Technical Report

NetApp Private Storage for Amazon Web Services (AWS)

Solution Architecture and Deployment Guide

Mark Beaupre, NetApp
August 2013 | TR-4133

Abstract

This document describes the architecture for the NetApp® Private Storage for Amazon Web services (AWS) solution. It also serves as a deployment guide for the NetApp Private Storage for AWS solution

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Scope

This technical report documents the storage architecture and deployment procedures for the NetApp Private Storage for AWS solution.

2 NetApp Private Storage for AWS Solution Architecture

2.1 Overview

The NetApp Private Storage for AWS solution is a joint effort between NetApp and its partner public cloud, colocation, and network providers. It provides a reference architecture that combines NetApp storage consolidated guidance and validated configurations with Amazon Web Services (AWS) Elastic Compute Cloud (EC2) compute resources, Equinix colocation facilities, and XO Communications long-haul networks.

The NetApp Private Storage for AWS hybrid cloud model provides much of the efficiency and agility of cloud computing along with the increased control and customization achieved through dedicated private resources. With the NetApp private cloud for AWS, NetApp and its partners provide organizations with both the control and the flexibility required to reap the full benefits of the hybrid cloud infrastructures.

The typical use cases for NetApp Private Storage for AWS are:

- High-performance workloads
- Big data analytics
- Development and test
- Disaster recovery
- Multitier backup
- Data with compliance requirements
- Data center migration and consolidation

NetApp SnapMirror® and SnapVault® can provide the ability for customers to move data from NetApp storage in an on-premises data center to NetApp storage that is closer to the compute resources from Amazon AWS EC2 and Amazon AWS Simple Storage Service (S3) storage resources for customers who need to store backups in the cloud.

From a business perspective, the solution offers customers the ability to shift capital expenses to operational expenses. Customers can dynamically allocate compute resources, application resources, or backup resources instead of building out on-premises infrastructure.

2.2 Technical Overview

The NetApp private cloud for AWS solution combines compute resources from Amazon EC2 with NetApp storage hosted at Amazon Direct Connect colocation facilities and long-haul network resources. This is made possible by leveraging the Amazon Direct Connect offering. Direct connect provides high-speed network connectivity to a colocation facility that is physically near Amazon data centers. The connectivity options start at a single 1Gbit or 10Gbit private link. You can add additional links as required, with no limit to the number of connections.

Within the colocation facility, the customer provides a router and NetApp storage resources. Virtual machines within Amazon EC2 connect to the NetApp storage by iSCSI, CIFS, or NFS. Additional long-haul network resources can also be connected to the router to provide network connectivity between Amazon EC2 regions. The following glossary defines the terms used to describe the technical architecture.

2.3 Glossary of Terms

Amazon Machine Image (AMI). AMI is a virtual machine image in Amazon EC2.

Amazon region. Amazon region is a pool of AWS cloud resources tied to a geographic site. Each Amazon region consists of multiple availability zones.

Availability zone. Availability zones are distinct locations within an Amazon region that are engineered to be isolated from failures in other availability zones and provide inexpensive, low-latency network connectivity to other availability zones in the same region.

Border Gateway Protocol (BGP). BGP is the border routing protocol Amazon uses to advertise routes between EC2 VPCs and resources located in Direct Connect facilities.

Direct connect. Direct connect is a service offered by Amazon and participating colocation providers to establish a high-speed connection to customer-provided hardware hosted in a colocation facility cage.

Open Shortest Path First (OSPF). OSPF is a network interior routing protocol.

Virtual private cloud (VPC). A VPC is an isolated IP address range within EC2. It can be connected to other VPCs, the Internet, or Direct Connect through a VGW.

Virtual private gateway (VGW). A VGW is a virtual router gateway used to connect your VPC to other networks.

3 Solution Architecture

The solution architecture consists of the following components:

- AWS EC2 compute
- AWS Virtual Private Cloud
- AWS AMI virtual machines
- AWS Direct Connect
- BGP configuration (single AWS region topologies)
- OSPF routing configuration (routing between multiple single AWS region topologies)
- Customer-provided network switches and routers
- NetApp storage (FAS/V-Series)
- Network storage protocols (CIFS, NFS, iSCSI)
- Long-haul network

3.1 AWS EC2 Compute

Amazon elastic compute cloud (Amazon EC2) is a Web service that provides resizable compute capacity in the cloud. This environment provides for preconfigured virtual machines or AMIs.

The AWS EC2 service is available on a per AWS region basis. Each AWS region is tied to a specific geographic location. The following is a list of AWS regions:

- Ireland
- Northern California
- Northern Virginia
- Oregon
- São Paolo
- Singapore
- Sydney

- Tokyo

Note: The Oregon and GovCloud AWS regions do not offer Direct Connect service, so these regions are not available for use in this solution.

The AWS EC2 management web interface is used to deploy AWS VPC and AMI resources for the NetApp Private Storage for AWS solution.

3.2 AWS Virtual Private Cloud

AWS Virtual Private Cloud is a dedicated virtual network into which AWS AMI virtual machines and other AWS services can be deployed. The VPC network configuration can be customized, which includes IP address ranges, subnets, routing, gateways, and network security using access control lists and security groups.

The VPCs can consist of different subnets. For example, there could be a subnet for storage connectivity between the AMI virtual machines and the NetApp storage and a second subnet for client access to an application installed on the AMI virtual machine.
Each VPC is connected to the NetApp storage using Amazon Direct Connect over a Layer 2 network connection from the Amazon EC2 resources to the customer-owned network switches in the Equinix colocated facility.

The VPC can span multiple availability zones within an Amazon region. VPC subnets cannot span multiple availability zones.

The NetApp storage controller is connected to the customer-owned network switches with the appropriate routing configured using BGP and OSPF (if deploying NetApp Private Storage for AWS in multiple AWS regions).

3.3 AWS AMI Virtual Machines

The Amazon Machine Image (AMI) virtual machines have various instance types that support the compute needs of a customer. The categories of machine instance types are:

- Standard instances
- First generation
- Second generation
- Micro instances
- High-memory instances
- High-CPU instances
- Cluster compute instances
- Cluster GPU instances
- High-I/O instances

Note: Refer to this link for more information about AMI instance types. Not all instance types are available for all AWS regions.

In addition to different instance types, AMI virtual machines can run different operating systems. The list of supported operating systems includes:

- Red Hat Enterprise Linux®
- Windows Server® (2003 R2, 2008, 2008 R2 and 2012)
- Oracle® Enterprise Linux
- SUSE Linux Enterprise (Enterprise Server 10 and 11)
- Amazon Linux AMI
- Ubuntu

- Fedora
- Gentoo Linux
- Debian

Amazon also offers AMI virtual machines preinstalled with applications. The types of preinstalled applications that are offered are:

- Database servers
- Application servers
- Content management servers
- Business Intelligence servers

You can also create a custom AMI virtual machine based on the available AMI virtual machine instances. The custom virtual machine is saved as an image for you to deploy other AMI virtual machine instances.

Note: Refer to this link for more information about the available operating systems and preinstalled applications with AMI virtual machines.

For each operating system and application type, validate version compatibility with NetApp client software and Data ONTAP® version using the NetApp Interoperability Matrix Tool.

By default, all Amazon EC2 instances are assigned one IP address at launch: a private (RFC 1918) IP address.

To connect to your instance, you use the public DNS name associated with the public IP address. However, this name is not static and can change, for example, when an instance reboots. If you want a persistent address to which to connect, use an AWS elastic IP address.

Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Additionally, elastic IP addresses are associated with your account, not specific instances. Any elastic IP addresses that you associate with your account remain associated with your account until you explicitly release them. Unlike traditional static IP addresses, however, elastic IP addresses allow you to mask instance or availability zone failures by rapidly remapping your public IP addresses to any instance in your account

Note: Refer to this link for more information about elastic IP addresses.

3.4 AWS Direct Connect

AWS Direct Connect is used to establish a dedicated network connection between the customer-provided network switch or router in the Equinix collocated facility and the Amazon Virtual Private Cloud. Direct Connect supports the use of industry standard 802.1q VLANs. By using multiple VLANs, the dedicated connection can be partitioned into multiple virtual interfaces.

Multiple VLANs can be used for different types of network traffic. For example, one VLAN can be used for AMI virtual machine storage connectivity to the NetApp storage and another VLAN can be used for client connectivity to any applications running on the AMI virtual machine. Access to S3 is also supported as well. Virtual interfaces can be reconfigured at any time to meet changing needs.

Direct Connect connections come in two types: 1Gb Ethernet and 10Gb Ethernet. The connection from the VPC to the network switch or router in the Equinix colocation is a Layer-2 connection from each Availability Zone used by the VPC.

It is recommended that at least two Direct Connect network connections be connected to two customer provided network switches or routers in the Equinix colocation.

3.5 Border Gateway Protocol

Border Gateway Protocol (BGP) is used to support network routing between the Amazon VPC networks and the customer network in the Equinix colocated facility over the Amazon Direct Connect network connection.

For simple single-region topologies, customer networks in the colocation facility are all directly connected to the customer-provided router. The router configuration advertises BGP routes to the AWS VPC network over the Direct Connect network connection and also receives the BGP advertisements from the AWS VPC network over the Direct Connect network connection. The AWS Direct Connect team and Equinix colocation provider will complete this basic BGP configuration.

3.6 Open Shortest Path First (OSPF)

For more advanced topologies, where you have multiple connected networks in the colocation facility or are routing between AWS regions, you will need to deploy an interior routing protocol such as OSPF and then import and export routes from each AWS regions. Network connectivity between AWS regions is provided using long-haul networks from XO Communications. BGP will still be used for routing between the customer network in the colocation facility and the VPC network over the Direct Connect network connection.

3.7 Sample Network Topologies

One of the strengths of NetApp Private Storage for AWS is that the solution can accommodate various customer topologies or scenarios, although it is impossible to cover every possible topology. The following diagrams illustrate two common routing configurations.

Figure 1) Example of routing configuration between colocated data center and EC2 virtual private cloud (BGP only).

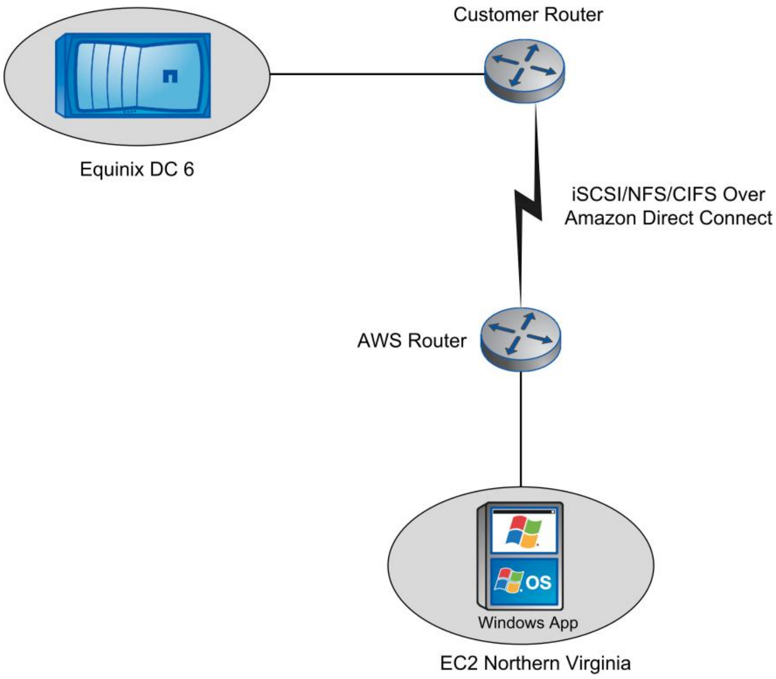
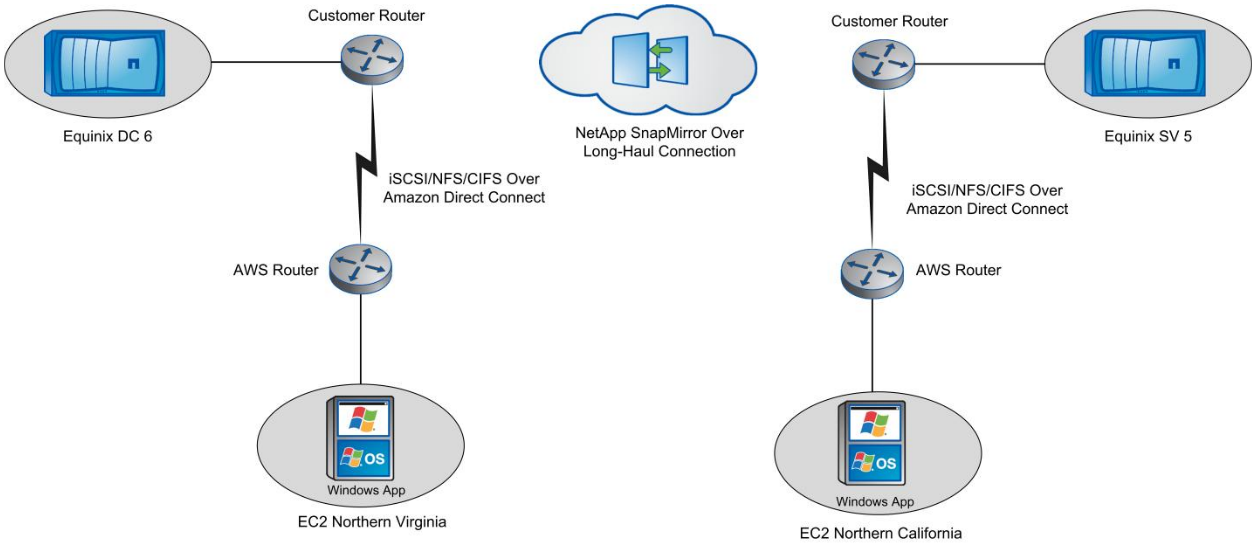


Figure 2) Example of complex routing configuration, including routing over private network between EC2 regions to support SnapMirror replication between colocated data centers (BGP and OSPF).



4 NetApp Private Storage for AWS Deployment Guide

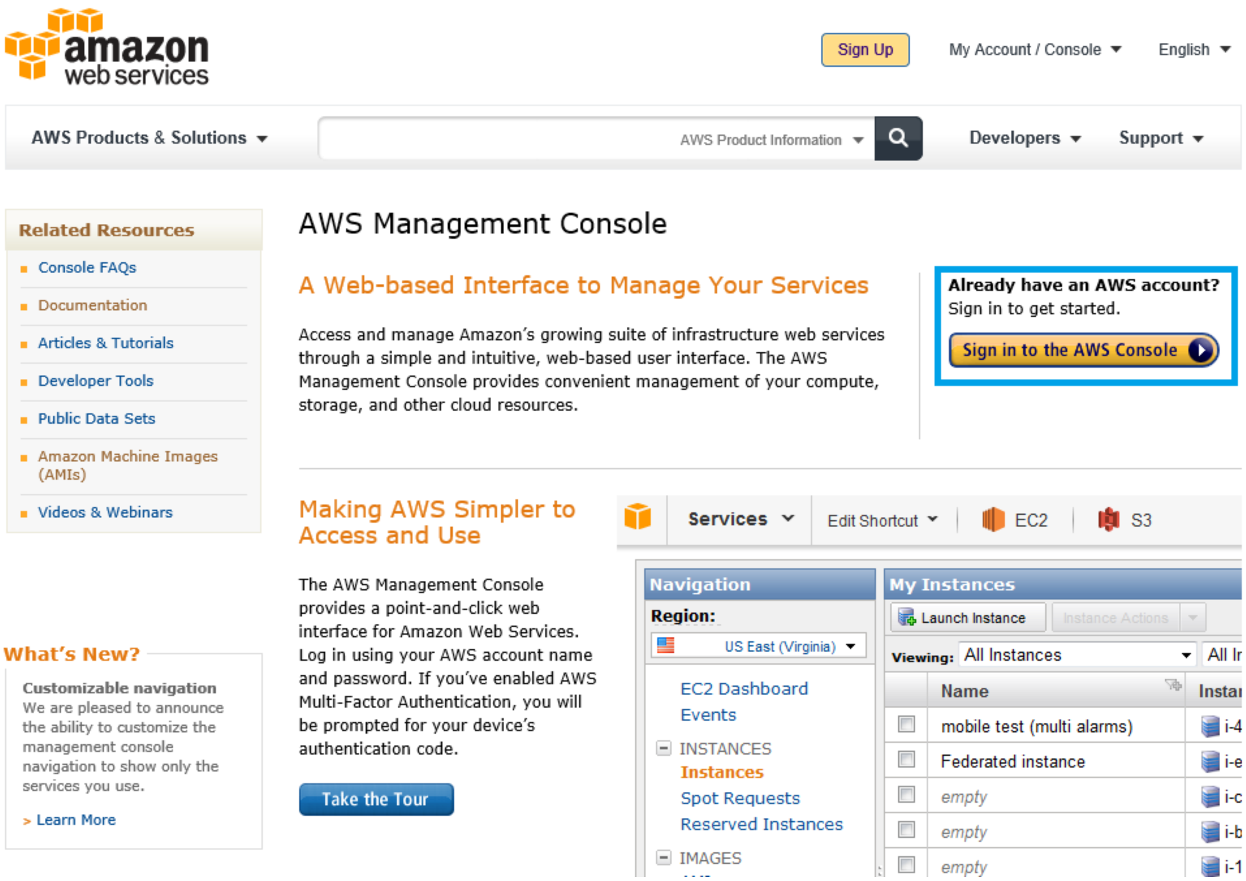
Table 1) NetApp Private Storage for AWS prerequisites.

Description
The customer must have an Amazon account created with an associated payment method and must have associated this account with Amazon Web services (http://aws.amazon.com).
Designate in which Amazon AWS region Amazon EC2 AMI virtual machines will be stored.
Identify the availability zones in the designated AWS region where AMI virtual machines will be created.
IP address plan for VPC (IP CIDR block and subnet information).
NetApp storage controller must be installed in the colocation facility for the designated Amazon AWS region.
Customer-provided network switch(es) and router(s) must be installed in the colocation facility for the designated Amazon AWS region.
Customer-provided network router(s) must have BGP support enabled.
Determine which type of AMI virtual machine will be deployed in EC2 for the solution.
NetApp storage system network interfaces connected to the customer-provided network switch(es).
NetApp storage system network interfaces enabled and configured.

4.1 Create and Configure Amazon AWS Virtual Private Cloud

To create and configure an Amazon AWS Virtual Private Cloud, complete the following steps:

1. Open a web browser and go to the URL for Amazon AWS, http://aws.amazon.com. Click “Sign in to the AWS Console” to access the AWS Console.



Related Resources

- Console FAQs
- Documentation
- Articles & Tutorials
- Developer Tools
- Public Data Sets
- Amazon Machine Images (AMIs)
- Videos & Webinars

AWS Management Console

A Web-based Interface to Manage Your Services

Access and manage Amazon's growing suite of infrastructure web services through a simple and intuitive, web-based user interface. The AWS Management Console provides convenient management of your compute, storage, and other cloud resources.

Already have an AWS account?
Sign in to get started.

Sign in to the AWS Console

What's New?

Customizable navigation
We are pleased to announce the ability to customize the management console navigation to show only the services you use.

> Learn More

Making AWS Simpler to Access and Use

The AWS Management Console provides a point-and-click web interface for Amazon Web Services. Log in using your AWS account name and password. If you've enabled AWS Multi-Factor Authentication, you will be prompted for your device's authentication code.

Navigation

Region: US East (Virginia)

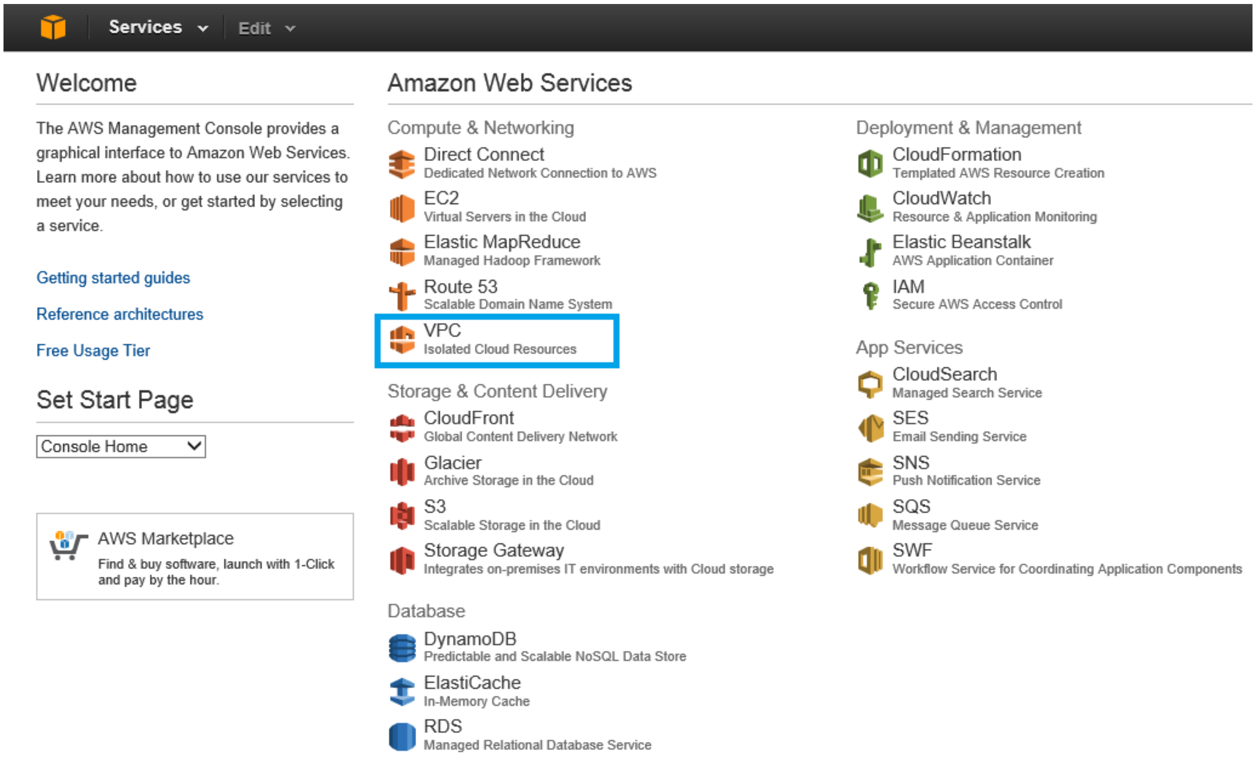
EC2 Dashboard
Events
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES

My Instances

Viewing: All Instances

	Name	Instai
□	mobile test (multi alarms)	i-4
□	Federated instance	i-e
□	empty	i-c
□	empty	i-b
□	empty	i-1

2. In the AWS Console, click the VPC link.



Welcome

The AWS Management Console provides a graphical interface to Amazon Web Services. Learn more about how to use our services to meet your needs, or get started by selecting a service.

Getting started guides
Reference architectures
Free Usage Tier

Set Start Page

Console Home

AWS Marketplace
Find & buy software, launch with 1-Click and pay by the hour.

Amazon Web Services

Compute & Networking
Direct Connect — Dedicated Network Connection to AWS
EC2 — Virtual Servers in the Cloud
Elastic MapReduce — Managed Hadoop Framework
Route 53 — Scalable Domain Name System
VPC — Isolated Cloud Resources

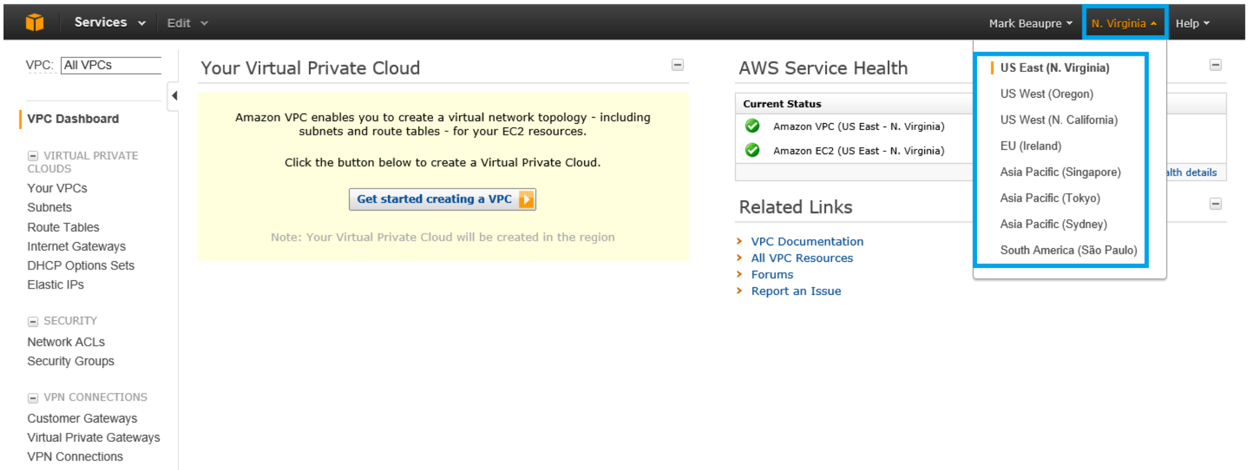
Storage & Content Delivery
CloudFront — Global Content Delivery Network
Glacier — Archive Storage in the Cloud
S3 — Scalable Storage in the Cloud
Storage Gateway — Integrates on-premises IT environments with Cloud storage

Database
DynamoDB — Predictable and Scalable NoSQL Data Store
ElastiCache — In-Memory Cache
RDS — Managed Relational Database Service

Deployment & Management
CloudFormation — Templated AWS Resource Creation
CloudWatch — Resource & Application Monitoring
Elastic Beanstalk — AWS Application Container
IAM — Secure AWS Access Control

App Services
CloudSearch — Managed Search Service
SES — Email Sending Service
SNS — Push Notification Service
SQS — Message Queue Service
SWF — Workflow Service for Coordinating Application Components

3. In the VPC dashboard, click the region name in the upper-right corner to select the desired Amazon region where the VPC will be created.

