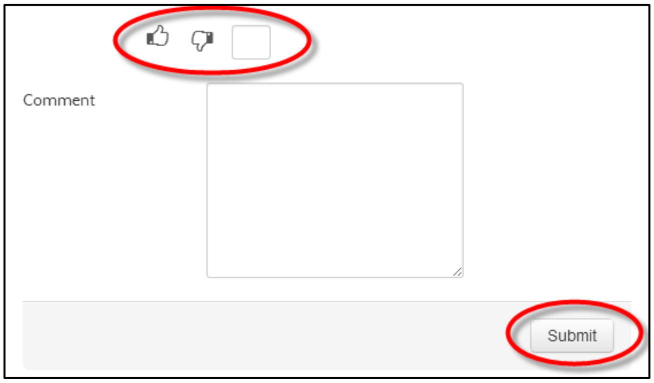
END LAB

Sign-out of the AWS Management Console.

Click the End Lab button in *qwikLAB™*.



Give the lab a thumbs-up/down, or enter a comment and click Submit


Comment
Submit