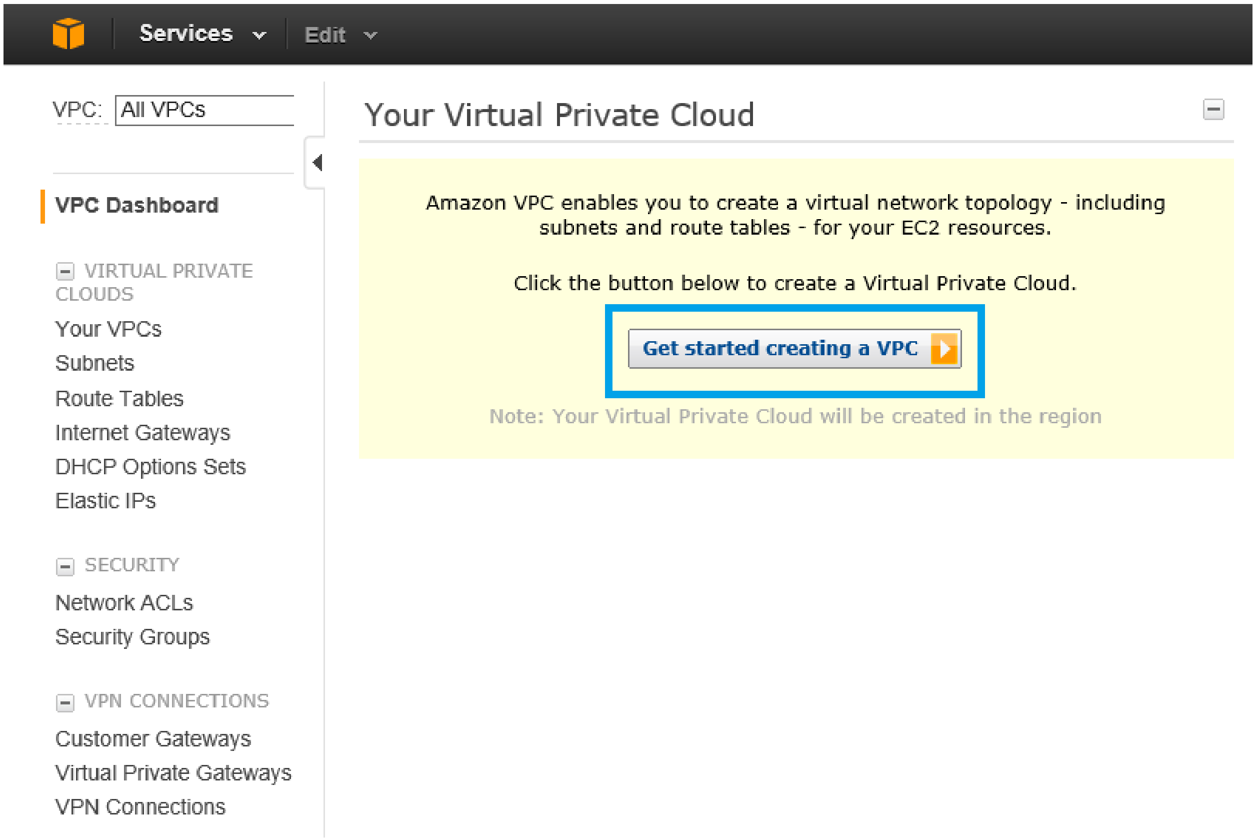


Amazon VPC enables you to create a virtual network topology - including subnets and route tables - for your EC2 resources.

Click the button below to create a Virtual Private Cloud.

Note: Your Virtual Private Cloud will be created in the region

4. After selecting the Amazon Region in the VPC Console, click “Get started to creating a VPC.”



Amazon VPC enables you to create a virtual network topology - including subnets and route tables - for your EC2 resources.

Click the button below to create a Virtual Private Cloud.

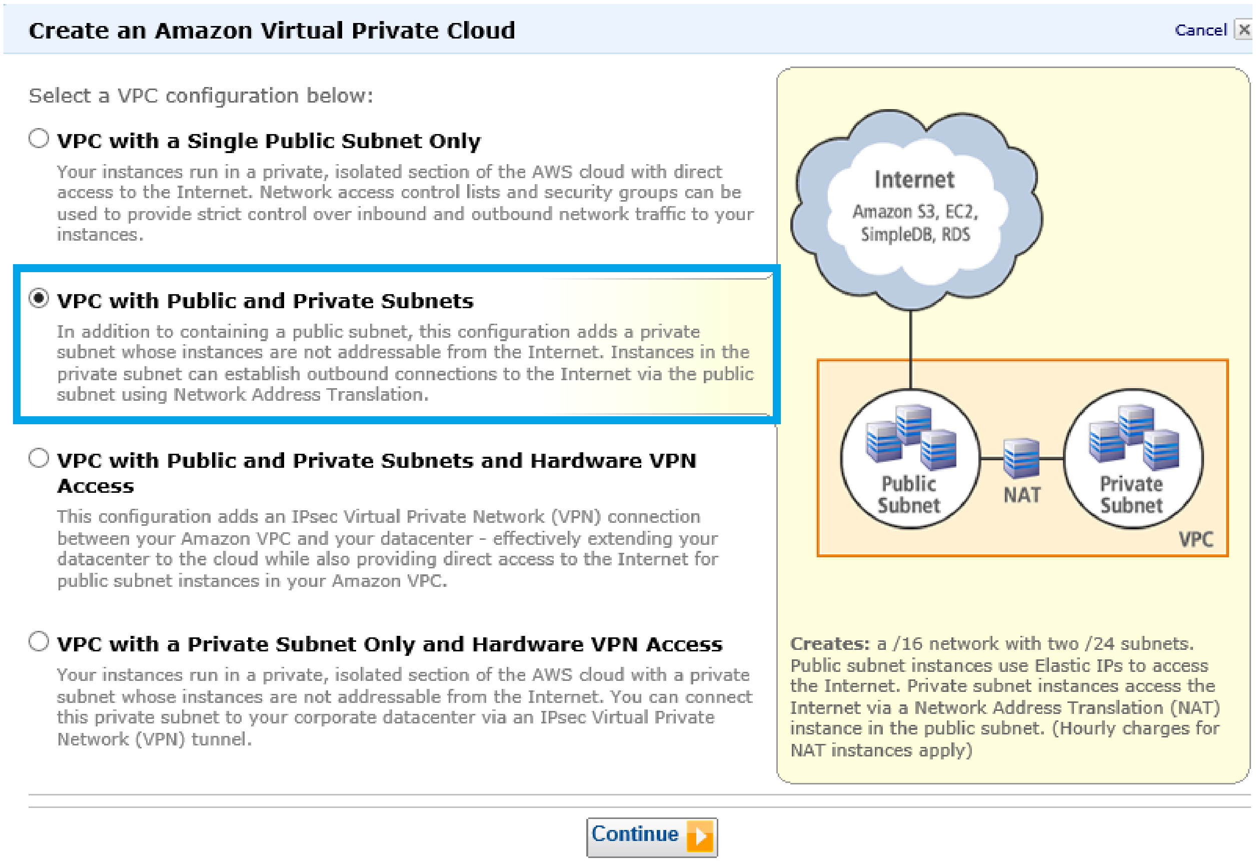
Note: Your Virtual Private Cloud will be created in the region

5. In the “Create an Amazon Private Cloud” wizard, select “VPC with Public and Private Subnets.”

Note: The option “VPC with Public and Private Subnets” will allow for a network configuration that will support LAN access to the EC2 AMI virtual machines and a private storage connection between the NetApp storage and the EC2 AMI virtual machines.

Note: Other VPC subnet options can be selected based on the requirements where the solution will be used.

6. Click Continue.



Create an Amazon Virtual Private Cloud

Cancel ☒

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.

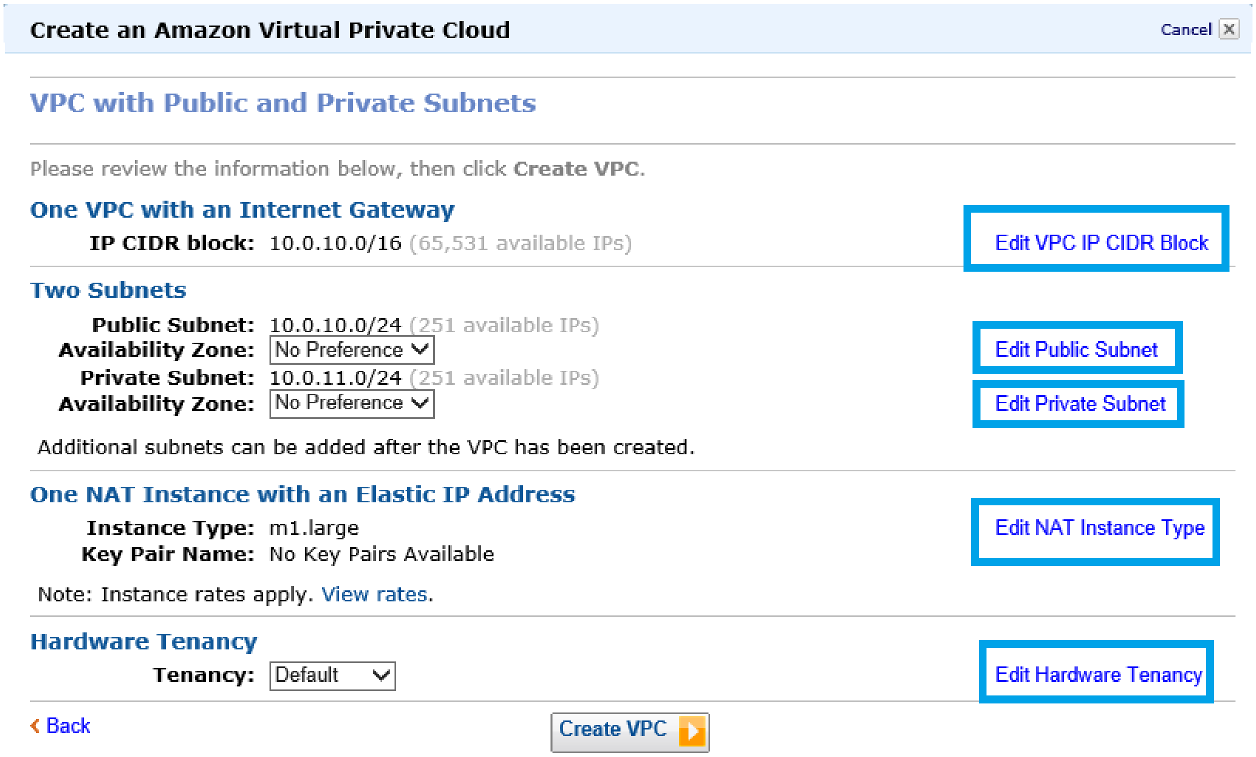
Creates: a /16 network with two /24 subnets. Public subnet instances use Elastic IPs to access the Internet. Private subnet instances access the Internet via a Network Address Translation (NAT) instance in the public subnet. (Hourly charges for NAT instances apply)

7. In the “Create an Amazon Virtual Cloud” page, set the following options for your environment:
   - “Edit VPC CIDR IP Block” to set the CIDR IP block for the VPC network (that is, 10.0.10.0/16).
   - “Edit Public Subnet” to set the public subnet in the CIDR IP block (that is, 10.0.10.0/24).
   - “Edit Private Subnet” to set the private subnet in the CIDR IP block (that is, 10.0.11.0/24).
   - “Edit NAT Instance Type” to set the EC2 AMI instance type. (that is, m1.large).

   Note: Your instance type will depend on the system requirements of the applications that will be run on the EC2 AMI instances.

   Note: An AMI instance will automatically be created and assigned to the VPC.

   - Set hardware tenancy, if desired.
8. Click “Create VPC.”



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: 10.0.10.0/16 (65,531 available IPs)

Two Subnets

Public Subnet: 10.0.10.0/24 (251 available IPs)
Availability Zone: No Preference
Private Subnet: 10.0.11.0/24 (251 available IPs)
Availability Zone: No Preference

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

One NAT Instance with an Elastic IP Address

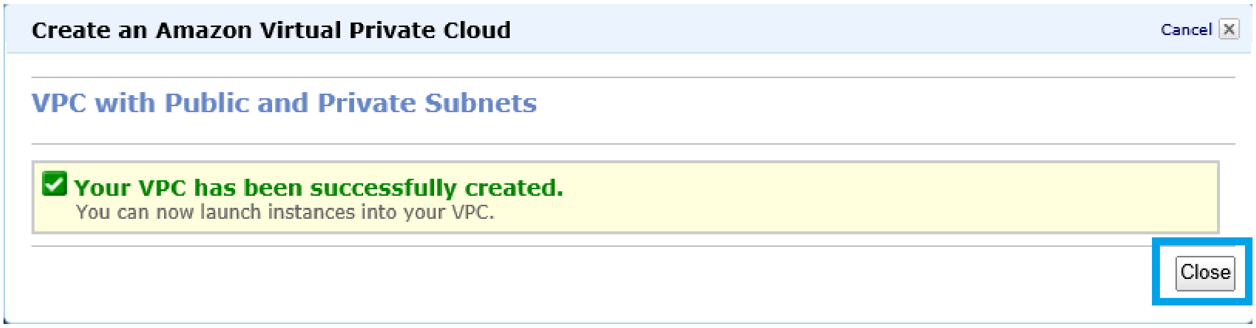
Instance Type: m1.large
Key Pair Name: No Key Pairs Available

Note: Instance rates apply. View rates.

Hardware Tenancy

Tenancy: Default

9. You will be notified of the successful creation of the VPC. Click Close.

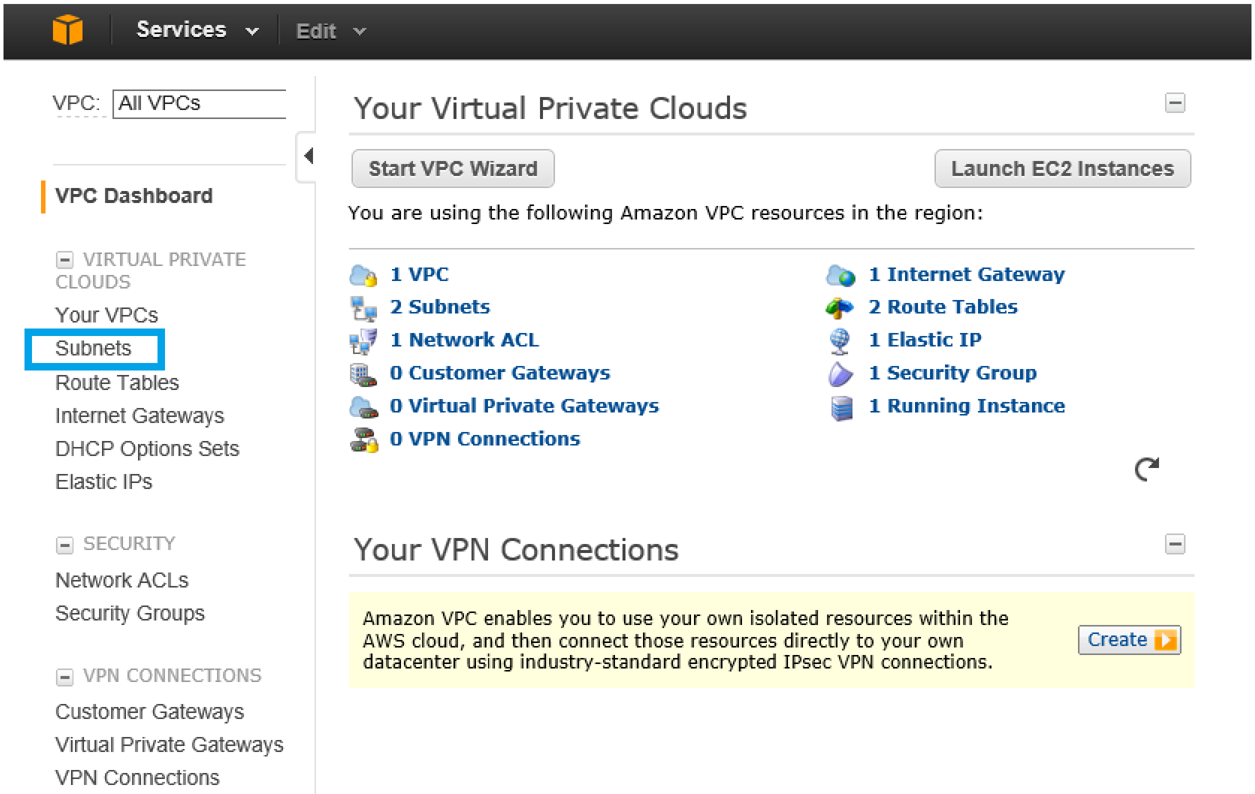


Create an Amazon Virtual Private Cloud

VPC with Public and Private Subnets

☑ **Your VPC has been successfully created.**
You can now launch instances into your VPC.

10. In the VPC dashboard, click Subnets to review the subnet status.



Your Virtual Private Clouds

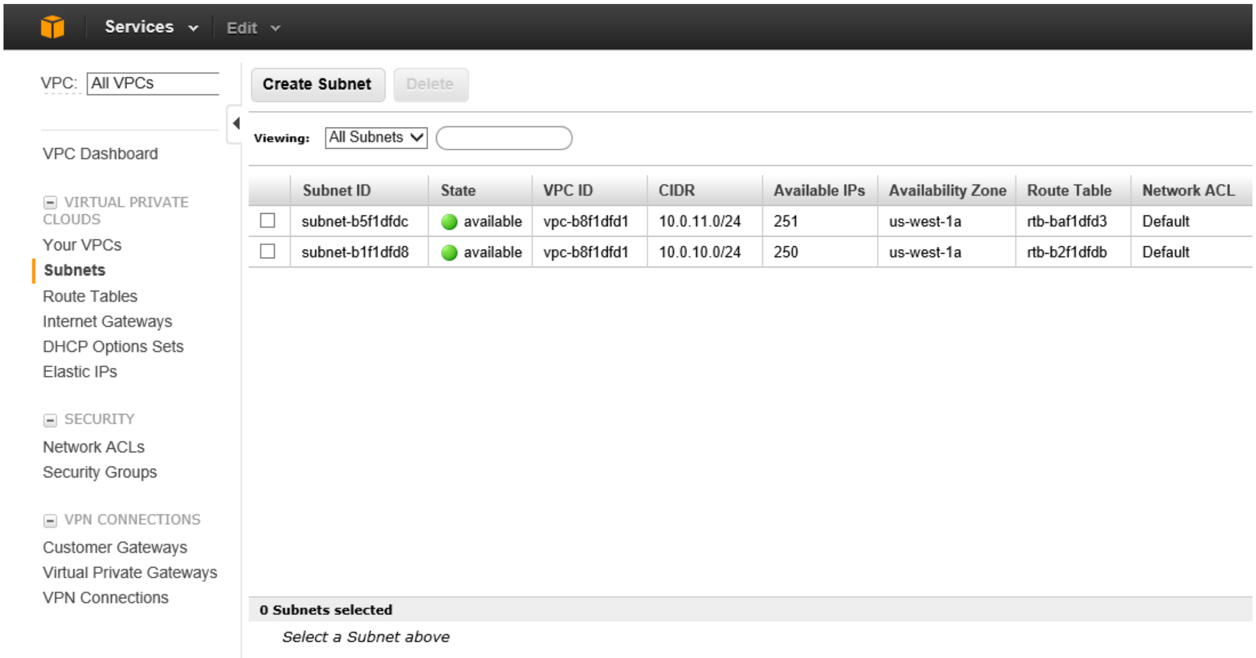
You are using the following Amazon VPC resources in the region:

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

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.

11. In the VPC dashboard, review the subnets that have been created with the VPC. If additional subnets need to be created, for the VPC, click “Create Subnet.”

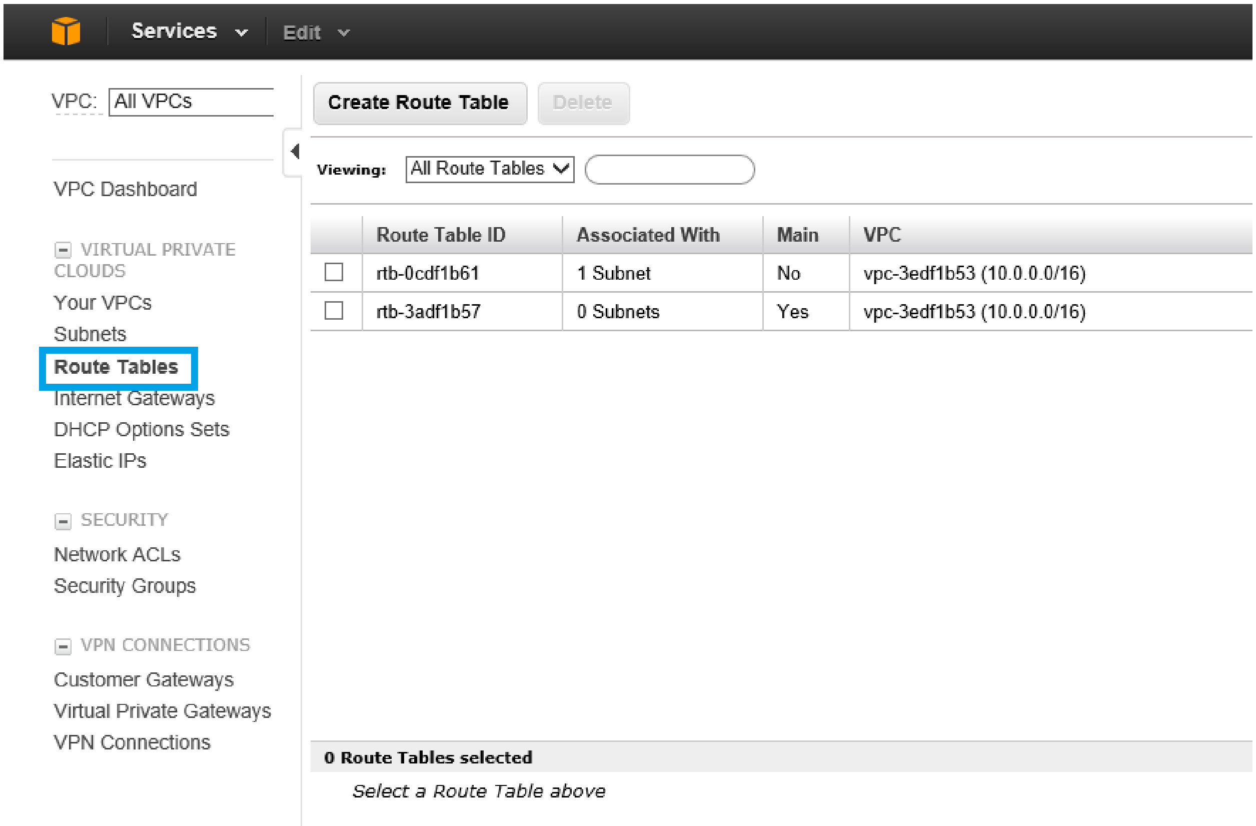


	Subnet ID	State	VPC ID	CIDR	Available IPs	Availability Zone	Route Table	Network ACL
□	subnet-b5f1dfdc	● available	vpc-b8f1dfd1	10.0.11.0/24	251	us-west-1a	rtb-baf1dfd3	Default
□	subnet-b1f1dfd8	● available	vpc-b8f1dfd1	10.0.10.0/24	250	us-west-1a	rtb-b2f1dfdb	Default

0 Subnets selected

Select a Subnet above

12. In the VPC Dashboard, click “Route Tables” to review the route tables for the subnets in the VPC. If additional route tables need to be created, for the VPC, click “Create Route Table”.



VPC: All VPCs

Viewing: All Route Tables

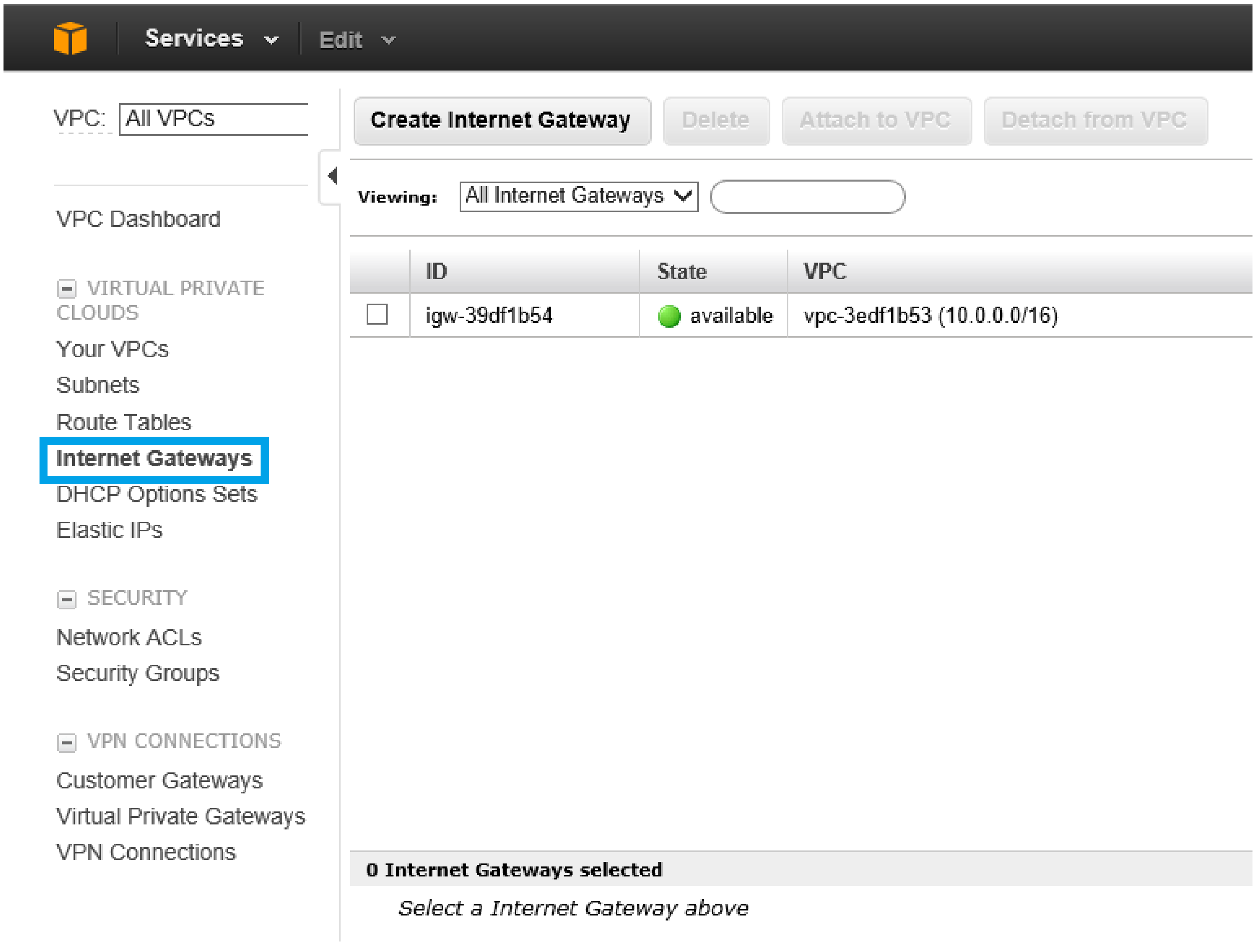
	Route Table ID	Associated With	Main	VPC
□	rtb-0cdf1b61	1 Subnet	No	vpc-3edf1b53 (10.0.0.0/16)
□	rtb-3adf1b57	0 Subnets	Yes	vpc-3edf1b53 (10.0.0.0/16)

0 Route Tables selected

Select a Route Table above

13. In the VPC Dashboard, click “Internet Gateways” to review the internet gateways configured for the VPC. An Internet gateway is the router on the AWS network that connects your VPC to the Internet.

Note: Internet gateways are optional. In most cases, internet gateways will not be configured because the internet network traffic will be routed back through the customer’s internet connection.



VPC: All VPCs

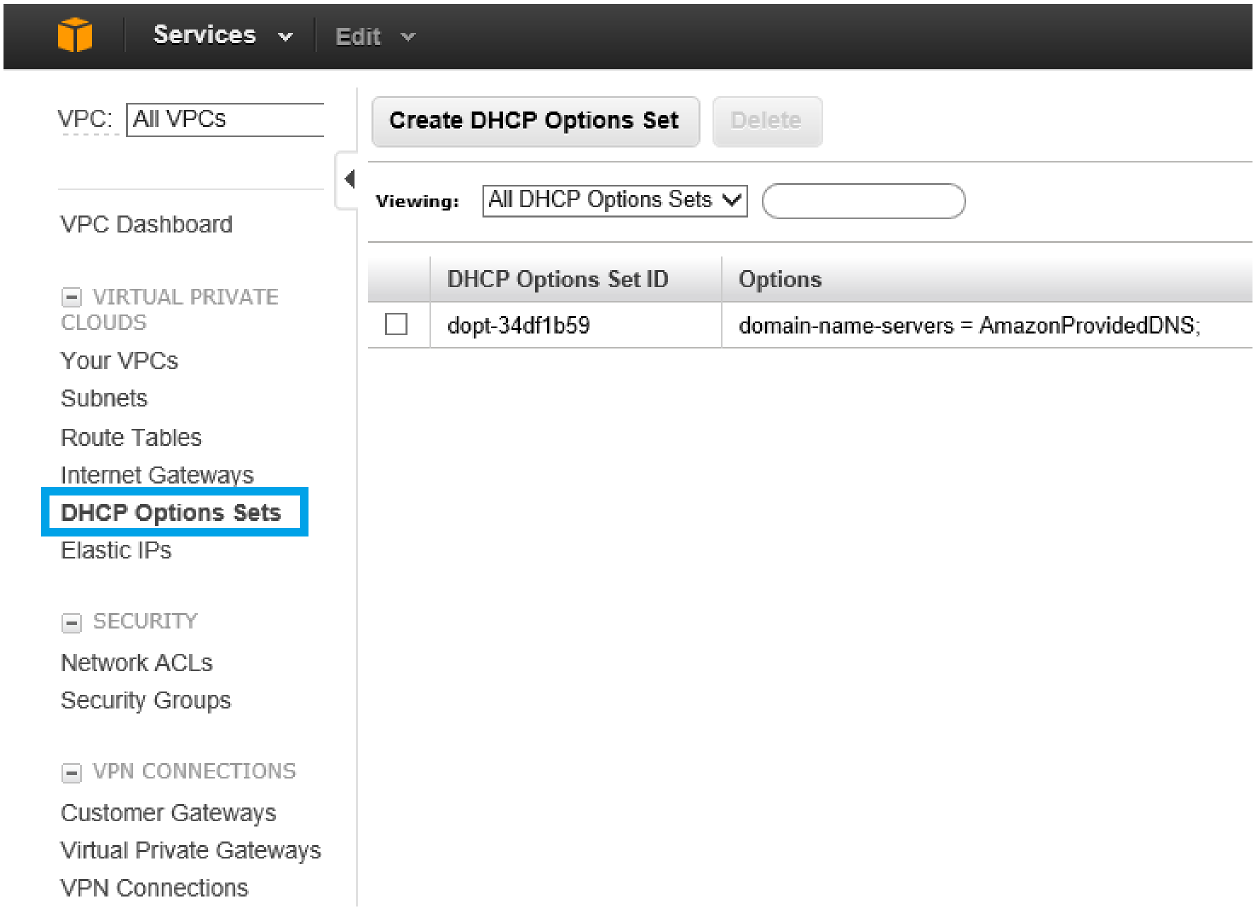
Viewing: All Internet Gateways

	ID	State	VPC
□	igw-39df1b54	● available	vpc-3edf1b53 (10.0.0.0/16)

0 Internet Gateways selected

Select a Internet Gateway above

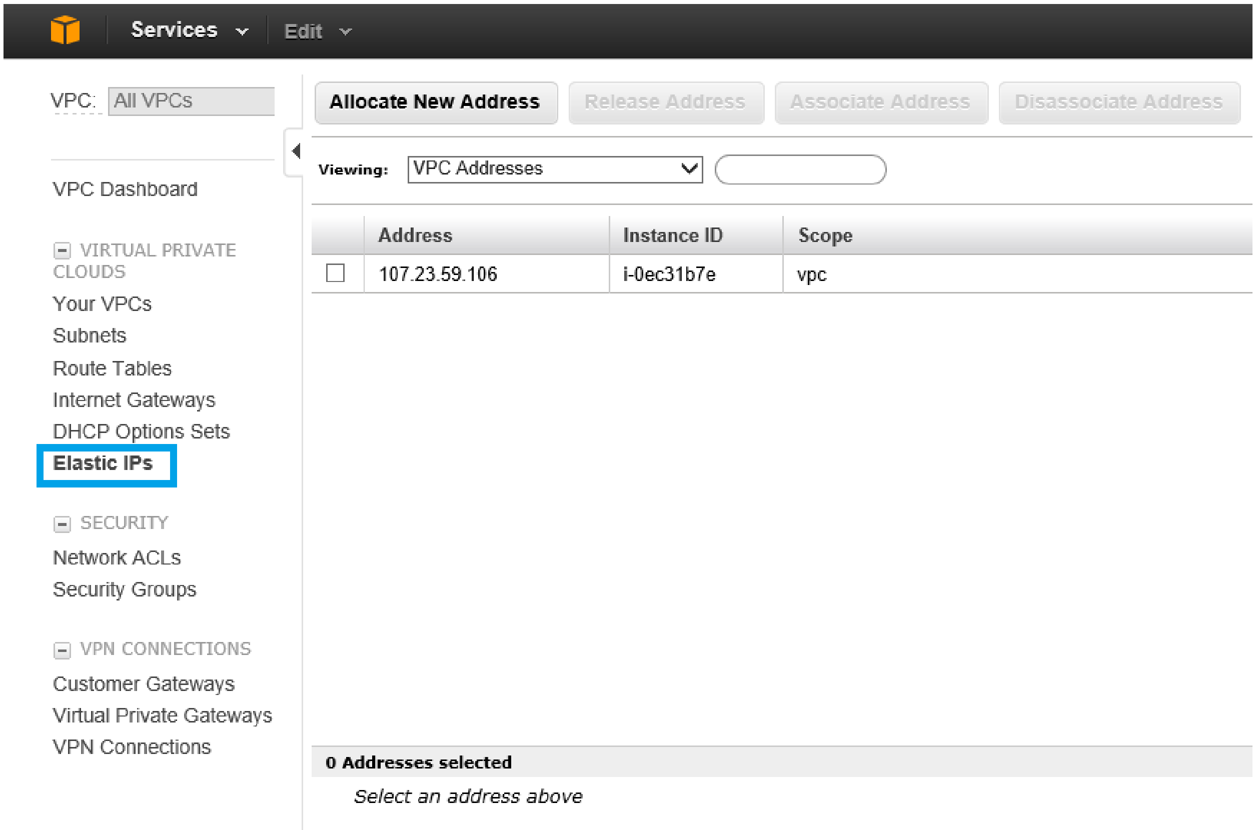
14. In the VPC dashboard, click “DHCP Options Sets” to configure the DHCP options. Click “Create DHCP Options Set” to create a new DHCP option configuration. Click Delete to delete any DHCP option sets. Configure the DHCP options required for your environment.



	DHCP Options Set ID	Options
□	dopt-34df1b59	domain-name-servers = AmazonProvidedDNS;

15. In the VPC dashboard, click “Elastic IPs” to manage elastic IP addresses assigned to the EC2 AMI virtual machines. There can be up to five elastic IP addresses per VPC. Elastic IPs can be dynamically assigned to different EC2 AMI virtual machines in the VPC as required.

    Note: The Elastic IP addresses are static IP addresses that can survive a reboot of an EC2 AMI virtual machine to which it is assigned.



Viewing: VPC Addresses

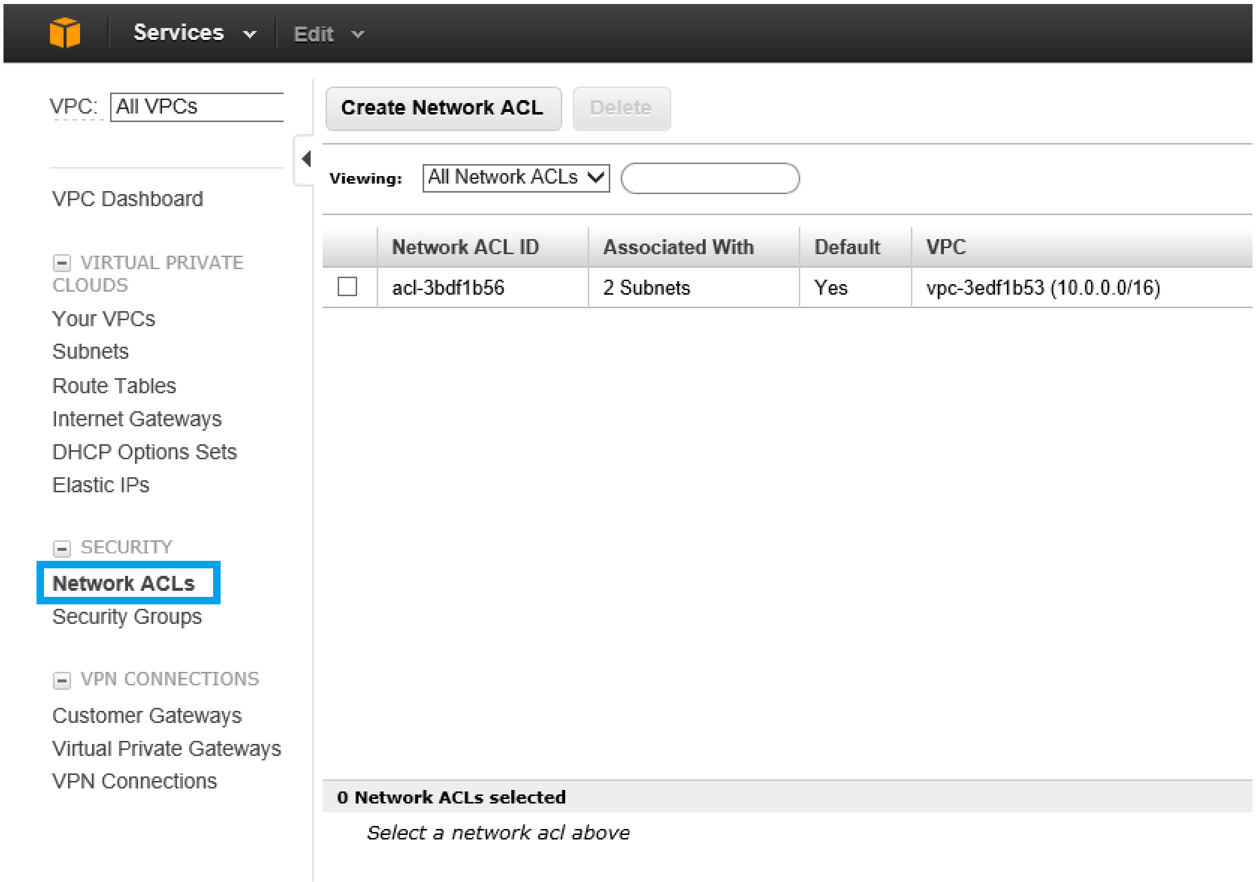
	Address	Instance ID	Scope
□	107.23.59.106	i-0ec31b7e	vpc

0 Addresses selected

Select an address above

16. After the VPC is created and configured, the network security must be set on the VPC. In the VPC dashboard, click “Network ACLs” to bring up the network ACL dashboard. Click “Create Network ACL” to create a new network ACL.

    Note: By default, an inbound and outbound network ACL and a network security group are created when the VPC is created. It is encouraged to use both network ACLs and network security groups to provide in-depth network security.



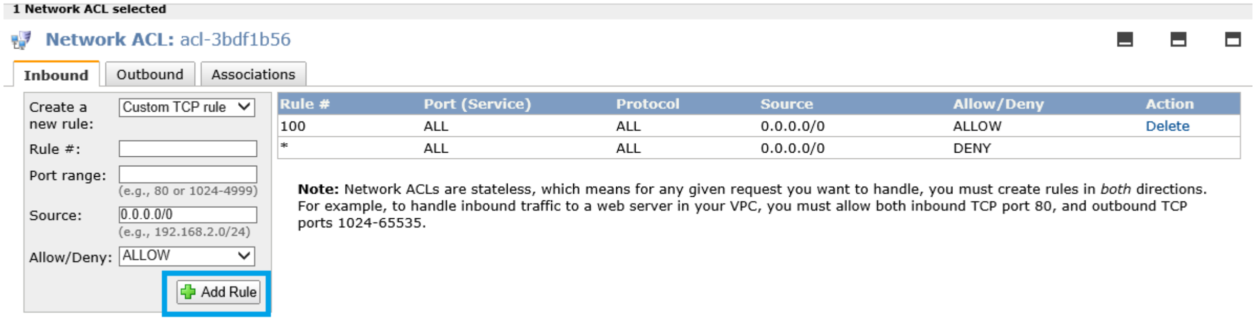
Viewing: All Network ACLs

	Network ACL ID	Associated With	Default	VPC
□	acl-3bdf1b56	2 Subnets	Yes	vpc-3edf1b53 (10.0.0.0/16)

0 Network ACLs selected

Select a network acl above

17. You can also add rules to an existing network ACL by clicking the network ACL and then clicking “Add Rule.” Add any additional ACL rules as required by your environment.



1 Network ACL selected

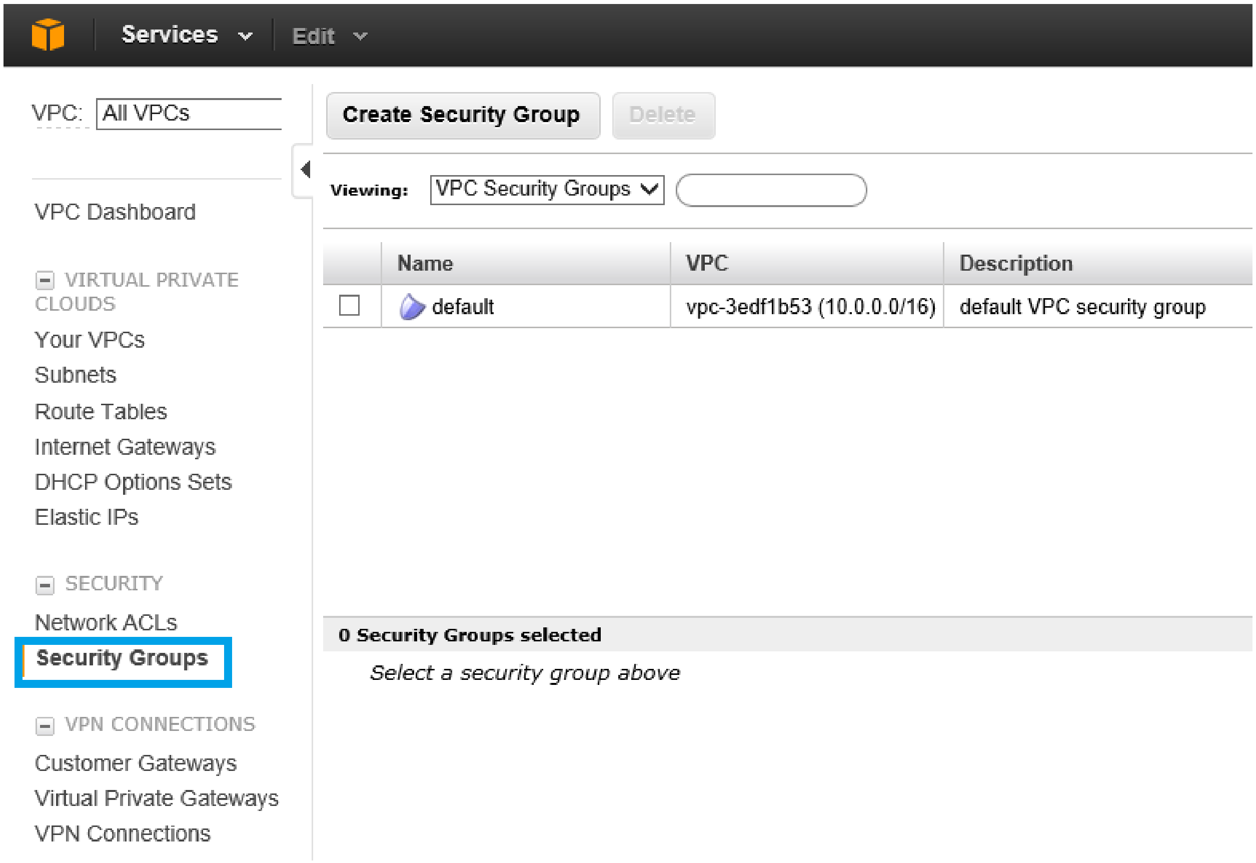
Network ACL: acl-3bdf1b56

Create a new rule:	Custom TCP rule
Rule #:	
Port range:	(e.g., 80 or 1024-4999)
Source:	0.0.0.0/0 (e.g., 192.168.2.0/24)
Allow/Deny:	ALLOW

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

Note: Network ACLs are stateless, which means for any given request you want to handle, you must create rules in *both* directions. For example, to handle inbound traffic to a web server in your VPC, you must allow both inbound TCP port 80, and outbound TCP ports 1024-65535.

18. If the use of network security groups is required, click “Security Groups” in the VPC dashboard to bring up the security groups dashboard. Click “Create Security Group” to create a new security group.



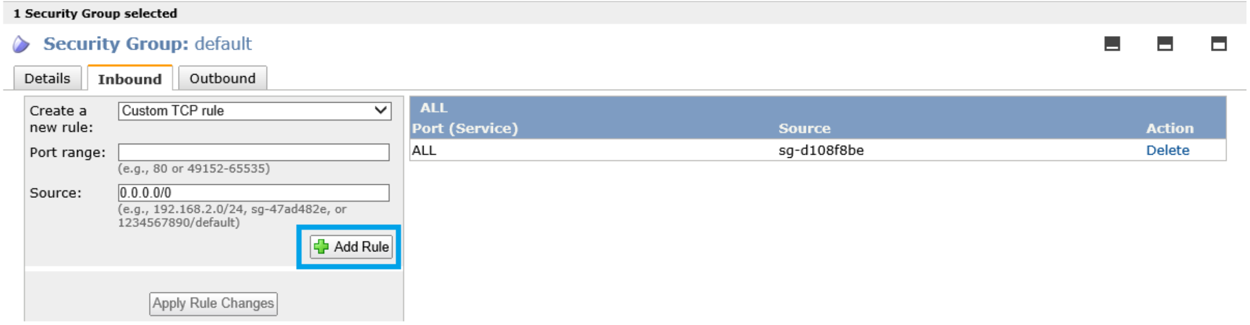
Viewing: VPC Security Groups

	Name	VPC	Description
□	default	vpc-3edf1b53 (10.0.0.0/16)	default VPC security group

0 Security Groups selected

Select a security group above

19. You can also add rules to an existing network security group by clicking the security group and then clicking either the Inbound or Outbound tab. Click “Add Rule” to add any additional security rules as required by your environment.



1 Security Group selected

Security Group: default

Create a new rule: Custom TCP rule

Port range:

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

Source: 0.0.0.0/0

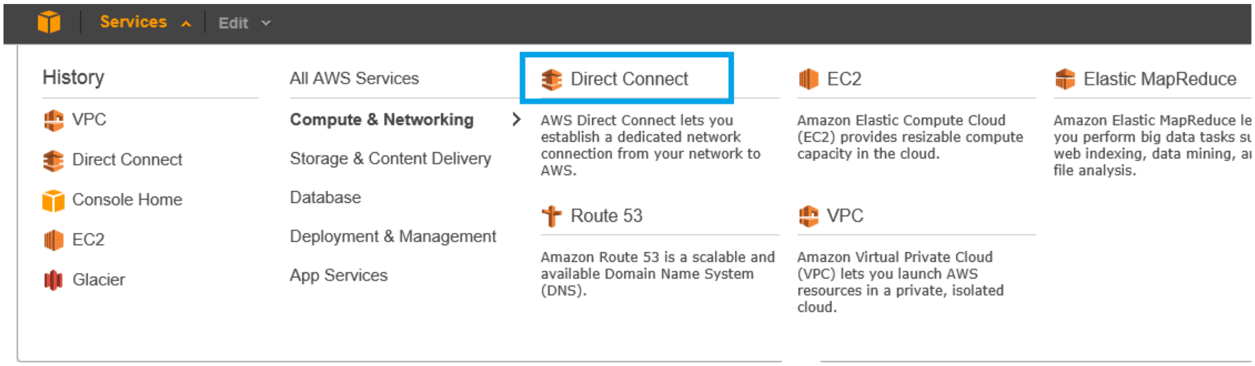
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

ALL

Port (Service)	Source	Action
ALL	sg-d108f8be	Delete

4.2 Create Amazon Direct Connect Network Connection

1. Launch the Direct Connect Network dashboard by clicking Services > Compute & Networking > Direct Connect.



AWS Direct Connect lets you establish a dedicated network connection from your network to AWS.

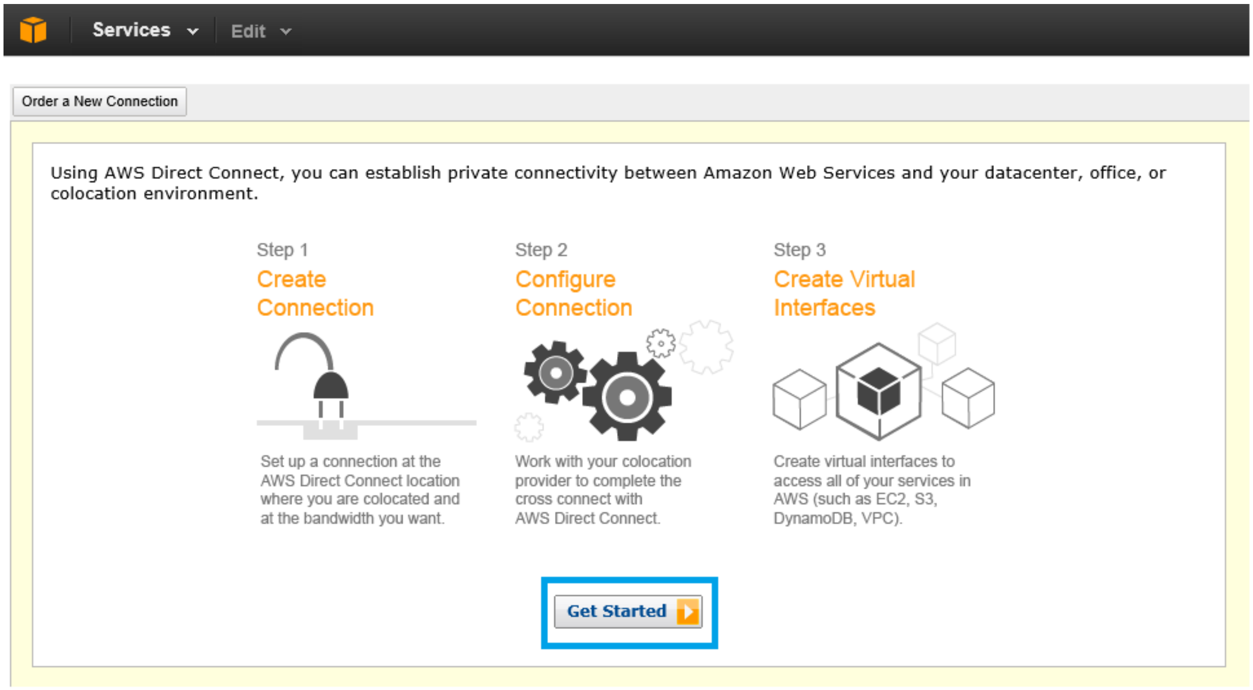
Amazon Elastic Compute Cloud (EC2) provides resizable compute capacity in the cloud.

Amazon Elastic MapReduce le you perform big data tasks su web indexing, data mining, ai file analysis.

Amazon Route 53 is a scalable and available Domain Name System (DNS).

Amazon Virtual Private Cloud (VPC) lets you launch AWS resources in a private, isolated cloud.

2. Click the “Get Started” button to start the Direct Connect wizard.



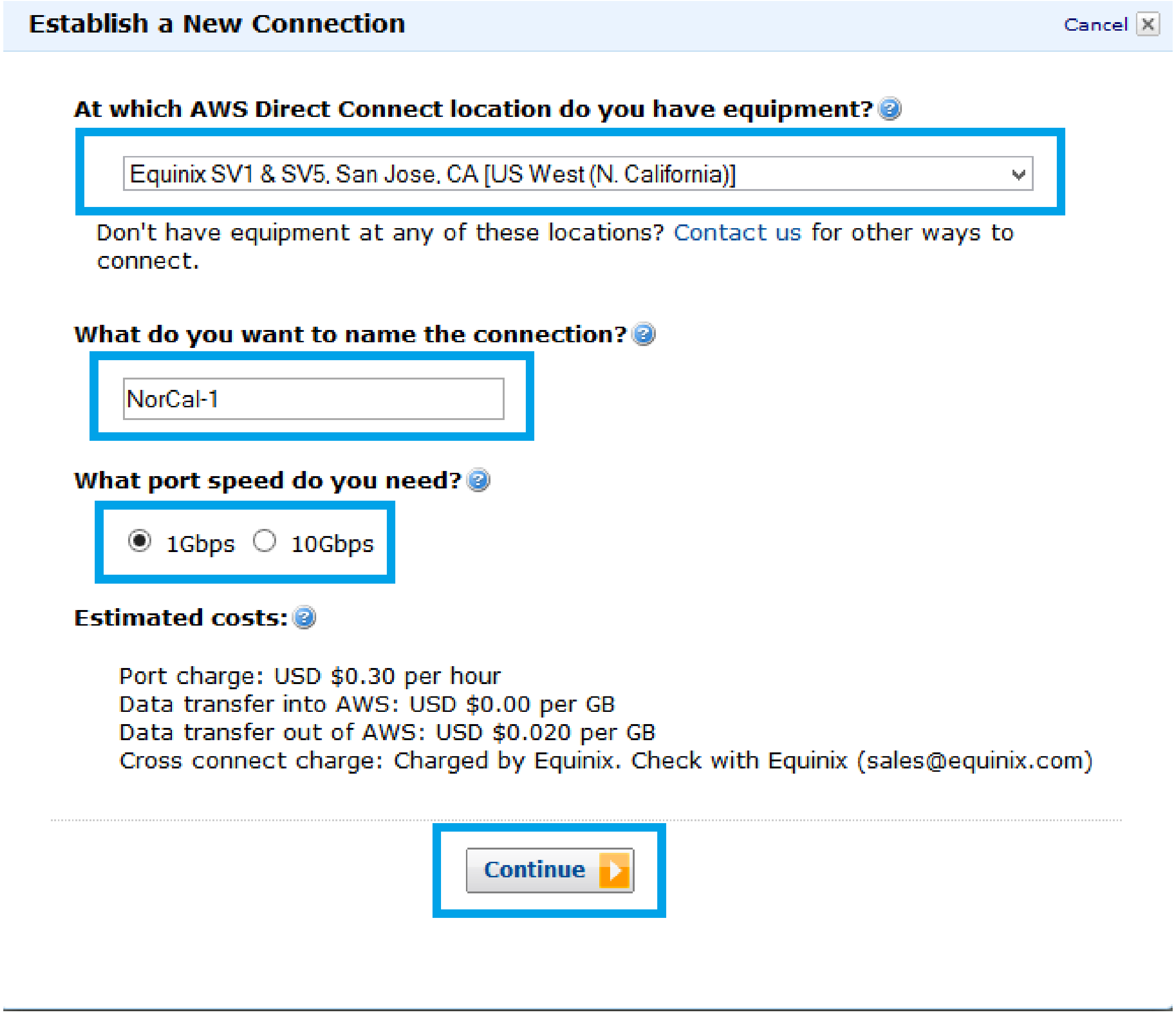
Using AWS Direct Connect, you can establish private connectivity between Amazon Web Services and your datacenter, office, or colocation environment.

Step 1
Create Connection
Set up a connection at the AWS Direct Connect location where you are colocated and at the bandwidth you want.

Step 2
Configure Connection
Work with your colocation provider to complete the cross connect with AWS Direct Connect.

Step 3
Create Virtual Interfaces
Create virtual interfaces to access all of your services in AWS (such as EC2, S3, DynamoDB, VPC).

3. In the “Establish a New Connection” wizard, select the AWS Direct Connect location where the NetApp storage is located (that is, Equinix SV1 and SV5, San Jose, CA). Provide a name for the connection and a port speed for the connection. Click Continue.



Establish a New Connection

At which AWS Direct Connect location do you have equipment?

Equinix SV1 & SV5, San Jose, CA [US West (N. California)]

Don't have equipment at any of these locations? Contact us for other ways to connect.

What do you want to name the connection?

NorCal-1

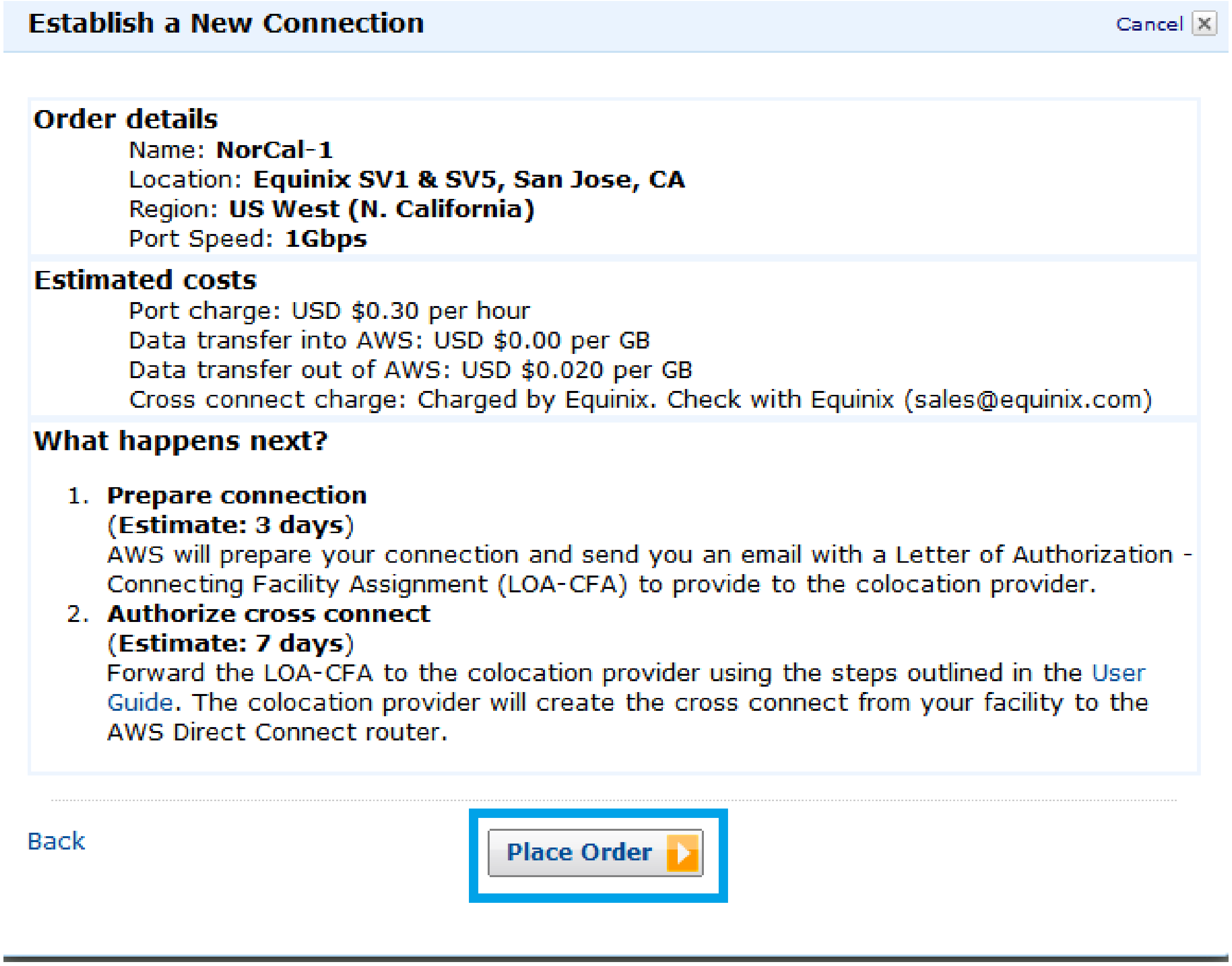
What port speed do you need?

● 1Gbps ○ 10Gbps

Estimated costs:

Port charge: USD $0.30 per hour
Data transfer into AWS: USD $0.00 per GB
Data transfer out of AWS: USD $0.020 per GB
Cross connect charge: Charged by Equinix. Check with Equinix (sales@equinix.com)

4. Review the Direct Connect connection order details. Click Place Order.



Order details

Name: **NorCal-1**
Location: **Equinix SV1 & SV5, San Jose, CA**
Region: **US West (N. California)**
Port Speed: **1Gbps**

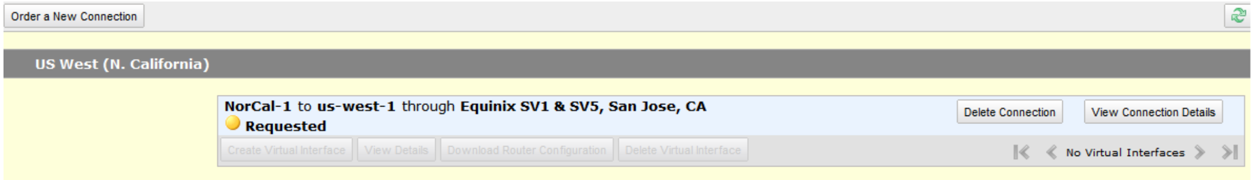
Estimated costs

Port charge: USD $0.30 per hour
Data transfer into AWS: USD $0.00 per GB
Data transfer out of AWS: USD $0.020 per GB
Cross connect charge: Charged by Equinix. Check with Equinix (sales@equinix.com)

What happens next?

1. **Prepare connection**
   (**Estimate: 3 days**)
   AWS will prepare your connection and send you an email with a Letter of Authorization - Connecting Facility Assignment (LOA-CFA) to provide to the colocation provider.
2. **Authorize cross connect**
   (**Estimate: 7 days**)
   Forward the LOA-CFA to the colocation provider using the steps outlined in the User Guide. The colocation provider will create the cross connect from your facility to the AWS Direct Connect router.

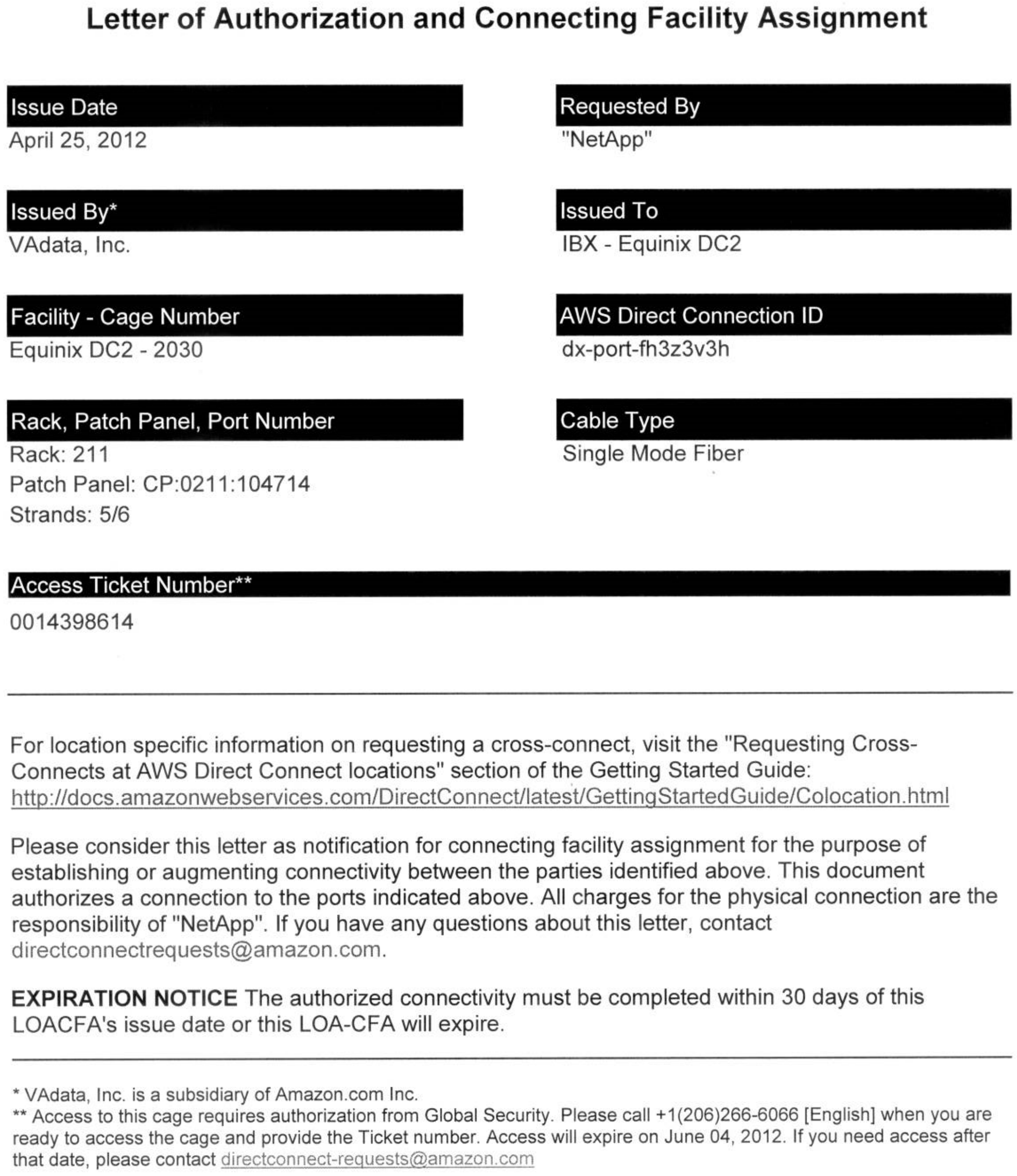
5. Verify that the new order is listed in the Order New Connection dashboard.



NorCal-1 to **us-west-1** through **Equinix SV1 & SV5, San Jose, CA**
Requested

6. Follow the procedures listed in the AWS Direct Connect User Guide, to request a cross connect (LOA-CFA). Each location has different procedures for requesting a cross connect. This request will create a ticket to the colocation provider so that they can physically wire the cross connect between AWS and the router in the cage where the NetApp storage is located. Figure 1 shows a sample letter of authorization and connecting facility assignment (LOA-CFA).

Figure 2) Sample letter of authorization.



Letter of Authorization and Connecting Facility Assignment

Issue Date	Requested By
April 25, 2012	"NetApp"
Issued By*	Issued To
VAdata, Inc.	IBX - Equinix DC2
Facility - Cage Number	AWS Direct Connection ID
Equinix DC2 - 2030	dx-port-fh3z3v3h
Rack, Patch Panel, Port Number	Cable Type
Rack: 211 Patch Panel: CP:0211:104714 Strands: 5/6	Single Mode Fiber

Access Ticket Number**

0014398614

For location specific information on requesting a cross-connect, visit the "Requesting Cross-Connects at AWS Direct Connect locations" section of the Getting Started Guide: http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Colocation.html

Please consider this letter as notification for connecting facility assignment for the purpose of establishing or augmenting connectivity between the parties identified above. This document authorizes a connection to the ports indicated above. All charges for the physical connection are the responsibility of "NetApp". If you have any questions about this letter, contact directconnectrequests@amazon.com.

EXPIRATION NOTICE The authorized connectivity must be completed within 30 days of this LOACFA's issue date or this LOA-CFA will expire.

* VAdata, Inc. is a subsidiary of Amazon.com Inc.

** Access to this cage requires authorization from Global Security. Please call +1(206)266-6066 [English] when you are ready to access the cage and provide the Ticket number. Access will expire on June 04, 2012. If you need access after that date, please contact directconnect-requests@amazon.com

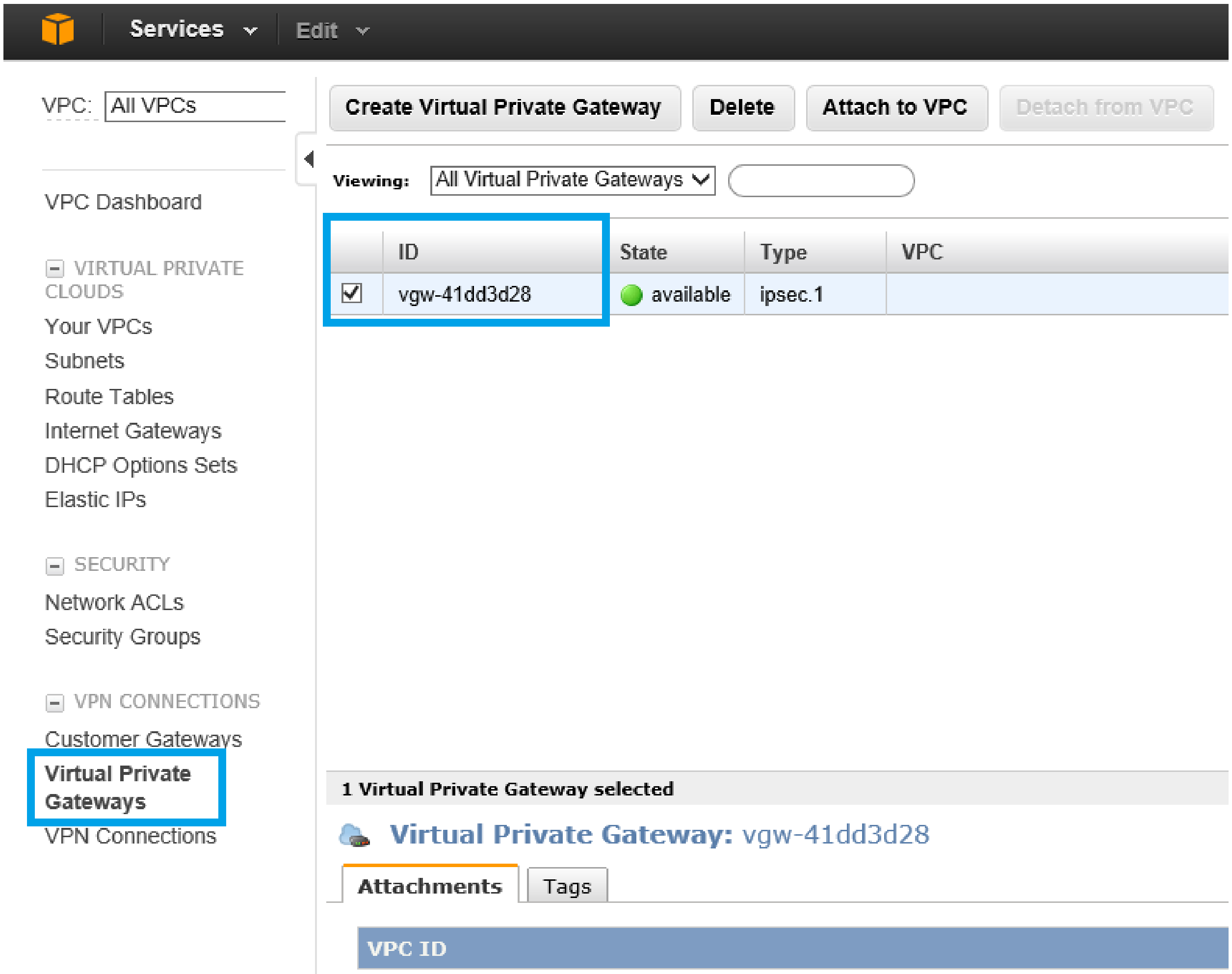
7. In addition to the LOA-CFA, provide the following information to the colocation provider:
   - A pair of private IP addresses in the 169.xxx.xxx.xxx range to use for the routing interfaces
   - The virtual gateway ID (VGW-ID) of the VPC you want to connect using this Direct Connect link
   - A pair of private autonomous system numbers (ASNs) for the connection

   Note: If you use a public ASN, make sure that you own the ASN. For private ASNs, make sure that they are unique.

   - A VLAN ID for traffic routed to and from AWS
   - BGP secret configuration information

8. In the VPC dashboard, click “Virtual Private Gateways” to view the virtual gateway ID (VGW-ID) configured for the VPC. Document the VGW-ID because you will need to provide this to the colocation provider.

   Note: A virtual private gateway is the router on the AWS network that connects your VPC to the Direct Connect Connection or other virtual private clouds.



VPC: All VPCs

Viewing: All Virtual Private Gateways

	ID	State	Type	VPC
☑	vgw-41dd3d28	● available	ipsec.1	

1 Virtual Private Gateway selected

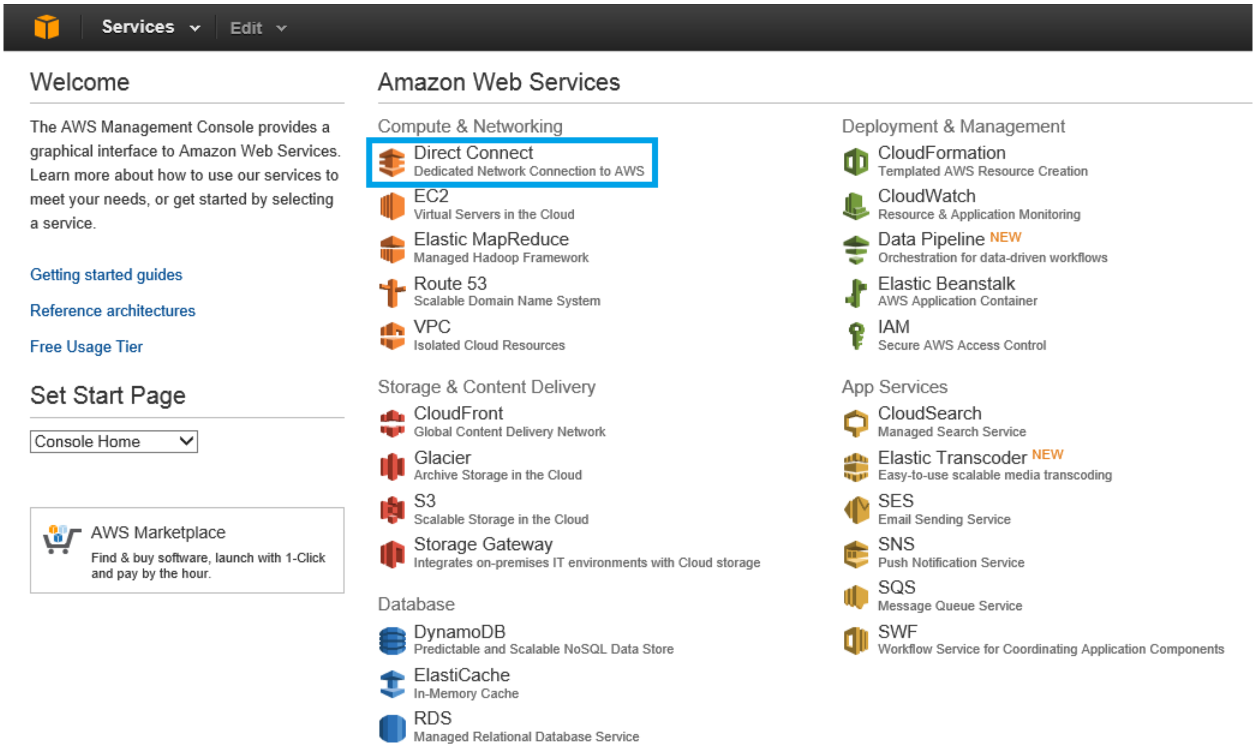
Virtual Private Gateway: vgw-41dd3d28

VPC ID

9. Repeat steps 1 through 8 for each additional virtual private cloud. Each virtual private cloud will be listed in the VPC dashboard.

4.3 Configure Network Router (BGP) in Colocation Facility

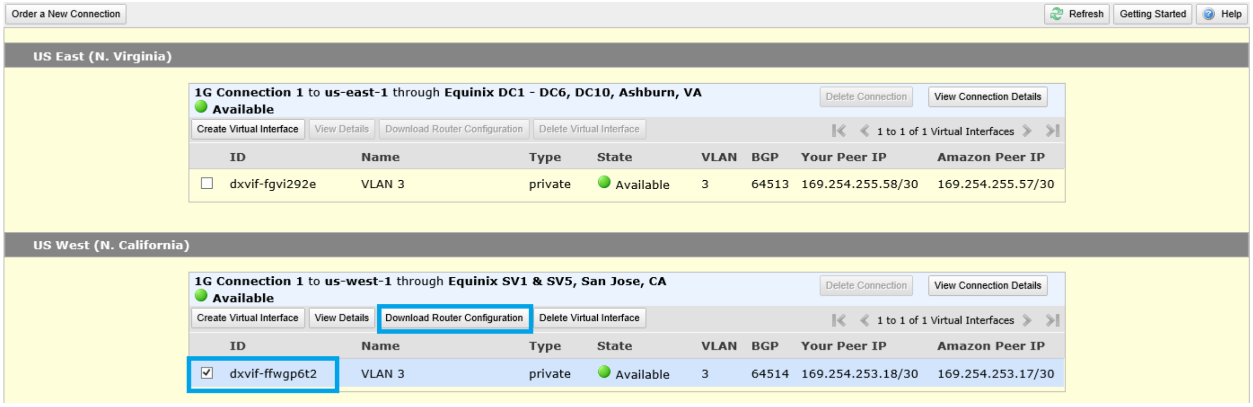
1. After the Direct Connect cross-connect has been patched, open the AWS management console and click the Direct Connect link to launch the Direct Connect dashboard.



The AWS Management Console provides a graphical interface to Amazon Web Services. Learn more about how to use our services to meet your needs, or get started by selecting a service.

Services
Edit
Welcome
Getting started guides
Reference architectures
Free Usage Tier
Set Start Page
Console Home
AWS Marketplace
Find & buy software, launch with 1-Click and pay by the hour.
Amazon Web Services
Compute & Networking
Direct Connect
Dedicated Network Connection to AWS
EC2
Virtual Servers in the Cloud
Elastic MapReduce
Managed Hadoop Framework
Route 53
Scalable Domain Name System
VPC
Isolated Cloud Resources
Storage & Content Delivery
CloudFront
Global Content Delivery Network
Glacier
Archive Storage in the Cloud
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates on-premises IT environments with Cloud storage
Database
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
RDS
Managed Relational Database Service
Deployment & Management
CloudFormation
Templated AWS Resource Creation
CloudWatch
Resource & Application Monitoring
Data Pipeline NEW
Orchestration for data-driven workflows
Elastic Beanstalk
AWS Application Container
IAM
Secure AWS Access Control
App Services
CloudSearch
Managed Search Service
Elastic Transcoder NEW
Easy-to-use scalable media transcoding
SES
Email Sending Service
SNS
Push Notification Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components

2. In the Direct Connect dashboard, click the Direct Connect connection ID checkbox. Click “Download Router Configuration.”



US East (N. Virginia)

1G Connection 1 to us-east-1 through Equinix DC1 - DC6, DC10, Ashburn, VA
Available

	ID	Name	Type	State	VLAN	BGP	Your Peer IP	Amazon Peer IP
☐	dxvif-fgvi292e	VLAN 3	private	● Available	3	64513	169.254.255.58/30	169.254.255.57/30

US West (N. California)

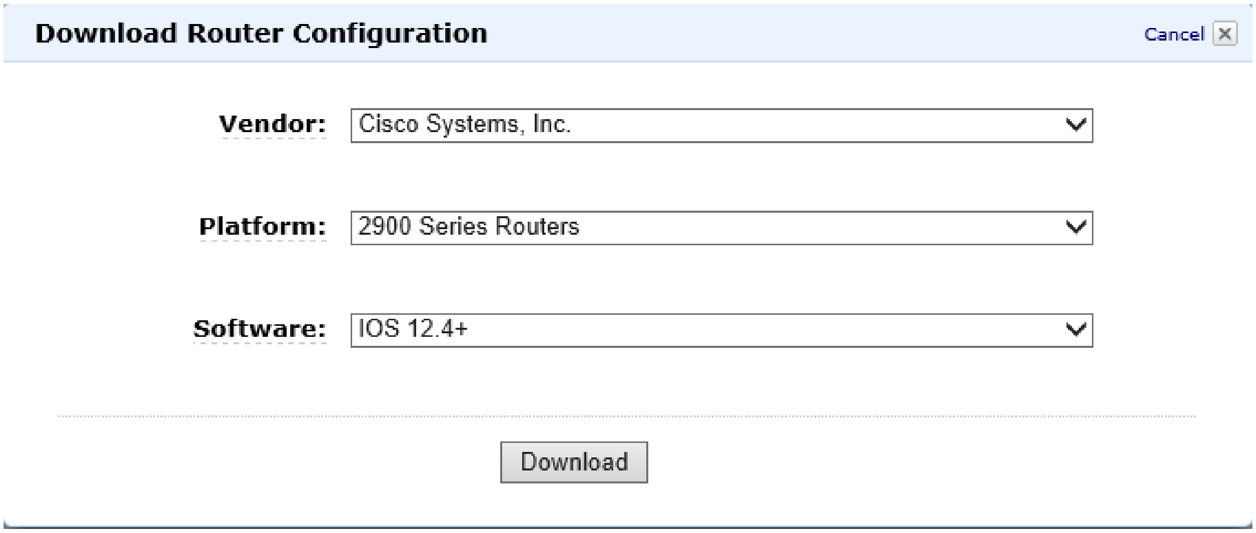
1G Connection 1 to us-west-1 through Equinix SV1 & SV5, San Jose, CA
Available

	ID	Name	Type	State	VLAN	BGP	Your Peer IP	Amazon Peer IP
☑	dxvif-ffwgp6t2	VLAN 3	private	● Available	3	64514	169.254.253.18/30	169.254.253.17/30

3. In the “Download Router Configuration” dialog box, select the appropriate values for the router configuration for your environment:
   - Vendor: The options are Cisco or Juniper.
   - Platform: The options are model numbers depending on the vendor type selected.
   - Software: The options are switch operating system versions that are dependent on the vendor and platform types selected.

Note: If you are not using a Cisco or Juniper router, document the AWS BGP secret and ASN and use that information to configure BGP.

4. After making the appropriate selections, click Download.



Vendor: Cisco Systems, Inc.

Platform: 2900 Series Routers

Software: IOS 12.4+

5. Save the AWS Direct Connect router configuration to a text file. The text file will contain the ASN and BGP secret used by the AWS Direct Connect router. Open the file in a text editor. The following is a sample BGP router configuration for a Cisco 2900+ router running Cisco IOS® Software 12.4+:

```
! Amazon Web Services
! Direct Connect
! Virtual Interface ID: dxvif-ffwgp6t2
!
! --------------------------------------------------------------------------------
! Interface Configuration

interface GigabitEthernet0/1
  no ip address

interface GigabitEthernet0/1.3
  description "Direct Connect to your Amazon VPC or AWS Cloud"
  encapsulation dot1Q 3
  ip address 169.254.253.18 255.255.255.252

! --------------------------------------------------------------------------------
! Border Gateway Protocol (BGP) Configuration
!
! BGP is used to exchange prefixes between the Direct Connect Router and your
! Customer Gateway.
!
! Your Customer Gateway may announce a default route (0.0.0.0/0),
! which can be done with the 'network' and 'default-originate' statements.
!
! To advertise additional prefixes, copy the 'network' statement and identify the
! prefix you wish to advertise. Make sure the prefix is present in the routing
! table of the device with a valid next-hop.
!
! The local BGP Autonomous System Number (ASN) (64514) is configured as
! part of your Customer Gateway. If the ASN must be changed, the Customer Gateway
! and Direct Connect Virtual Interface will need to be recreated with AWS.

router bgp 64514
  neighbor 169.254.253.17 remote-as 7224
  neighbor 169.254.253.17 password xxxxxxxxxxxxxxxxxxxxxxx
  network 0.0.0.0
exit
```

```
! Additional Notes and Questions
!  - Amazon Web Services Direct Connect Getting Started Guide:
!       http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html
```

6. On the network router, configure BGP to advertise routes to AWS and receive BGP advertisements from AWS.

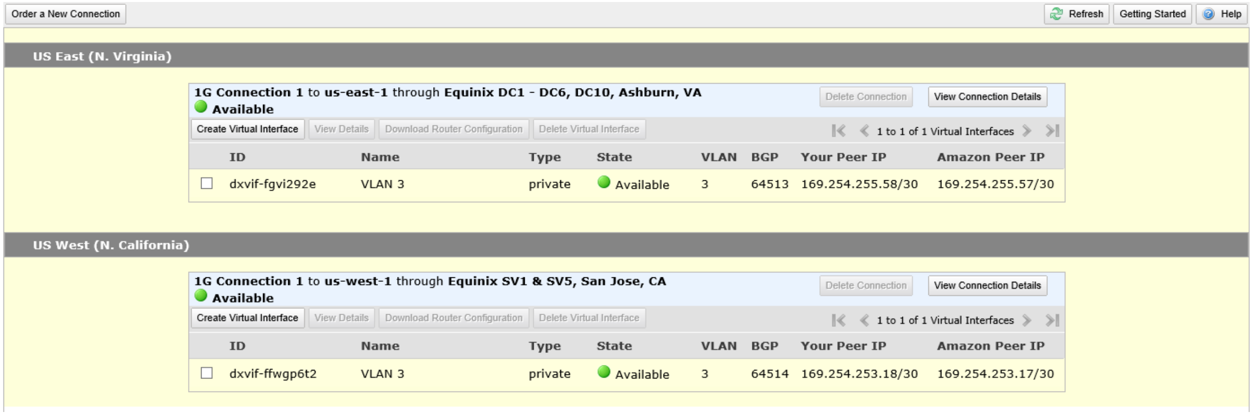
Note: BGP relies on autonomous system numbers to identify networks for routing purposes. The customer-provided router in the colocation facility is assigned an AS number. This number must be unique and not conflict with any reserved AS numbers that Amazon uses. Use the BGP configuration information from the router configuration downloaded from the Direct Connect dashboard and apply this configuration to the customer-provided router.

Note: The following is a sample configuration for a Cisco 2900 router. Note the BGP configuration section:

```
POC-4908-SV#show run
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname POC-4908-SV
!
enable secret 5 xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
enable password xxxxxx
!
ip subnet-zero
bridge irb
!
!
!
interface GigabitEthernet1
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface GigabitEthernet1.10
 encapsulation dot1Q 10
 no ip directed-broadcast
 bridge-group 10
!
interface GigabitEthernet1.11
 encapsulation dot1Q 11
 no ip directed-broadcast
 bridge-group 11
!
interface GigabitEthernet1.12
 encapsulation dot1Q 12
 no ip directed-broadcast
 bridge-group 12
!
interface GigabitEthernet2
 no ip address
 no ip directed-broadcast
!
interface GigabitEthernet2.1
 encapsulation dot1Q 3
 no ip directed-broadcast
 bridge-group 2
!
interface GigabitEthernet3
 no ip address
 no ip directed-broadcast
!
interface GigabitEthernet4
 no ip address
 no ip directed-broadcast
 shutdown
!
interface GigabitEthernet5
 no ip address
 no ip directed-broadcast
 shutdown
!
interface GigabitEthernet6
 no ip address
 no ip directed-broadcast
 shutdown
!
interface GigabitEthernet7
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface GigabitEthernet7.1
 encapsulation dot1Q 3
 ip address 169.254.253.18 255.255.255.252
 no ip directed-broadcast
!
interface GigabitEthernet8
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface GigabitEthernet8.3
 encapsulation dot1Q 3
 no ip directed-broadcast
 bridge-group 2
!
interface GigabitEthernet8.10
 encapsulation dot1Q 10
 no ip directed-broadcast
 bridge-group 10
!
interface GigabitEthernet8.11
 encapsulation dot1Q 11
 no ip directed-broadcast
 bridge-group 11
!
interface GigabitEthernet8.12
 encapsulation dot1Q 12
 no ip directed-broadcast
 bridge-group 12
!
interface BVI2
 ip address 192.168.1.100 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
!
interface BVI3
 no ip address
 no ip directed-broadcast
 no ip route-cache cef
 shutdown
!
interface BVI10
 ip address 10.10.10.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
!
interface BVI11
 ip address 10.10.11.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
!
interface BVI12
 ip address 10.10.12.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache cef
!
router bgp 64514
 network 10.10.10.0 mask 255.255.255.0
 network 192.168.1.0
 neighbor 169.254.253.17 remote-as 7224
 neighbor 169.254.253.17 password xxxxxxxxxxxxxxxxxxxxxxxx
!
ip classless
!
```

7. After the Direct Connect connection is established and the BGP configuration is set up, the status of the Direct Connect connection will change to green in the Direct Connect dashboard.



US East (N. Virginia)

1G Connection 1 to **us-east-1** through **Equinix DC1 - DC6, DC10, Ashburn, VA**
● **Available**

	ID	Name	Type	State	VLAN	BGP	Your Peer IP	Amazon Peer IP
□	dxvif-fgvi292e	VLAN 3	private	● Available	3	64513	169.254.255.58/30	169.254.255.57/30

US West (N. California)

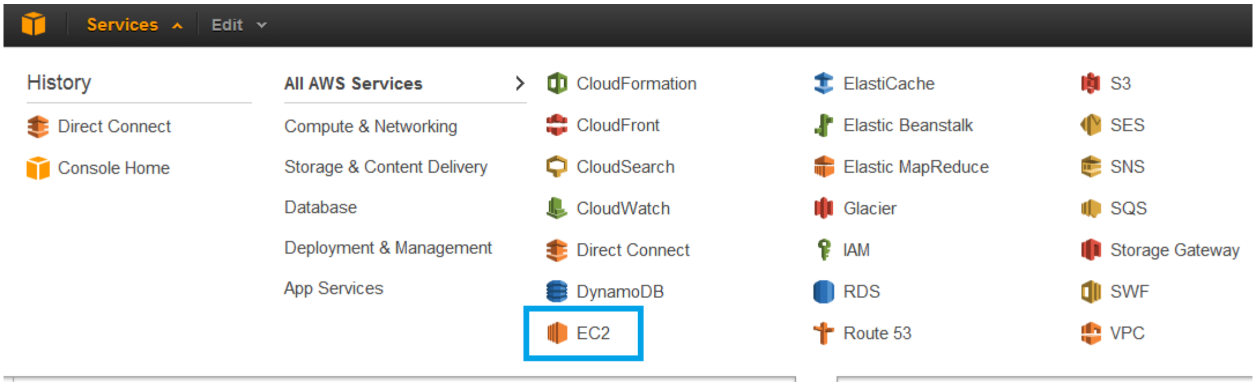
1G Connection 1 to **us-west-1** through **Equinix SV1 & SV5, San Jose, CA**
● **Available**

	ID	Name	Type	State	VLAN	BGP	Your Peer IP	Amazon Peer IP
□	dxvif-ffwgp6t2	VLAN 3	private	● Available	3	64514	169.254.253.18/30	169.254.253.17/30

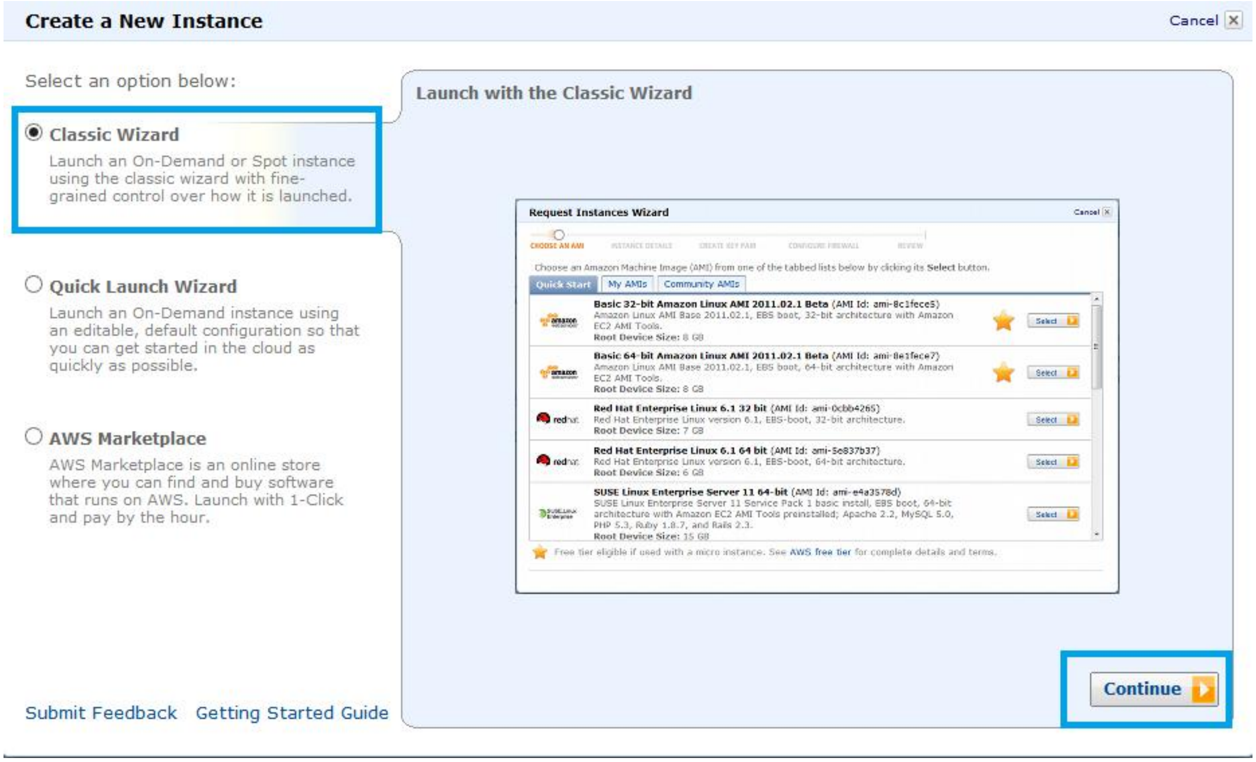
8. Repeat steps 1 through 7 for each additional Direct Connect connection. Each Direct Connect connection will be listed in the Direct Connect dashboard.

4.4 Create AWS AMI Virtual Machines

1. Launch the EC2 dashboard, by clicking Services > Compute & Networking > EC2.



2. In the EC2 dashboard, click “Launch Instance” to start the “Create a New Instance” wizard. Select the Wizard option (that is, Classic Wizard) and click Continue.



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.

Launch with the Classic Wizard

Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

Basic 32-bit Amazon Linux AMI 2011.02.1 Beta (AMI Id: ami-8c1fece5)
Amazon Linux AMI Base 2011.02.1, EBS boot, 32-bit architecture with Amazon EC2 AMI Tools.
Root Device Size: 8 GB

Basic 64-bit Amazon Linux AMI 2011.02.1 Beta (AMI Id: ami-8e1fece7)
Amazon Linux AMI Base 2011.02.1, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools.
Root Device Size: 8 GB

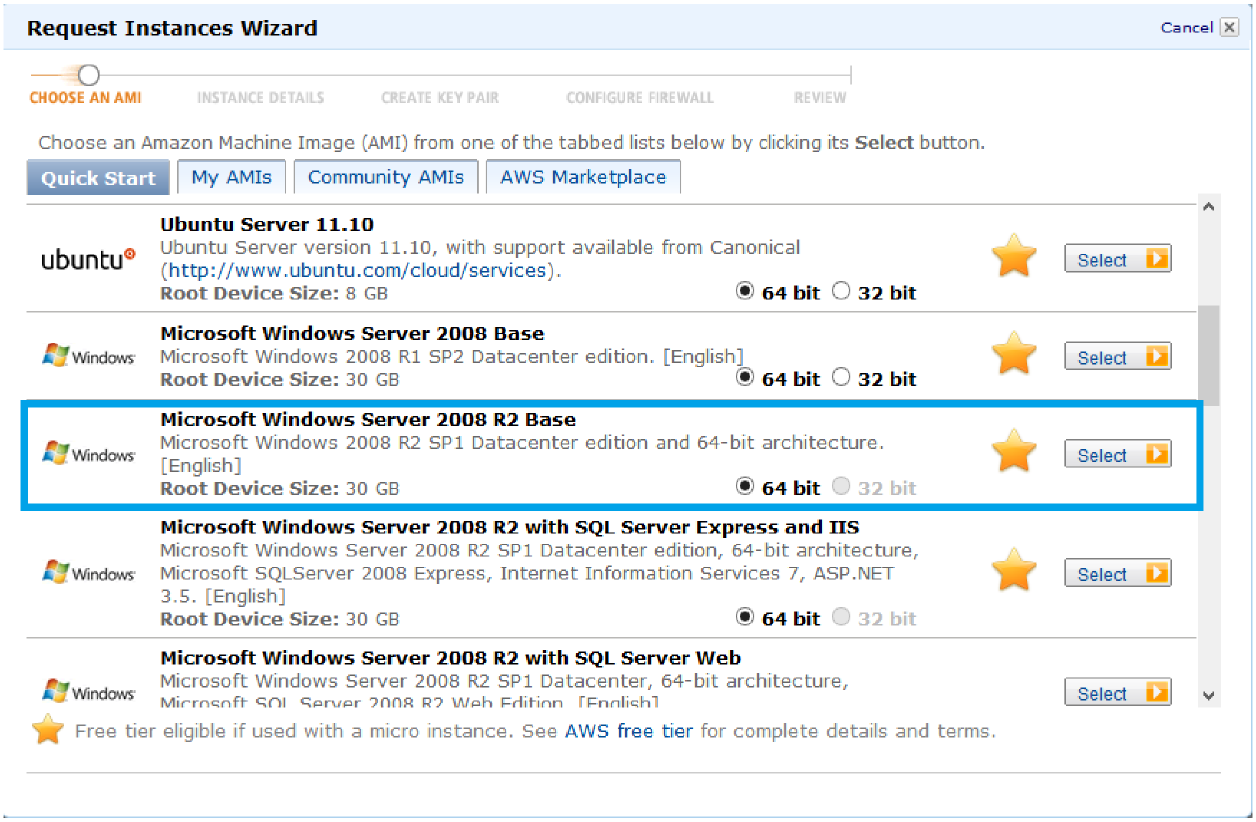
Red Hat Enterprise Linux 6.1 32 bit (AMI Id: ami-0cbb4265)
Red Hat Enterprise Linux version 6.1, EBS-boot, 32-bit architecture.
Root Device Size: 7 GB

Red Hat Enterprise Linux 6.1 64 bit (AMI Id: ami-5e837b37)
Red Hat Enterprise Linux version 6.1, EBS-boot, 64-bit architecture.
Root Device Size: 6 GB

SUSE Linux Enterprise Server 11 64-bit (AMI Id: ami-e4a3578d)
SUSE Linux Enterprise Server 11 Service Pack 1 basic install, EBS boot, 64-bit architecture with Amazon EC2 AMI Tools preinstalled; Apache 2.2, MySQL 5.0, PHP 5.3, Ruby 1.8.7, and Rails 2.3.
Root Device Size: 15 GB

Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.

3. Select an Amazon Machine Image (AMI) from the catalog in the request instances wizard. Click Select next to the desired AMI (that is, Microsoft® Windows® 2008 R2 Base 64-bit).



Choose an Amazon Machine Image (AMI) from one of the tabbed lists below by clicking its **Select** button.

Ubuntu Server 11.10
Ubuntu Server version 11.10, with support available from Canonical (http://www.ubuntu.com/cloud/services).
Root Device Size: 8 GB ● 64 bit ○ 32 bit

Microsoft Windows Server 2008 Base
Microsoft Windows 2008 R1 SP2 Datacenter edition. [English]
Root Device Size: 30 GB ● 64 bit ○ 32 bit

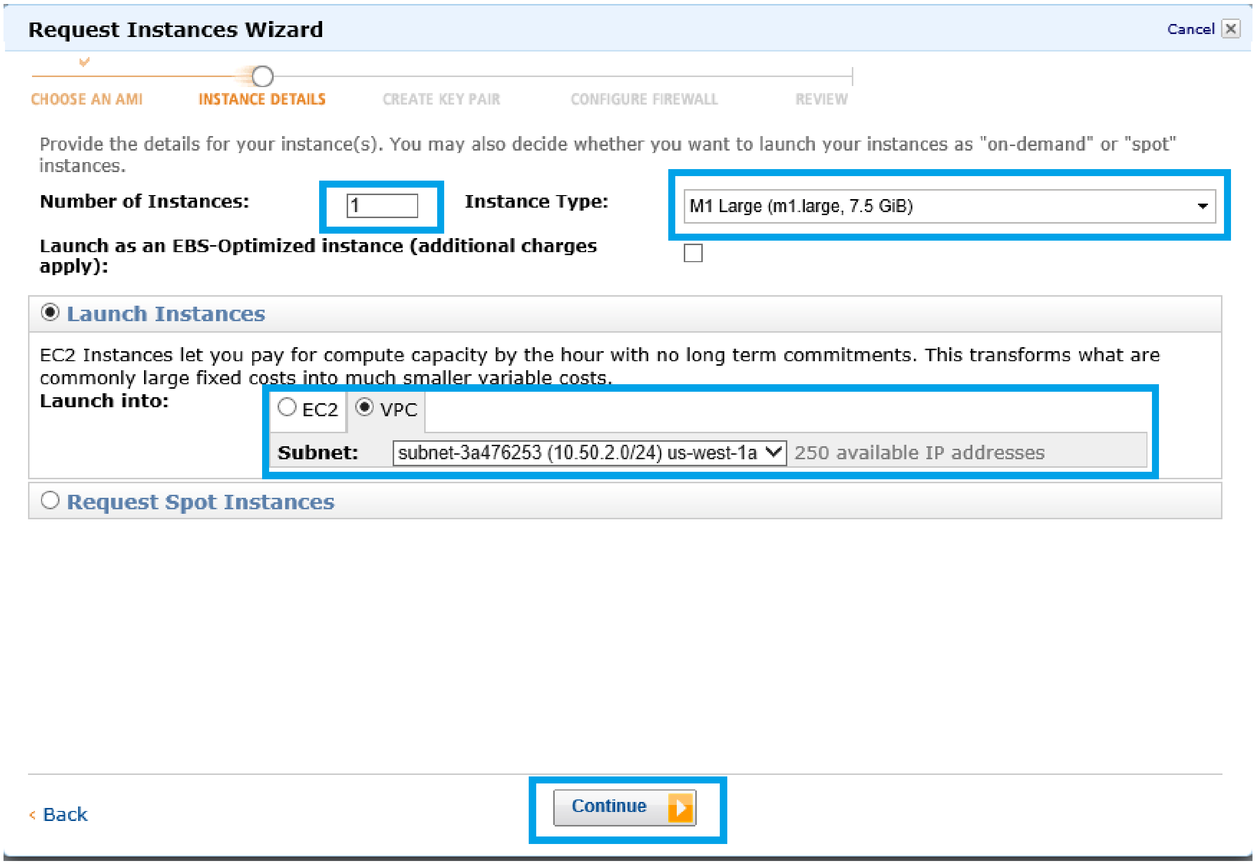
Microsoft Windows Server 2008 R2 Base
Microsoft Windows 2008 R2 SP1 Datacenter edition and 64-bit architecture. [English]
Root Device Size: 30 GB ● 64 bit ○ 32 bit

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]
Root Device Size: 30 GB ● 64 bit ○ 32 bit

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

Free tier eligible if used with a micro instance. See AWS free tier for complete details and terms.

4. In the Request Instances Wizard, select the following information:
   - Number of instances: This is the number of instances to be created (that is, 1).
   - Instance type: This is the type of instances associated with the AMI image (that is, M1 medium).
   - Launch instances: Select the VPC and the desired subnet assigned to the VPC.
5. Click Continue.



Request Instances Wizard

Provide the details for your instance(s). You may also decide whether you want to launch your instances as "on-demand" or "spot" instances.

Number of Instances: 1

Instance Type: M1 Large (m1.large, 7.5 GiB)

Launch as an EBS-Optimized instance (additional charges apply): □

● Launch Instances

EC2 Instances let you pay for compute capacity by the hour with no long term commitments. This transforms what are commonly large fixed costs into much smaller variable costs.

Launch into: ○ EC2 ● VPC

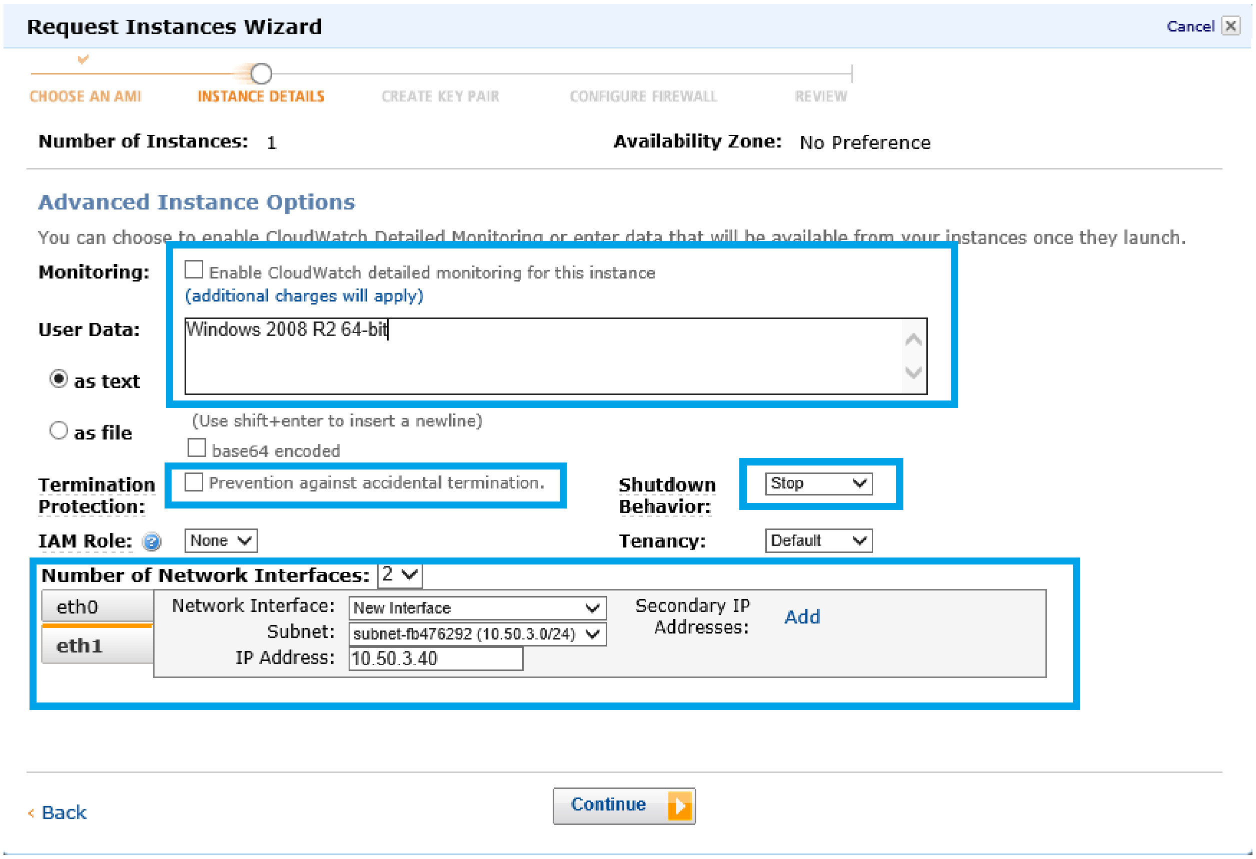
Subnet: subnet-3a476253 (10.50.2.0/24) us-west-1a 250 available IP addresses

○ Request Spot Instances

6. Under the “Advanced Instance Options,” set CloudWatch monitoring for the instance, user data describing the instance, termination protection, and shutdown behavior. Select the number of network interfaces for the instance (that is, 2).

   Note: Review the SAN Configuration Guide for the version of NetApp Data ONTAP used in the architecture. Starting with Data ONTAP 8.1, the SAN Configuration Guide is a part of the Data ONTAP product documentation. This guide provides recommendations on the iSCSI network design and VLAN configurations. For redundant iSCSI connectivity to the NetApp storage, configure multiple Direct Connect connections. Each iSCSI session would use a different Direct Connect network connection. It is also recommended to use redundant network switches in the colocation facility to protect against switch failure.

7. Click Continue.



Number of Instances: 1

Availability Zone: No Preference

Advanced Instance Options

You can choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Monitoring: □ Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

User Data: Windows 2008 R2 64-bit

● as text

○ as file

(Use shift+enter to insert a newline)

□ base64 encoded

Termination Protection: □ Prevention against accidental termination.

Shutdown Behavior: Stop

IAM Role: None

Tenancy: Default

Number of Network Interfaces: 2

eth0

eth1

Network Interface: New Interface

Subnet: subnet-fb476292 (10.50.3.0/24)

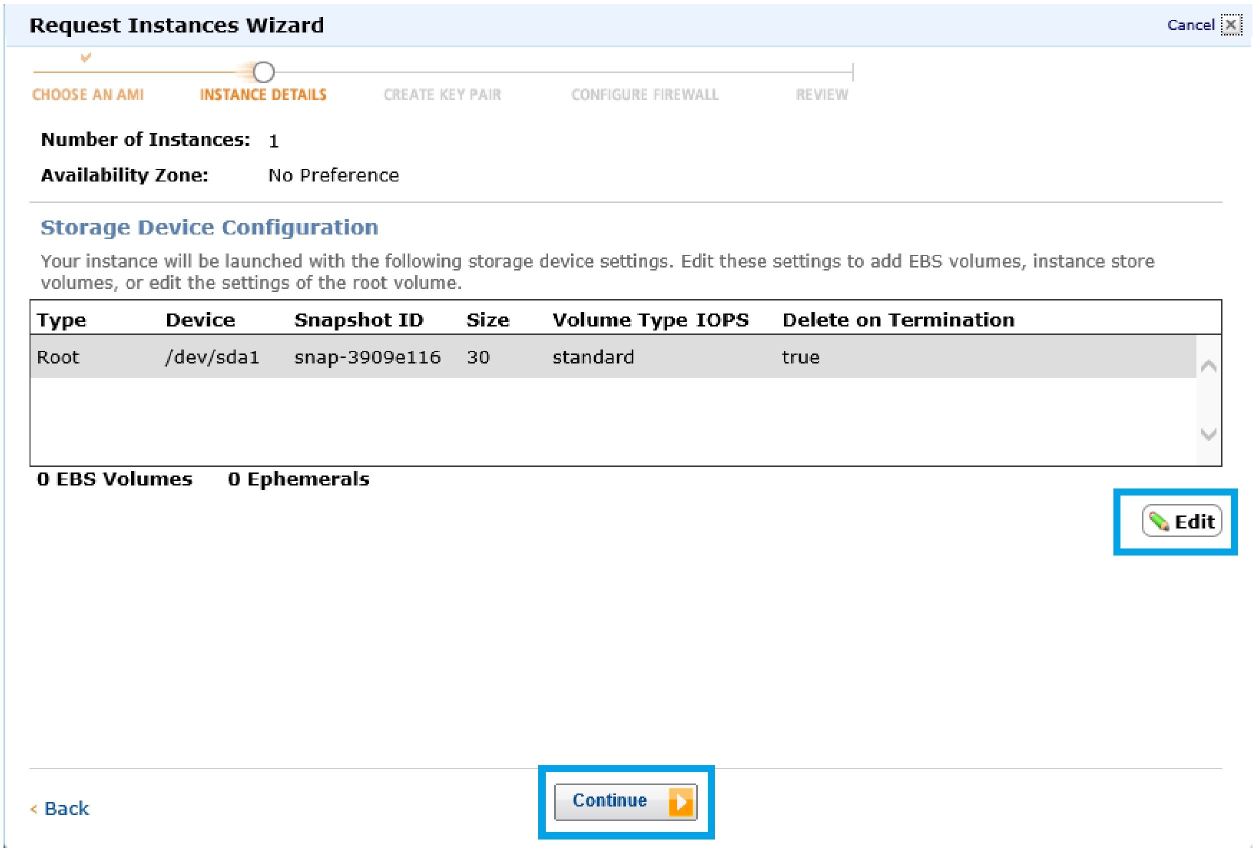
IP Address: 10.50.3.40

Secondary IP Addresses: Add

8. In “Storage Device Configuration,” click Edit to set storage options for the AMI instance.

   Note: If you click Edit, you can set the size of the root volume for the instance, set the volume type, assign Amazon EBS storage, and instance store volumes.

9. After setting the desired instance storage options, click Continue.



Number of Instances: 1

Availability Zone: No Preference

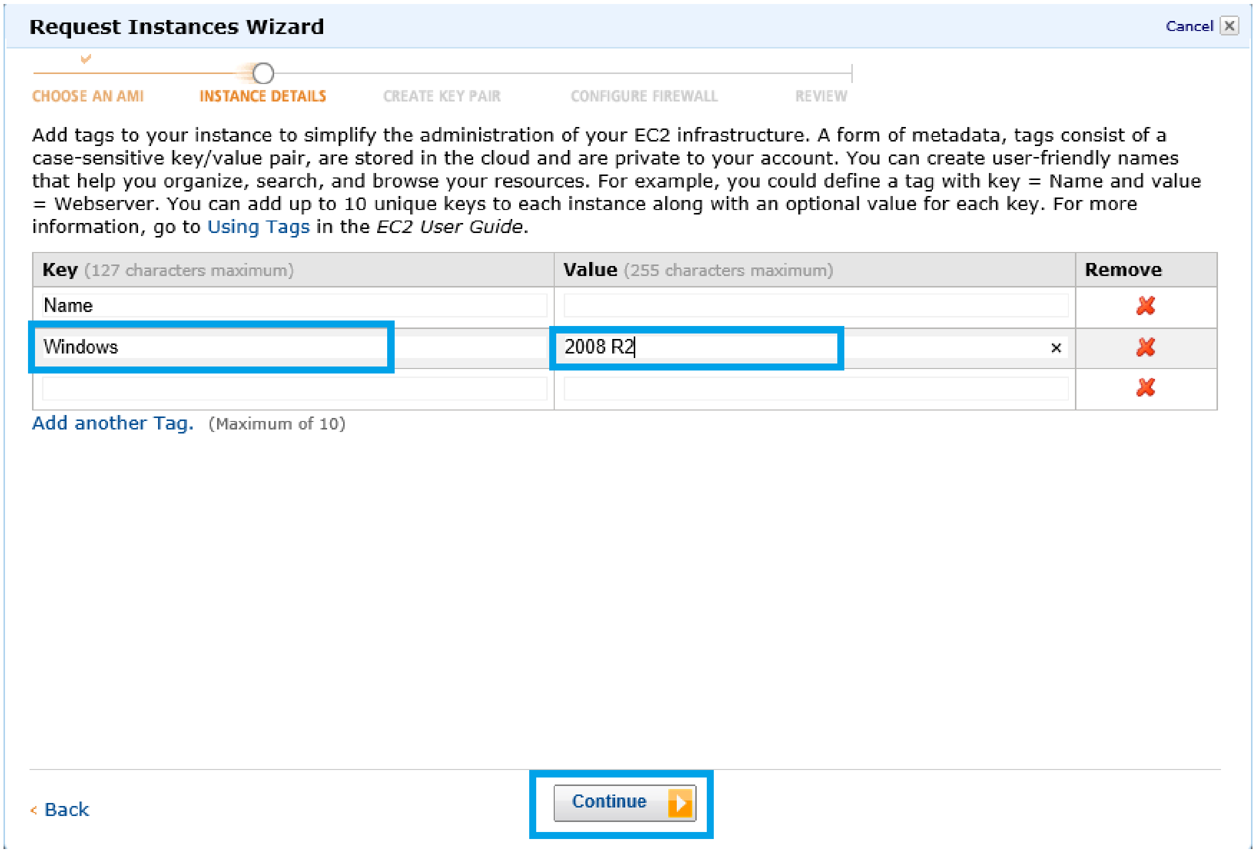
Storage Device Configuration

Your instance will be launched with the following storage device settings. Edit these settings to add EBS volumes, instance store volumes, or edit the settings of the root volume.

Type	Device	Snapshot ID	Size	Volume Type	IOPS	Delete on Termination
Root	/dev/sda1	snap-3909e116	30	standard		true

0 EBS Volumes 0 Ephemerals

10. If desired, create metadata tags to simplify the administration of your AMI instances. The tags consist of user-friendly names that help organize and browse resources. Enter in a key (that is, Windows) and a value (2008 R2). Click Continue.



Add tags to your instance to simplify the administration of your EC2 infrastructure. A form of metadata, tags consist of a case-sensitive key/value pair, are stored in the cloud and are private to your account. You can create user-friendly names that help you organize, search, and browse your resources. For example, you could define a tag with key = Name and value = Webserver. You can add up to 10 unique keys to each instance along with an optional value for each key. For more information, go to Using Tags in the *EC2 User Guide*.

Key (127 characters maximum)	**Value** (255 characters maximum)	**Remove**
Name		✗
Windows	2008 R2	✗
		✗

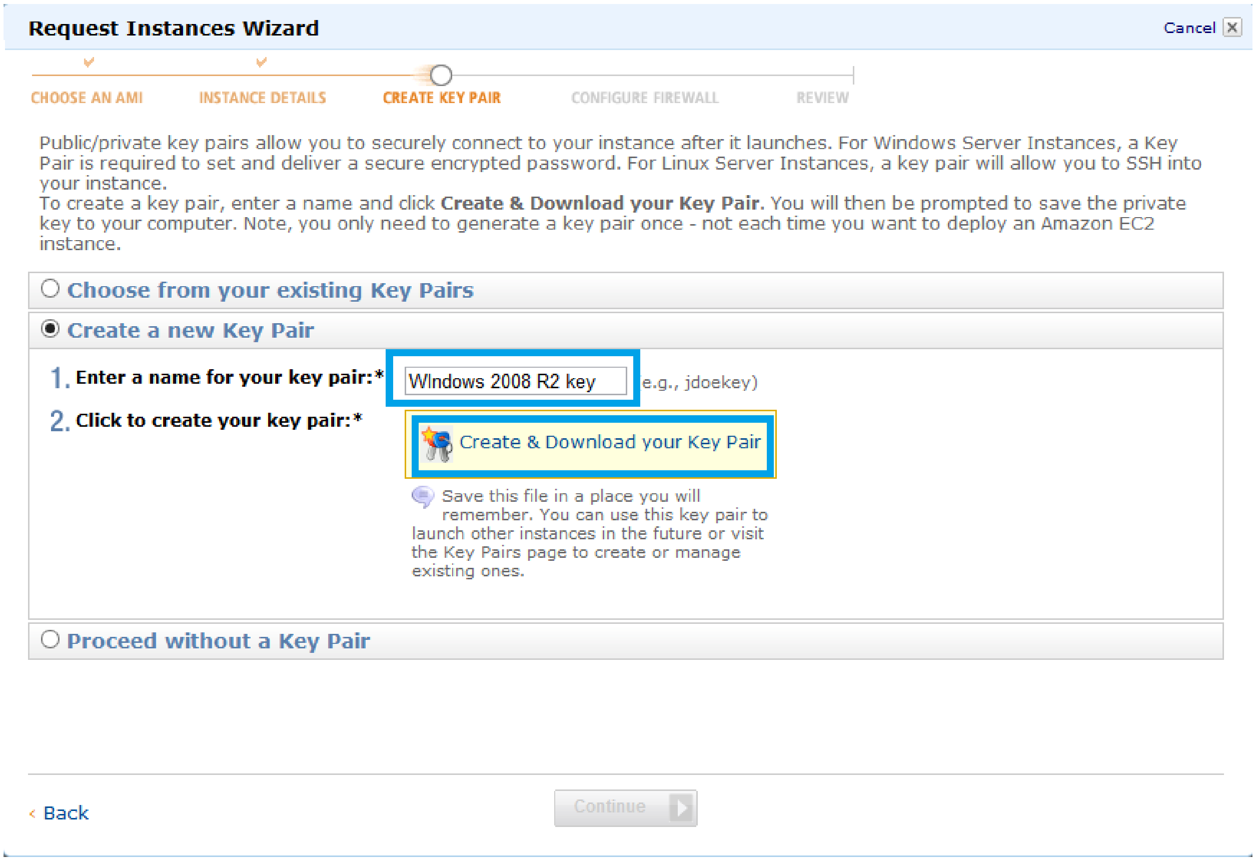
Add another Tag. (Maximum of 10)

11. For new installations, create a new key pair to support the ability to securely connect to the instance after it launches. Type in the name of the key (that is, Windows 2008 R2 key) and click “Create & Download your Key Pair.” The file will be saved with a .pem file extension.

    Note: For a Windows Server instance, a key pair is required to set and deliver a secure encrypted password.

    Note: For Linux Server instances, a key pair will allow SSH access to the instance.

    Note: It is vital to save the key file in a secure location because this file is needed to generate the Windows password for the AMI virtual machine instance.



Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server Instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux Server Instances, a key pair will allow you to SSH into your instance.
To create a key pair, enter a name and click **Create & Download your Key Pair**. You will then be prompted to save the private key to your computer. Note, you only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

○ Choose from your existing Key Pairs

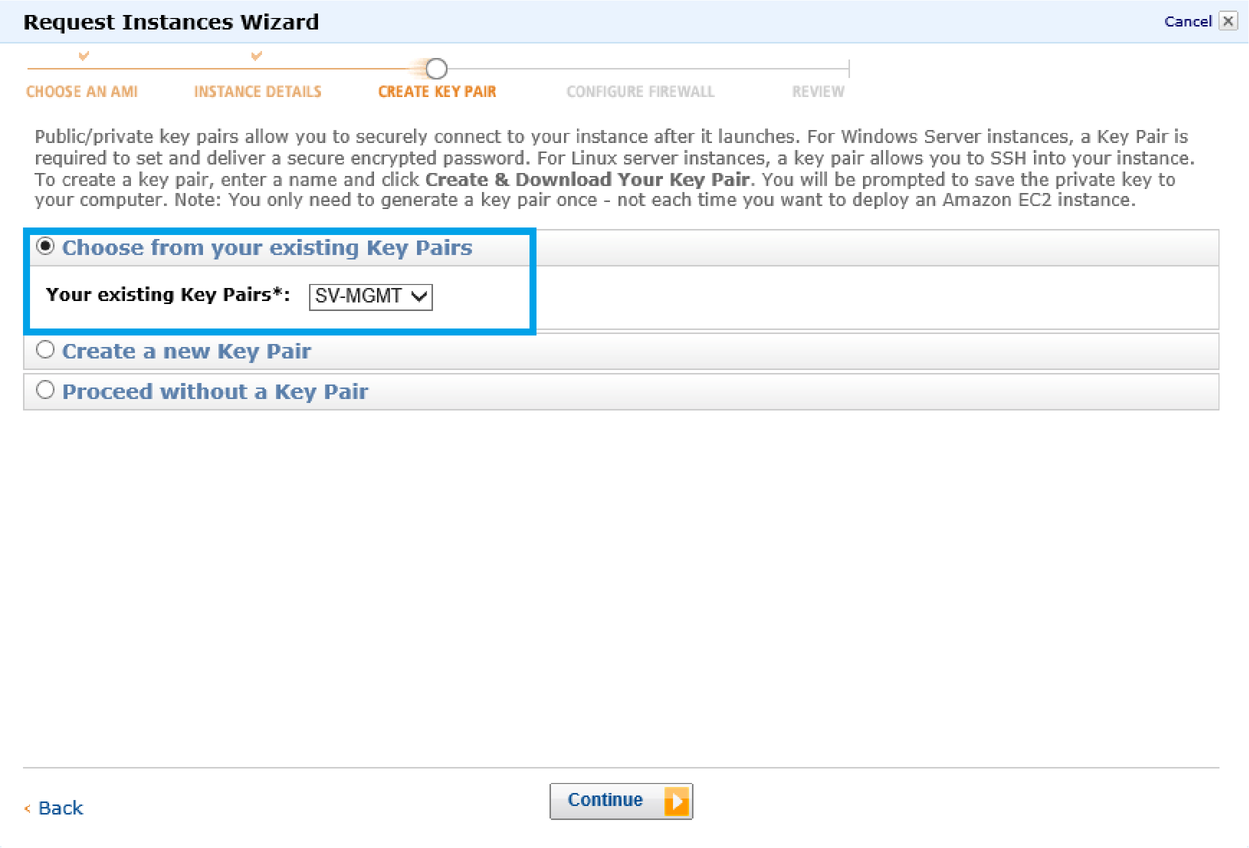
● Create a new Key Pair

1. Enter a name for your key pair:* WIndows 2008 R2 key (e.g., jdoekey)
2. Click to create your key pair:*

Save this file in a place you will remember. You can use this key pair to launch other instances in the future or visit the Key Pairs page to create or manage existing ones.

○ Proceed without a Key Pair

12. For existing configurations, select “Choose from your existing Key Pairs.” Select the preexisting key pair from the “Your existing Key Pairs” drop-down list. After selecting the existing key pair, click Continue.



Request Instances Wizard

Public/private key pairs allow you to securely connect to your instance after it launches. For Windows Server instances, a Key Pair is required to set and deliver a secure encrypted password. For Linux server instances, a key pair allows you to SSH into your instance. To create a key pair, enter a name and click **Create & Download Your Key Pair**. You will be prompted to save the private key to your computer. Note: You only need to generate a key pair once - not each time you want to deploy an Amazon EC2 instance.

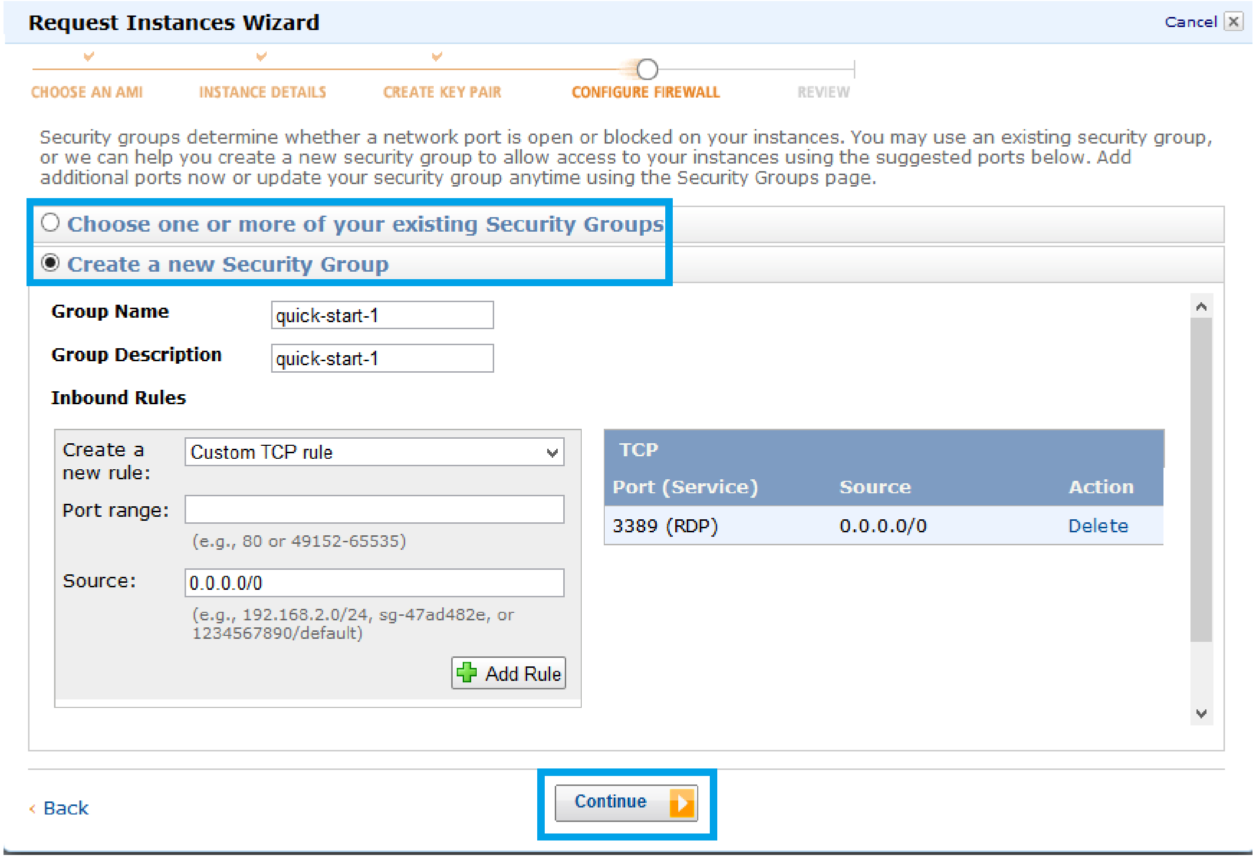
● Choose from your existing Key Pairs

Your existing Key Pairs*: SV-MGMT

○ Create a new Key Pair

○ Proceed without a Key Pair

13. For new installations, select an existing network security group created when the VPC was created, or create a new network security group. If you create a new security group, you will set the group name, group description, and inbound rules to the instance. After selecting the security group options, click Continue.



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 using the suggested ports below. Add additional ports now or update your security group anytime using the Security Groups page.

○ Choose one or more of your existing Security Groups

● Create a new Security Group

Group Name: quick-start-1

Group Description: quick-start-1

Inbound Rules

Create a new rule: Custom TCP rule

Port range:

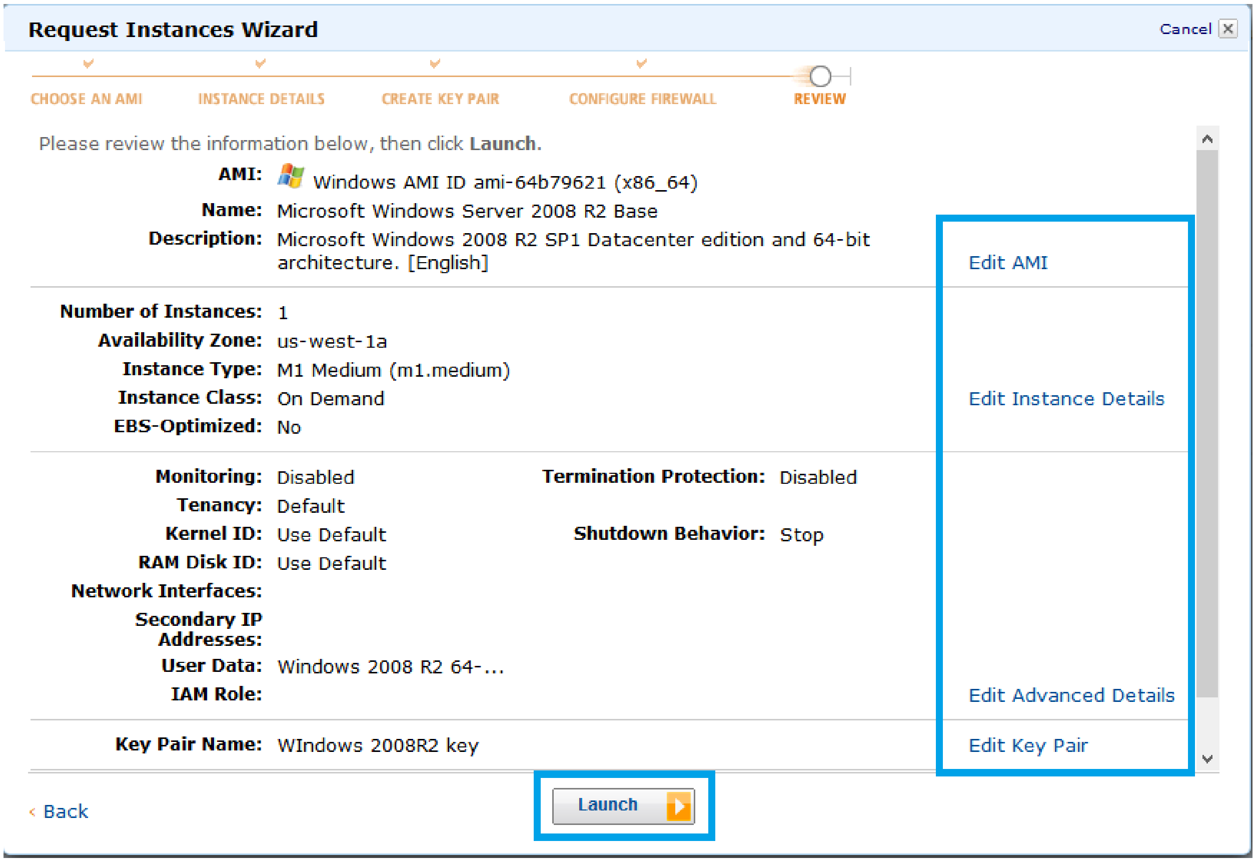
(e.g., 80 or 49152-65535)

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

14. Review the instance details prior to launch. Edit any details that are not correct. Click Launch to continue.



Please review the information below, then click **Launch**.

AMI: Windows AMI ID ami-64b79621 (x86_64)

Name: Microsoft Windows Server 2008 R2 Base

Description: Microsoft Windows 2008 R2 SP1 Datacenter edition and 64-bit architecture. [English]

Number of Instances: 1

Availability Zone: us-west-1a

Instance Type: M1 Medium (m1.medium)

Instance Class: On Demand

EBS-Optimized: No

Monitoring: Disabled

Termination Protection: Disabled

Tenancy: Default

Kernel ID: Use Default

Shutdown Behavior: Stop

RAM Disk ID: Use Default

Network Interfaces:

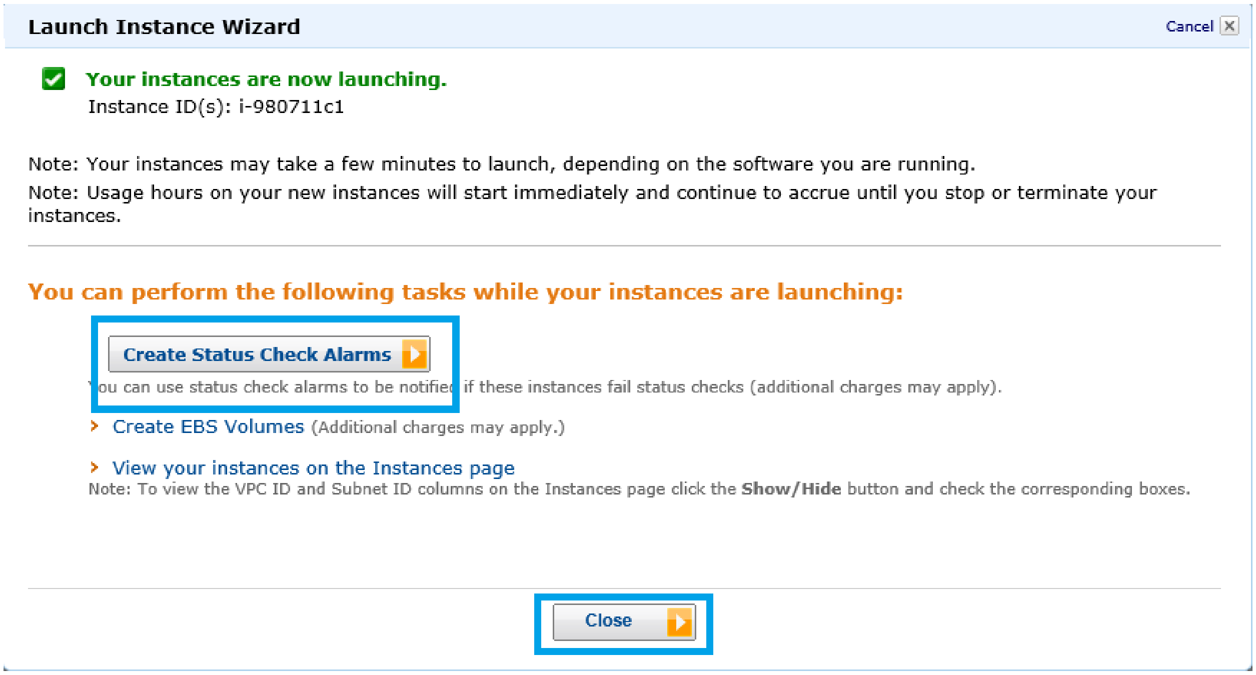
Secondary IP Addresses:

User Data: Windows 2008 R2 64-…

IAM Role:

Key Pair Name: WIndows 2008R2 key

15. After the launch of the instance is initiated, you can create a status check alarm or add AWS EBS volumes to the instance. Click Close to complete the wizard.



☑ **Your instances are now launching.**

Instance ID(s): i-980711c1

Note: Your instances may take a few minutes to launch, depending on the software you are running.

Note: Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

You can perform the following tasks while your instances are launching:

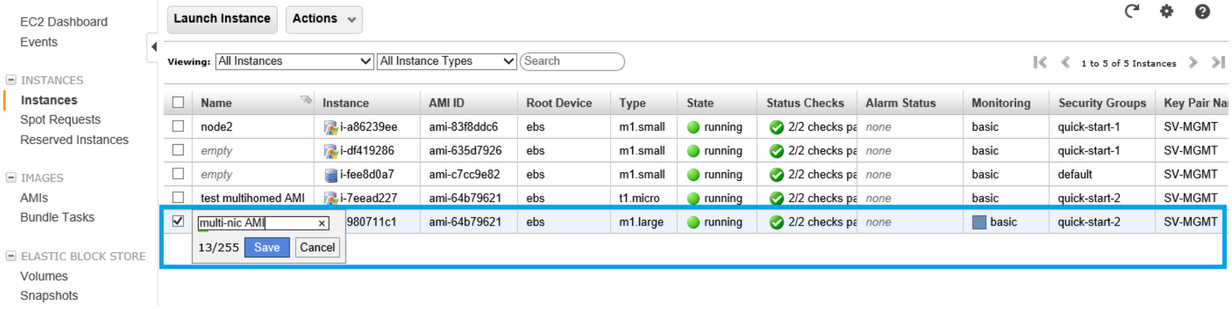
You can use status check alarms to be notified if these instances fail status checks (additional charges may apply).

› Create EBS Volumes (Additional charges may apply.)

› View your instances on the Instances page

Note: To view the VPC ID and Subnet ID columns on the Instances page click the **Show/Hide** button and check the corresponding boxes.

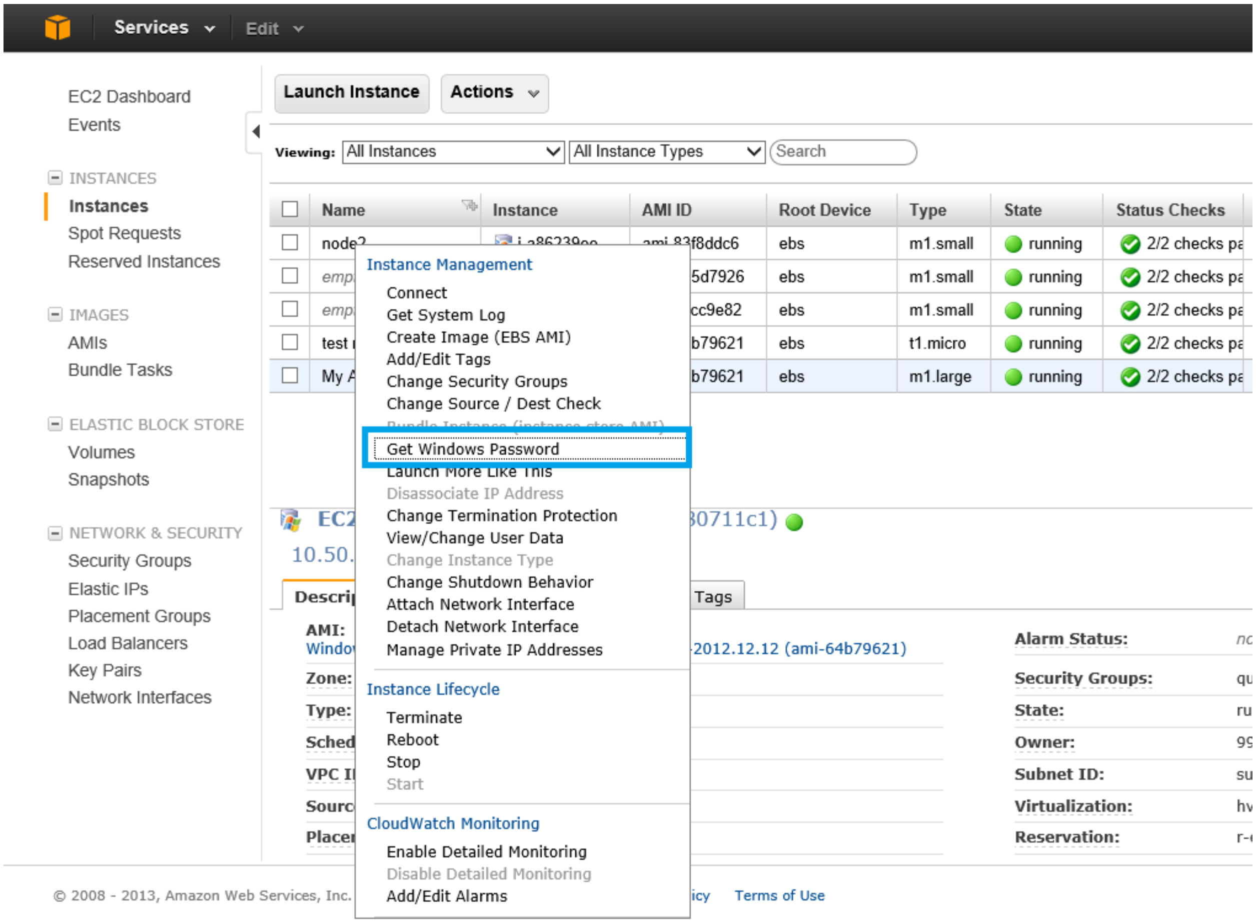
16. The EC2 dashboard will show the new AMI instance that was created. Click on the Tag field for the new AMI instance to assign a Tag to the new AMI instance. Click Save to save the changes.



☐	Name	Instance	AMI ID	Root Device	Type	State	Status Checks	Alarm Status	Monitoring	Security Groups	Key Pair Na
☐	node2	i-a86239ee	ami-83f8ddc6	ebs	m1.small	running	✓ 2/2 checks pa	*none*	basic	quick-start-1	SV-MGMT
☐	*empty*	i-df419286	ami-635d7926	ebs	m1.small	running	✓ 2/2 checks pa	*none*	basic	quick-start-1	SV-MGMT
☐	*empty*	i-fee8d0a7	ami-c7cc9e82	ebs	m1.small	running	✓ 2/2 checks pa	*none*	basic	default	SV-MGMT
☐	test multihomed AMI	i-7eead227	ami-64b79621	ebs	t1.micro	running	✓ 2/2 checks pa	*none*	basic	quick-start-2	SV-MGMT
☑	multi-nic AMI	980711c1	ami-64b79621	ebs	m1.large	running	✓ 2/2 checks pa	*none*	basic	quick-start-2	SV-MGMT

17. In the EC2 Dashboard, right-click the instance name, and select Get Windows Password.

Note: AWS requires that you wait at least 15 minutes after launching an instance for the first time before attempting to retrieve the local administrator password for the instance.



☐	Name	Instance	AMI ID	Root Device	Type	State	Status Checks
☐	node2	i-a86239ee	ami-83f8ddc6	ebs	m1.small	running	✓ 2/2 checks pa
☐	*emp*		5d7926	ebs	m1.small	running	✓ 2/2 checks pa
☐	*emp*		cc9e82	ebs	m1.small	running	✓ 2/2 checks pa
☐	test i		b79621	ebs	t1.micro	running	✓ 2/2 checks pa
☐	My A		b79621	ebs	m1.large	running	✓ 2/2 checks pa

AMI: Windo 2012.12.12 (ami-64b79621)

Zone:

Type:

Sched

VPC I

Sourc

Placer

Alarm Status: nc

Security Groups: qu

State: ru

Owner: 99

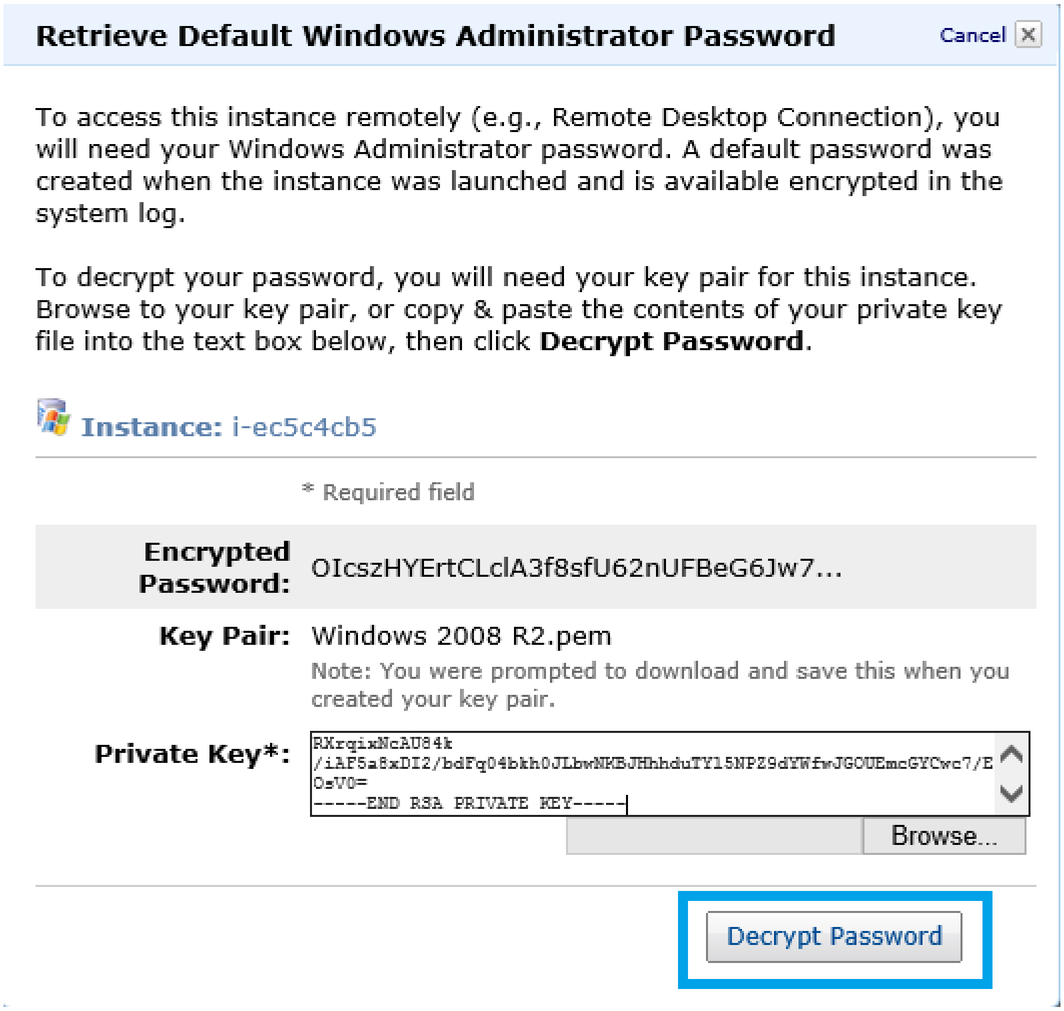
Subnet ID: su

Virtualization: hv

Reservation: r-

© 2008 - 2013, Amazon Web Services, Inc. icy Terms of Use

18. In the Retrieve Windows Administrator Password dialog box, copy the contents from the .pem key pair file that is being used by the instance into the Private Key field. Click “Decrypt Password” to retrieve the local password for the AMI virtual machine instance.



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-ec5c4cb5

* Required field

Encrypted Password: OIcszHYErtCLclA3f8sfU62nUFBeG6Jw7...

Key Pair: Windows 2008 R2.pem

Note: You were prompted to download and save this when you created your key pair.

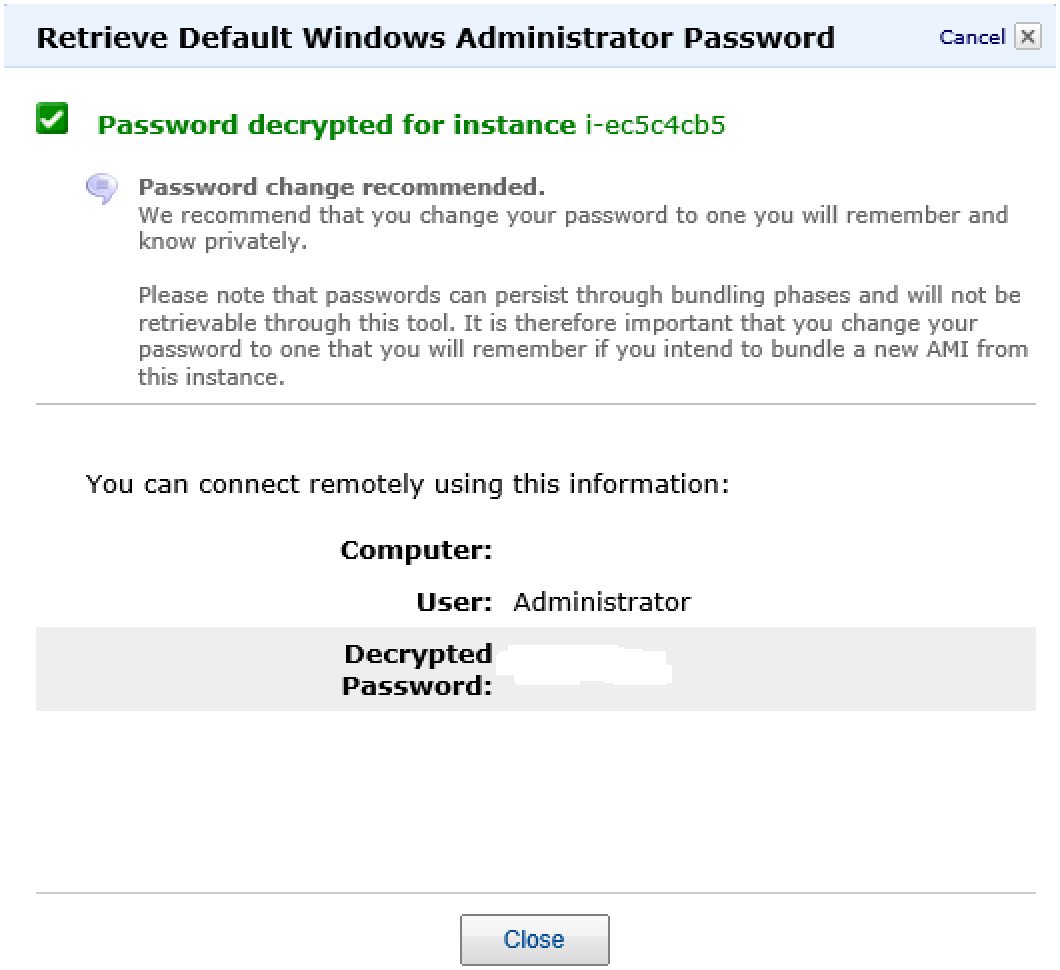
Private Key*:

```
RXrqixNcAU84k
/iAF5a8xDI2/bdFq04bkh0JLbwNKBJHhhduTY15NPZ9dYWfwJGOUEmcGYCwc7/E
OsV0=
-----END RSA PRIVATE KEY-----
```

19. If the Key Pair information is correct, the local administrator password will be shown.

    Note: It is recommended to change the password.

20. Click Close.



Retrieve Default Windows Administrator Password

☑ Password decrypted for instance i-ec5c4cb5

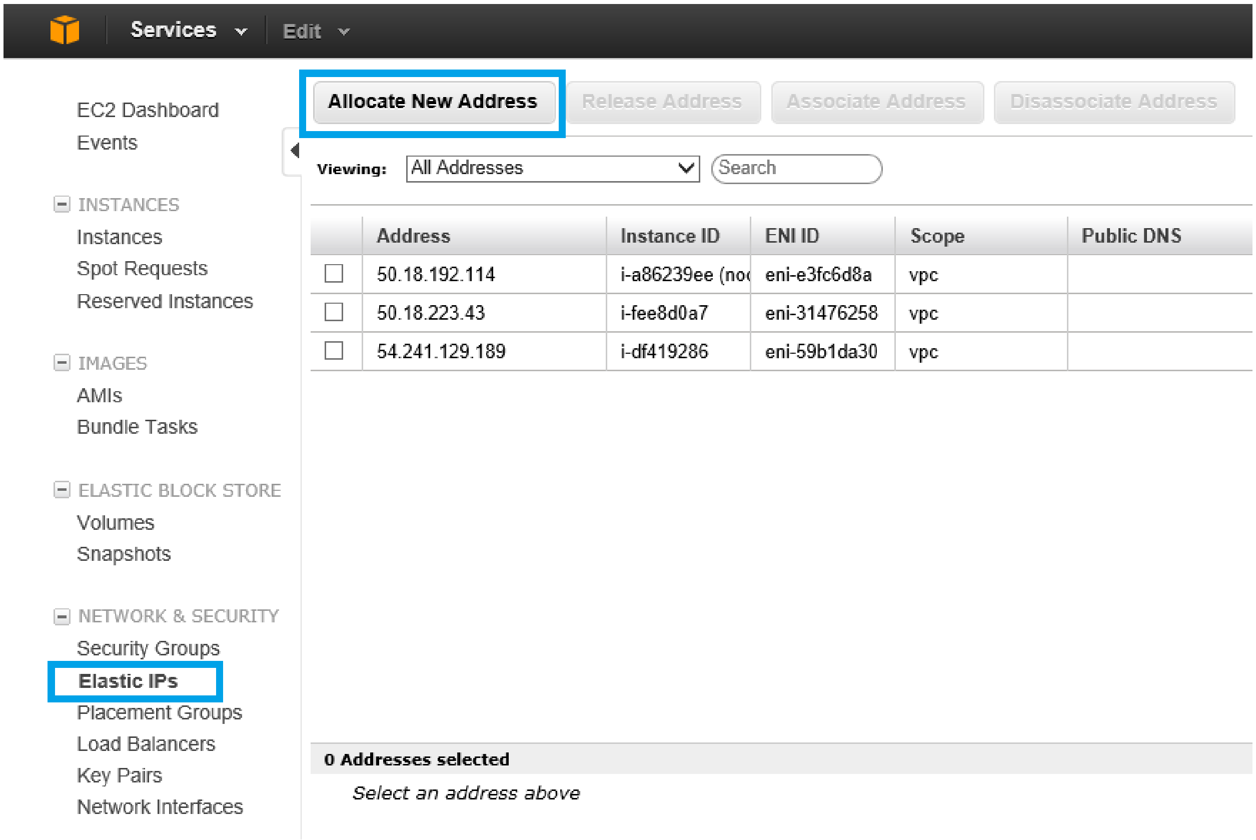
Password change recommended.
We recommend that you change your password to one you will remember and know privately.

Please note that passwords can persist through bundling phases and will not be retrievable through this tool. It is therefore important that you change your password to one that you will remember if you intend to bundle a new AMI from this instance.

You can connect remotely using this information:

Computer:	
User:	Administrator
Decrypted Password:	

21. In the EC2 dashboard, click Elastic IPs to launch the elastic IP dashboard. If less than five elastic IP addresses have been allocated for the VPC, click the Allocate IP Address link.



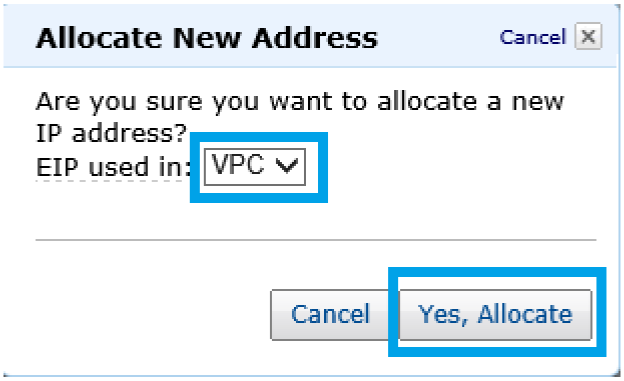
Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
□	50.18.192.114	i-a86239ee (noc	eni-e3fc6d8a	vpc	
□	50.18.223.43	i-fee8d0a7	eni-31476258	vpc	
□	54.241.129.189	i-df419286	eni-59b1da30	vpc	

0 Addresses selected

Select an address above

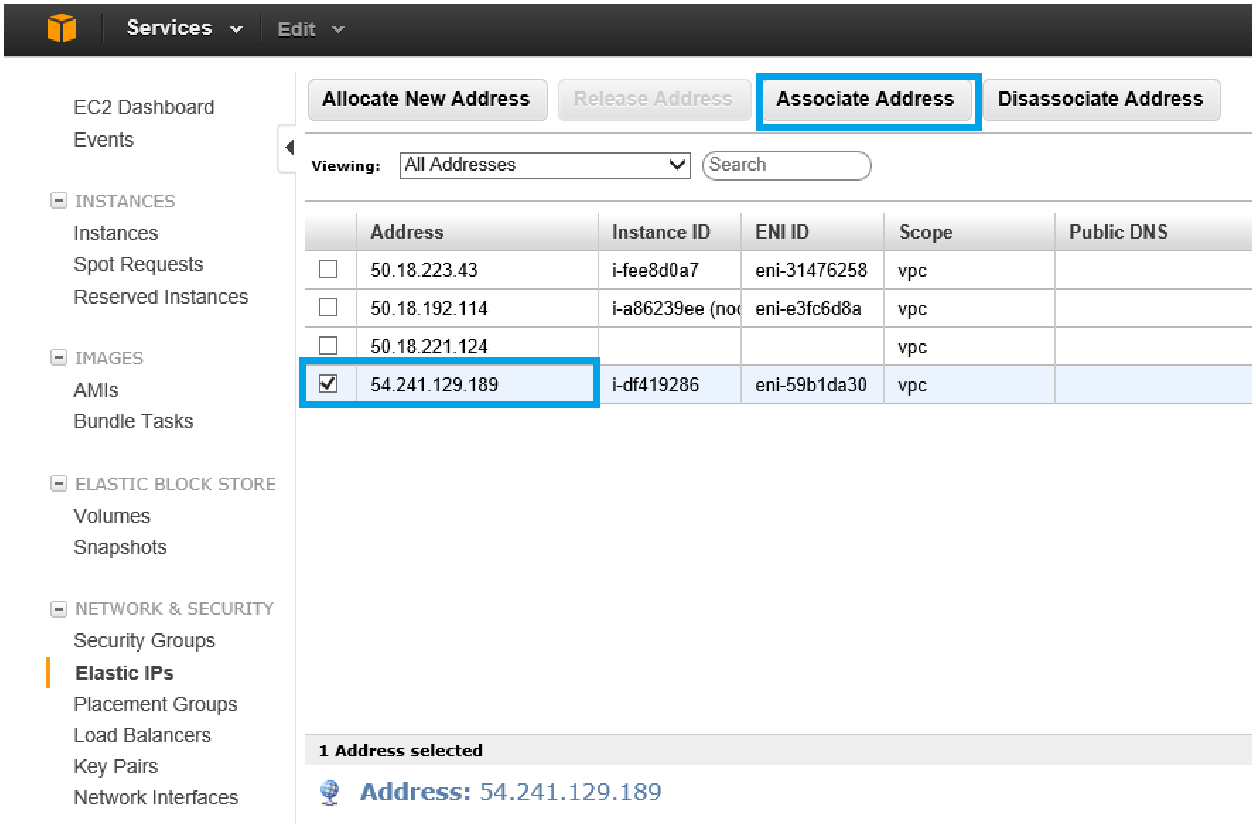
22. In the Allocate New Address dialog, select VPC from the drop-down list. Click “Yes, Allocate” to continue.



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

EIP used in: VPC

23. Click the allocated elastic IP address and then click Associate Address.



Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
□	50.18.223.43	i-fee8d0a7	eni-31476258	vpc	
□	50.18.192.114	i-a86239ee (noı	eni-e3fc6d8a	vpc	
□	50.18.221.124			vpc	
☑	54.241.129.189	i-df419286	eni-59b1da30	vpc	

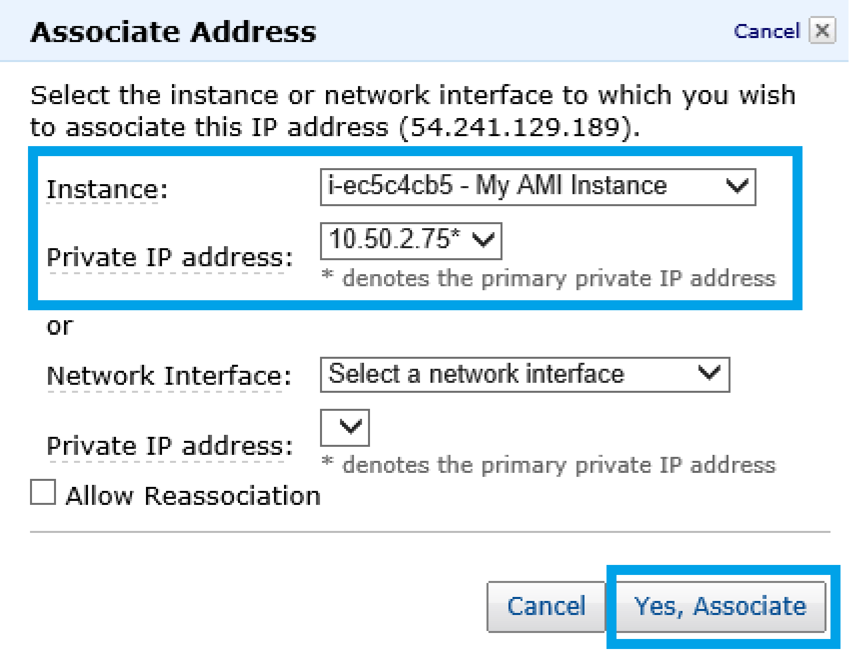
1 Address selected

Address: 54.241.129.189

24. In the Associate Address dialog box, select the instance that was created and the IP address for the interface with which the elastic IP address will be associated.

    Note: Alternatively, you can associate by interface name.

25. Click “Yes, Associate” to continue.



Associate Address

Select the instance or network interface to which you wish to associate this IP address (54.241.129.189).

Instance: i-ec5c4cb5 - My AMI Instance

Private IP address: 10.50.2.75*

* denotes the primary private IP address

or

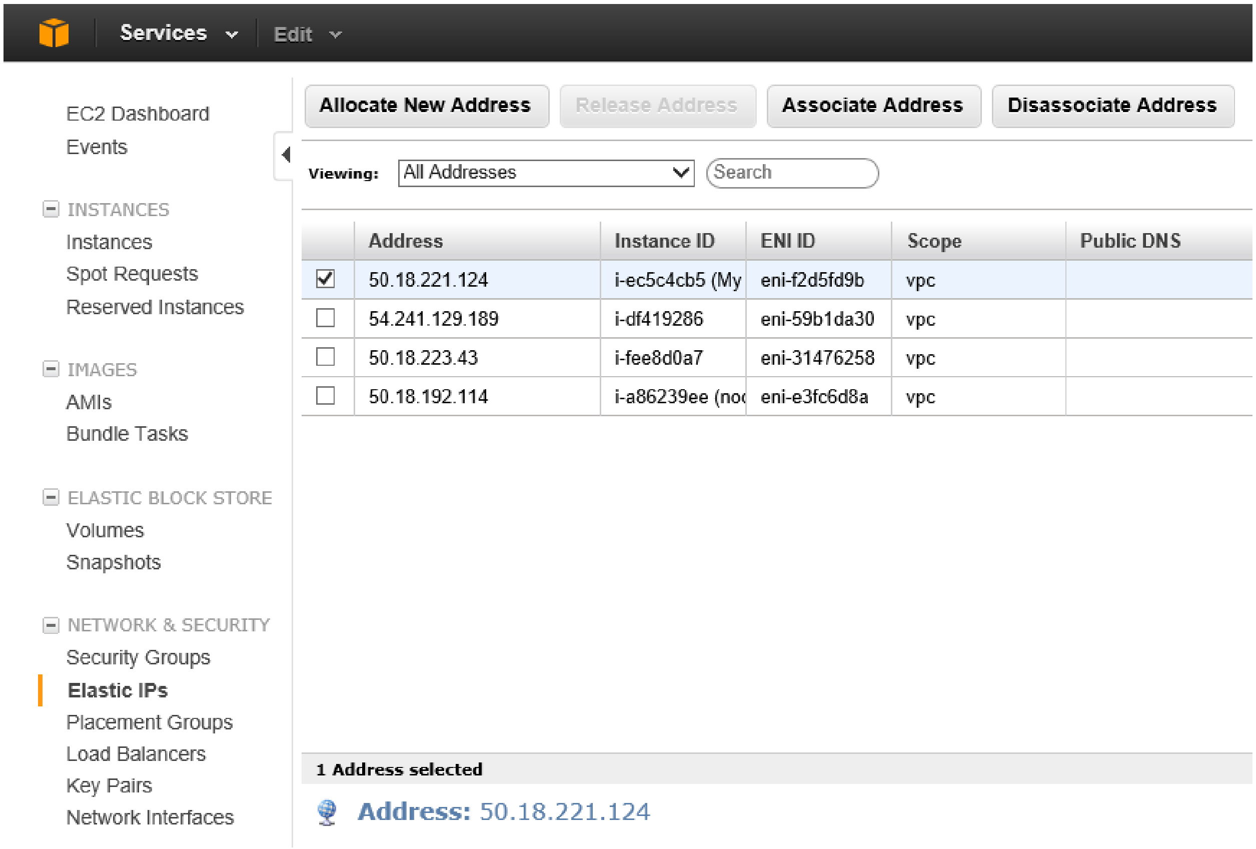
Network Interface: Select a network interface

Private IP address:

* denotes the primary private IP address

□ Allow Reassociation

26. Review the elastic IP dashboard to show that the elastic IP has been associated with the AMI virtual machine instance.



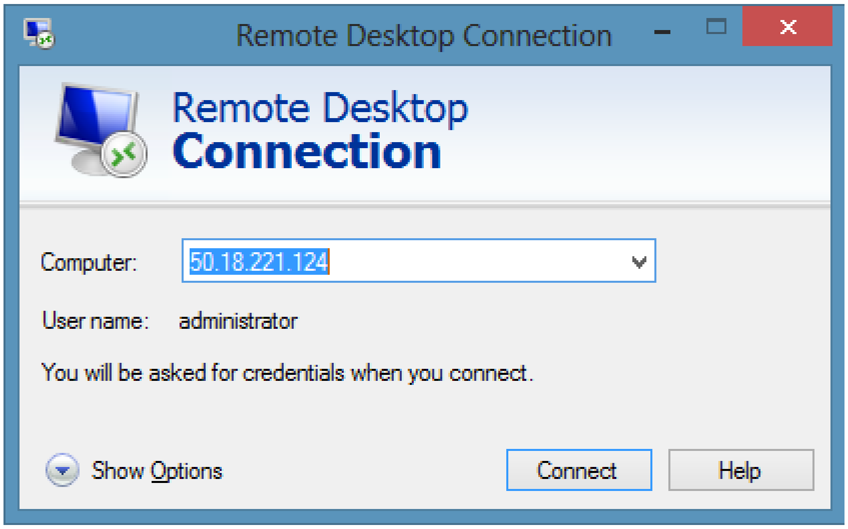
Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
☑	50.18.221.124	i-ec5c4cb5 (My	eni-f2d5fd9b	vpc	
□	54.241.129.189	i-df419286	eni-59b1da30	vpc	
□	50.18.223.43	i-fee8d0a7	eni-31476258	vpc	
□	50.18.192.114	i-a86239ee (noc	eni-e3fc6d8a	vpc	

1 Address selected

Address: 50.18.221.124

27. From a Windows host connected to the Internet, open the remote desktop (RDP) client. Provide the elastic IP address, the administrator user name, and password for the new AMI virtual machine instance and log into the virtual machine.



Computer: 50.18.221.124

User name: administrator

You will be asked for credentials when you connect.

28. Repeat steps 1 through 27 for any additional AMI instances that will be needed.

4.5 NetApp Private Storage for AWS OSPF Deployment Guide

Table 2) NetApp Private Storage for AWS OSPF prerequisites.

Description
Multiple NetApp private cloud for AWS configurations implemented in two different Amazon AWS regions in two different colocation facilities.
Customer-provided routers that have OSPF licensed and enabled located in both colocation facilities.
Administrative access to each customer-provided router.
Network connectivity is established between the different Amazon AWS regions or Amazon VPCs using the customer-provided routers.
Autonomous system (AS) numbers of the BGP networks available for each AWS Direct Connect connection.

Open Shortest Path First (OSPF) is an interior gateway routing protocol that supports routing between multiple routers in different networks. In the case of NPS for AWS, OSPF is used to route IP traffic between two different NPS for AWS solutions separated by a WAN link or between two different routers in the same VPC.

To set up a WAN link (long-haul network, for example), contact a network provider that can provide network connectivity between the colocation facilities.

4.6 NetApp Private Storage for AWS OSFP

1. Log in to the customer provided router in the colocation facility with administrative access on the router.
2. Configure OSPF to support routing between the NPS for AWS configurations.

   Note: Care must be taken to make sure that no routing loops are created when configuring OSPF.

   For more information about how to configure OSPF, review the router documentation for the switch being used in your environment.

   The following contains sample Cisco IOS 12.4 configuration commands for OSPF to support the routing between two NPS for AWS configurations. In this sample, the NPS for AWS configuration has a single Direct Connect network connection for a router in a colocation facility in California.

   The command: `route-map BGP2OSPF deny 20` is used to prevent a routing loop.

```
router ospf 32768
 redistribute bgp 64514 subnets route-map BGP2OSPF
 network 10.10.10.0 0.0.0.255 area 0
!
router bgp 64514
 bgp redistribute-internal
 network 10.10.10.0 mask 255.255.255.0
 network 192.168.1.0
 redistribute ospf 32768 match internal external 2
 neighbor 169.254.253.17 remote-as 7224
 neighbor 169.254.253.17 password <<bgp secret>>
!
ip classless
!
ip prefix-list Cali seq 5 permit 172.16.2.0/24
route-map BGP2OSPF permit 10
 match ip address prefix-list Cali
!
route-map BGP2OSPF deny 20
 match route-type external
!
```

3. Repeat steps 1 through 2 for each additional NPS for AWS configuration.

   The following contains sample Cisco IOS 12.4 configuration commands for OSPF to support the routing between two NPS for AWS configurations. In this sample, the NPS for AWS configuration has a single Direct Connect network connection for a router in a colocation facility in Virginia.

   The command: `route-map BGP2OSPF deny 20` is used to prevent a routing loop.

```
router ospf 32769
 redistribute bgp 64513 subnets route-map BGP2OSPF
 network 10.10.10.0 0.0.0.255 area 0
!
router bgp 64513
 bgp redistribute-internal
 network 10.10.10.0 mask 255.255.255.0
 network 10.10.10.0
 network 192.168.1.0
 redistribute ospf 32769 match internal external 2
 neighbor 169.254.255.57 remote-as 7224
 neighbor 169.254.255.57 password <<bgp secret>>
!
ip classless
!
ip prefix-list Virginia seq 5 permit 172.16.1.0/24
route-map BGP2OSPF permit 10
 match ip address prefix-list Virginia
!
route-map BGP2OSPF deny 20
 match route-type external
!
```

5 NetApp Private Storage for AWS BPG Test Procedures

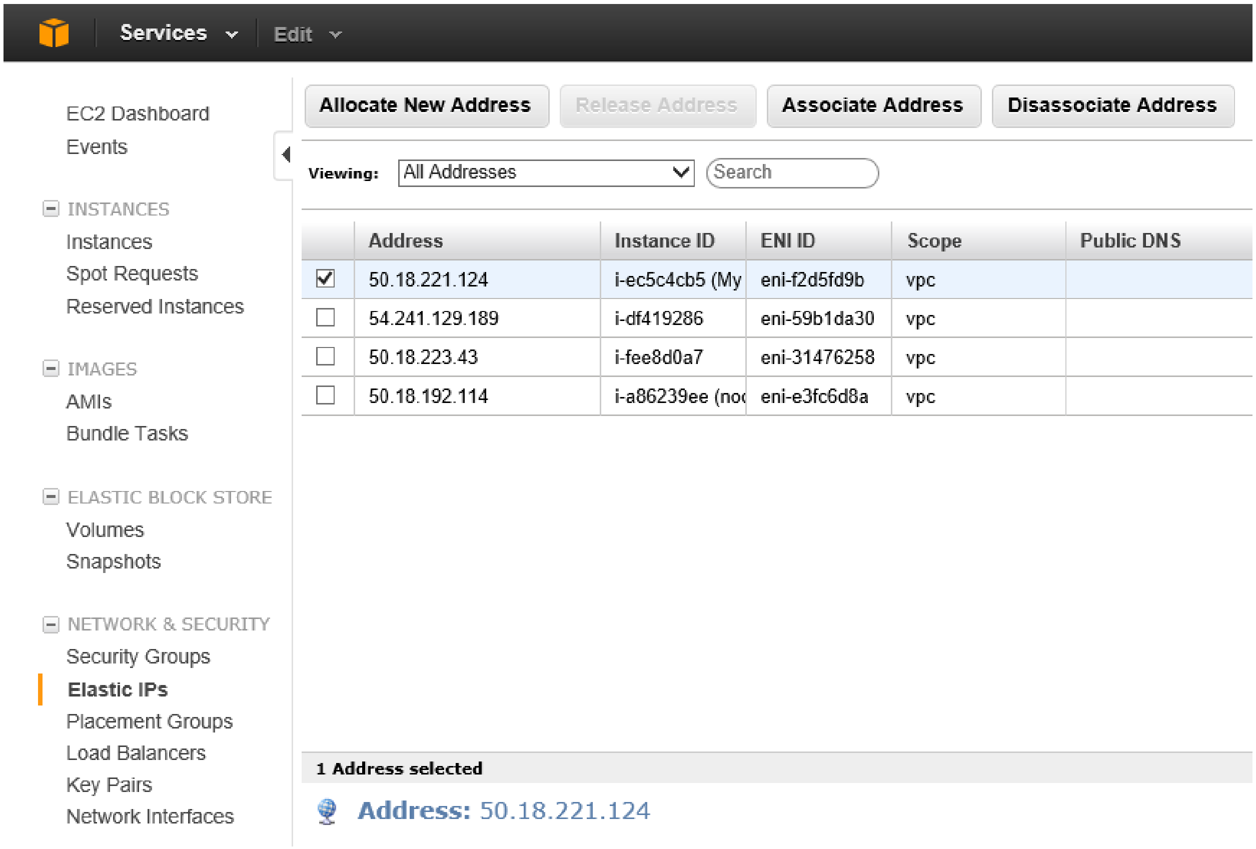
5.1 Verify Direct Connect Network Connections

Test Case	Details
Test No:	NPSAWSBPG-1
Tester:	
Date:	
Test Prerequisites:	• The physical network connectivity from AWS EC2 to the NetApp storage using an AWS Direct Connect network connection has been established. • Network interface configuration for the NetApp storage has been configured to use the AWS Direct Connect network connection. • The AMI virtual machine instance is up and running. • The AMI virtual machine instance is configured with a virtual network interface to communicate to the NetApp storage. • Local administrator access to the AMI virtual machine instance. • BGP configuration on the customer-provided router in the colocation facility. • The Direct Connect network rules allow ICMP ping to the AMI virtual machine instances. • An AWS elastic IP address is assigned to the AMI virtual machine for out-of-band access to the virtual machine.
Expected Outcome:	The ping test succeeds (0% packet loss) and network information is displayed.
Test Results:	Passed/Failed

Test Case	Details
Comments:	

Test Procedure

1. Log into the AWS management console. In the VPC dashboard, click “Elastic IPs” to manage elastic IP addresses used for out-of-band management of the EC2 AMI virtual machines. There can be up to five elastic IP addresses per VPC. Elastic IPs can be dynamically assigned to different EC2 AMI virtual machines in the VPC as required.
2. Document the elastic IP assigned to the AMI instance. If the AMI instance does not have an elastic IP address, assign an elastic IP using the Associate New Address button in the elastic IP dashboard.



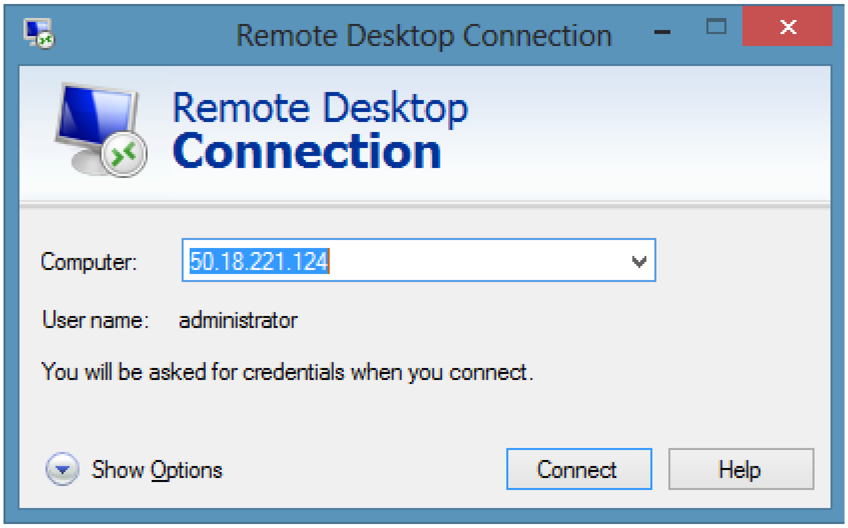
Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
☑	50.18.221.124	i-ec5c4cb5 (My	eni-f2d5fd9b	vpc	
□	54.241.129.189	i-df419286	eni-59b1da30	vpc	
□	50.18.223.43	i-fee8d0a7	eni-31476258	vpc	
□	50.18.192.114	i-a86239ee (noı	eni-e3fc6d8a	vpc	

1 Address selected

Address: 50.18.221.124

3. From a Windows host connected to the Internet, open the remote desktop (RDP) client. Provide the elastic IP address, the administrator user name, and password for the new AMI virtual machine instance and log into the virtual machine.



Computer: 50.18.221.124

User name: administrator

You will be asked for credentials when you connect.

4. Open a command prompt and type the following command. This command will perform a ping test against one of the network interfaces on the NetApp storage (that is, 192.168.1.102):

```
ping 192.168.1.102
```

5. If the Direct Connect network is properly configured between the AMI virtual machine instance and the NetApp storage, the result of the ping test is:

```
Pinging 192.168.1.102 with 32 bytes of data:
Reply from 192.168.1.102: bytes=32 time=2ms TTL=251
Reply from 192.168.1.102: bytes=32 time=1ms TTL=251
Reply from 192.168.1.102: bytes=32 time=1ms TTL=251
Reply from 192.168.1.102: bytes=32 time=1ms TTL=251

Ping statistics for 192.168.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

6 NetApp Private Storage for AWS OSPF Test Procedures

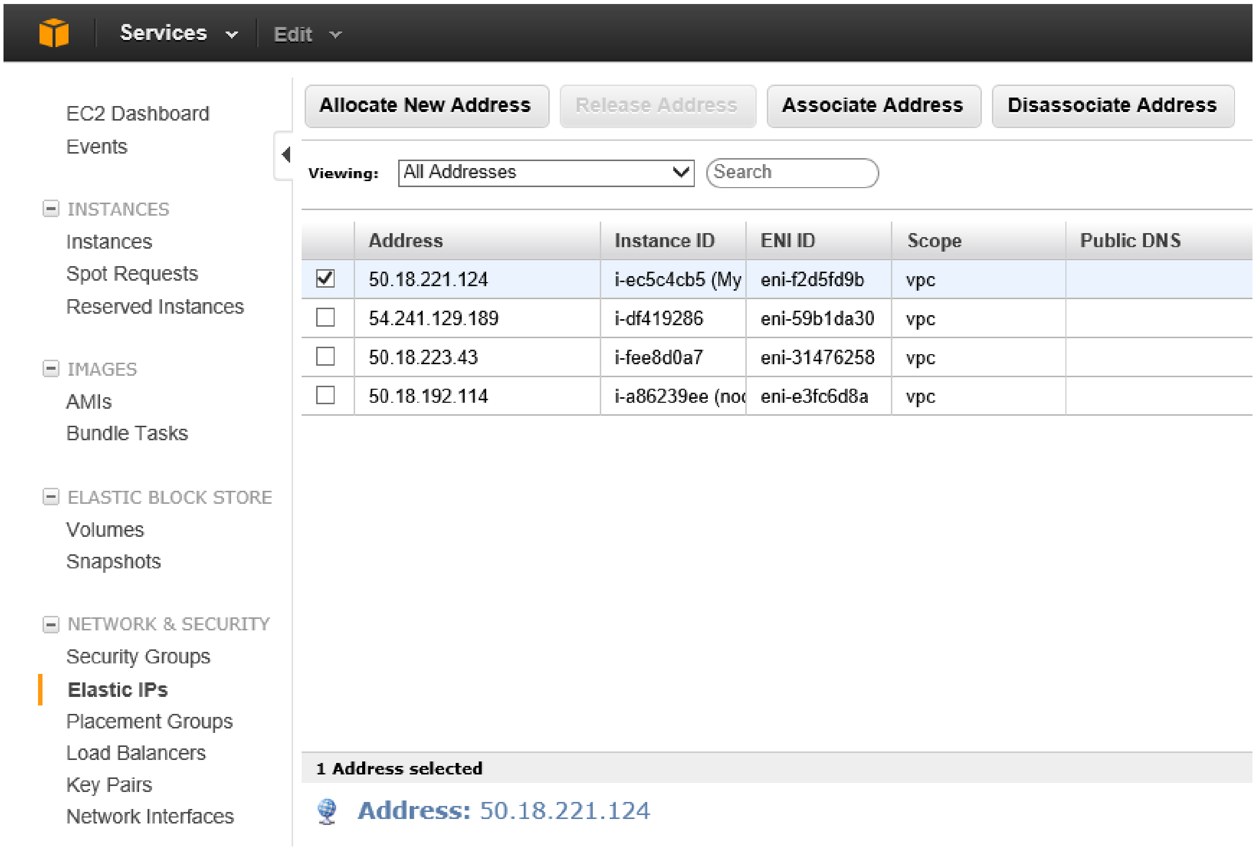
6.1 Verify Routing Across WAN

Test Case	Details
Test No:	NPSAWSOSPF-1
Tester:	
Date:	

Test Case	Details
Test Prerequisites:	• NetApp Private Storage for AWS solution has been installed and configured in two different colocation facilities and two different Amazon AWS regions. • The long-haul network (MPLS)/VPN connectivity between the two NetApp Private Storage for AWS solutions has been established. • Two AMI virtual machine instances are up and running. Each AMI is in different VPCs in different AWS regions. • The AMI virtual machine instance is configured with at least one virtual network interface. • Local administrator access to the AMI virtual machines. • OSPF configuration on the customer-provided router in both colocation facilities. • An AWS elastic IP address is assigned to each AMI virtual machine for out-of-band access to the virtual machines.
Expected Outcome:	The ping test succeeds (0% packet loss) and network information is displayed.
Test Results:	Passed/Failed
Comments:	

Test Procedure

1. Log in to the AWS management console and select the primary region. In the VPC dashboard, click “Elastic IPs” to manage elastic IP addresses used for out-of-band management of the EC2 AMI virtual machines. There can be up to five elastic IP addresses per VPC. Elastic IPs can be dynamically assigned to different EC2 AMI virtual machines in the VPC as required.
2. Document the elastic IP assigned to the AMI instance. If the AMI instance does not have an elastic IP address, assign an elastic IP using the “Associate New Address” button in the elastic IP dashboard.



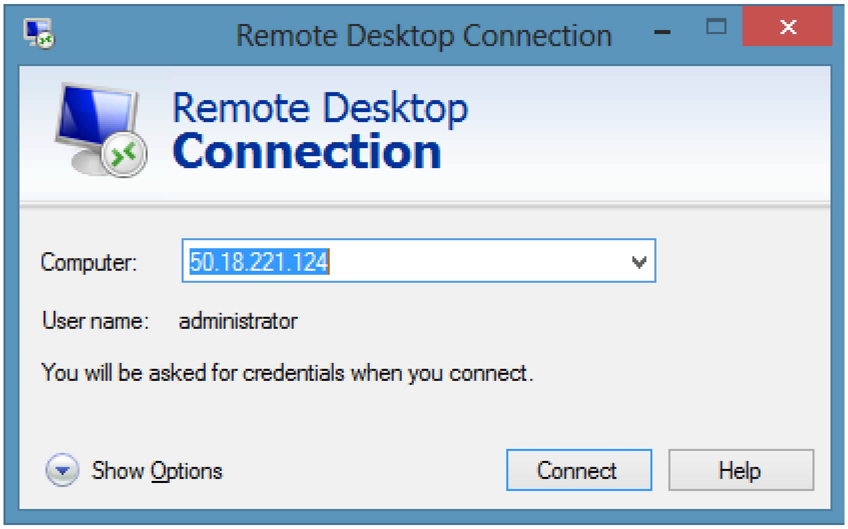
Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
☑	50.18.221.124	i-ec5c4cb5 (My	eni-f2d5fd9b	vpc	
□	54.241.129.189	i-df419286	eni-59b1da30	vpc	
□	50.18.223.43	i-fee8d0a7	eni-31476258	vpc	
□	50.18.192.114	i-a86239ee (noc	eni-e3fc6d8a	vpc	

1 Address selected

Address: 50.18.221.124

3. From a Windows host connected to the internet, open the Remote Desktop (RDP) Client. Provide the elastic IP Address, the administrator user name and password for the AMI virtual machine instance and log into the virtual machine.



Computer: 50.18.221.124

User name: administrator

You will be asked for credentials when you connect.

4. Open a command prompt and type the following command. This command will perform a ping test against one of the network interfaces on the NetApp storage in the secondary colocation facility (that is, 192.168.1.101):

```
ping 192.168.1.101
```

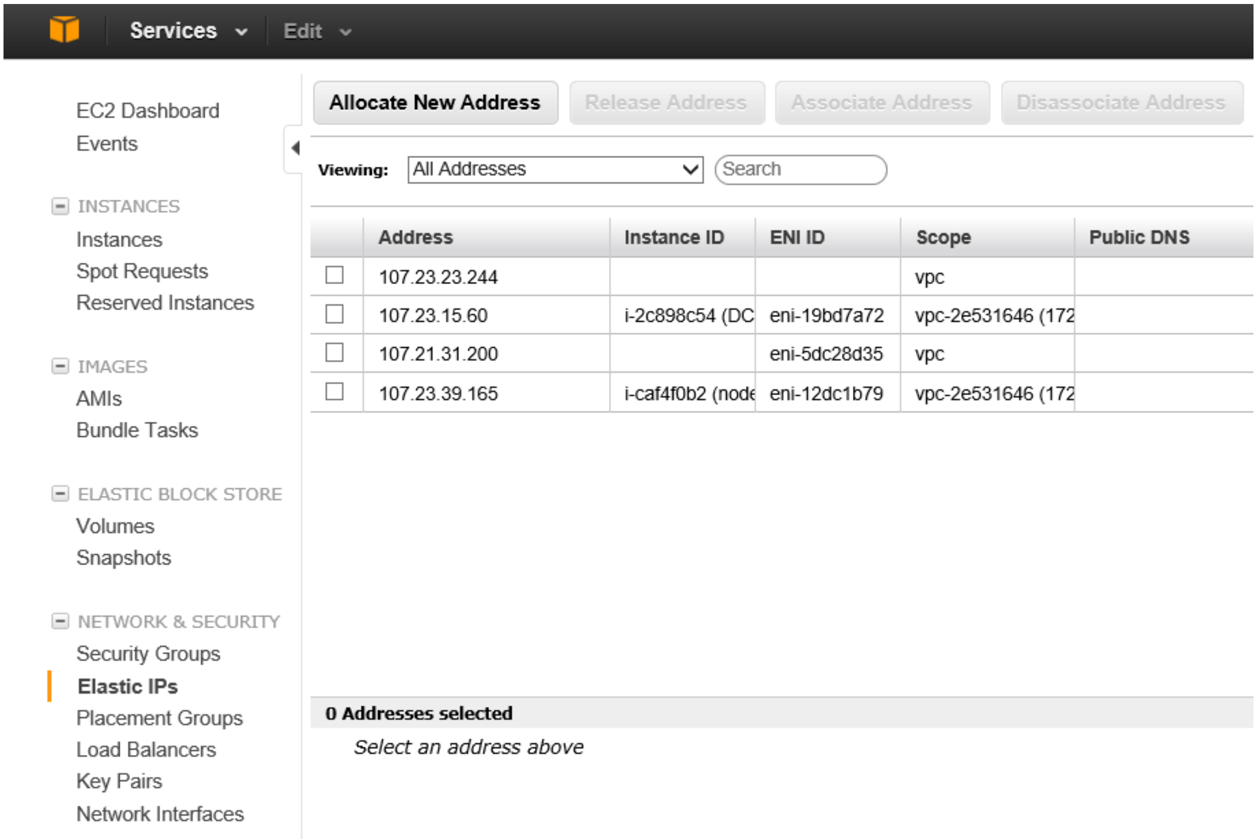
5. If the network routing is properly configured between the AMI virtual machine instance in the primary AWS region and the NetApp storage in the secondary colocation facility, the result of the ping test is:

```
Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=71ms TTL=251
Reply from 192.168.1.101: bytes=32 time=71ms TTL=251
Reply from 192.168.1.101: bytes=32 time=71ms TTL=251
Reply from 192.168.1.101: bytes=32 time=71ms TTL=251

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 71ms, Maximum = 71ms, Average = 71ms
```

6. In the AWS management console and select the secondary region. In the VPC dashboard, click “Elastic IPs” to manage elastic IP addresses used for out-of-band management of the EC2 AMI virtual machines. There can be up to five elastic IP addresses per VPC. Elastic IPs can be dynamically assigned to different EC2 AMI virtual machines in the VPC as required.

7. Document the elastic IP assigned to the AMI instance in the secondary region. If the AMI instance does not have an elastic IP address, assign an elastic IP using the “Associate New Address” button in the elastic IP dashboard.



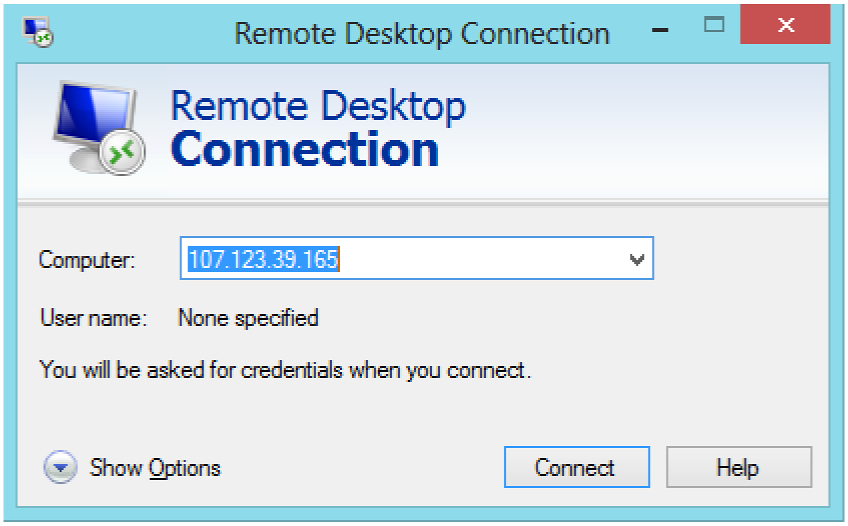
Viewing: All Addresses

	Address	Instance ID	ENI ID	Scope	Public DNS
□	107.23.23.244			vpc	
□	107.23.15.60	i-2c898c54 (DC	eni-19bd7a72	vpc-2e531646 (172	
□	107.21.31.200		eni-5dc28d35	vpc	
□	107.23.39.165	i-caf4f0b2 (node	eni-12dc1b79	vpc-2e531646 (172	

0 Addresses selected

Select an address above

8. From a Windows host connected to the Internet, open the remote desktop (RDP) client. Provide the elastic IP address, the administrator user name, and password for the AMI virtual machine instance in the secondary region and log into the virtual machine.



Computer: 107.123.39.165

User name: None specified

You will be asked for credentials when you connect.

9. Open a command prompt and type the following command. This command will perform a ping test against one of the network interfaces on the NetApp storage in the secondary colocation facility (that is, 192.168.1.101):

```
ping 192.168.1.101
```

10. If the network routing is properly configured between the AMI virtual machine instance in the primary AWS region and the NetApp storage in the secondary colocation facility the result of the ping test is:

```
Pinging 192.168.1.101 with 32 bytes of data:
Reply from 192.168.1.101: bytes=32 time=70ms TTL=251
Reply from 192.168.1.101: bytes=32 time=70ms TTL=251
Reply from 192.168.1.101: bytes=32 time=70ms TTL=251
Reply from 192.168.1.101: bytes=32 time=70ms TTL=251

Ping statistics for 192.168.1.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 70ms, Maximum = 70ms, Average = 70ms
```

References

The following references were used in this report:

- Amazon Web Services Direct Connect Getting Started Guide
  http://docs.amazonwebservices.com/DirectConnect/latest/GettingStartedGuide/Welcome.html
- Amazon Web Services Direct Connect User Guide
  http://docs.amazonwebservices.com/directconnect/latest/UserGuide/Colocation.html

Version History

Version	Date	Document Version History
Version 1.0	March 2013	Initial release.
Version 1.1	August 2013	Content updated based on feedback.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

NetApp®
www.netapp.com