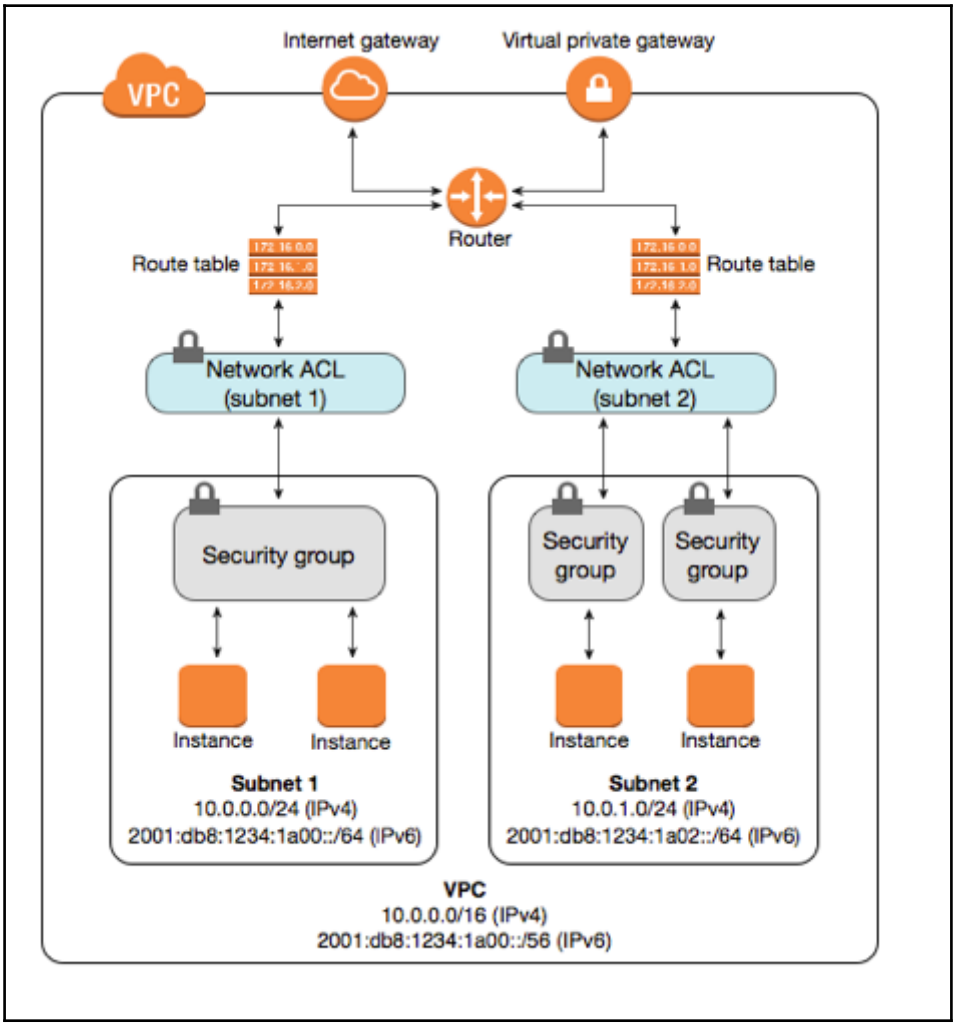
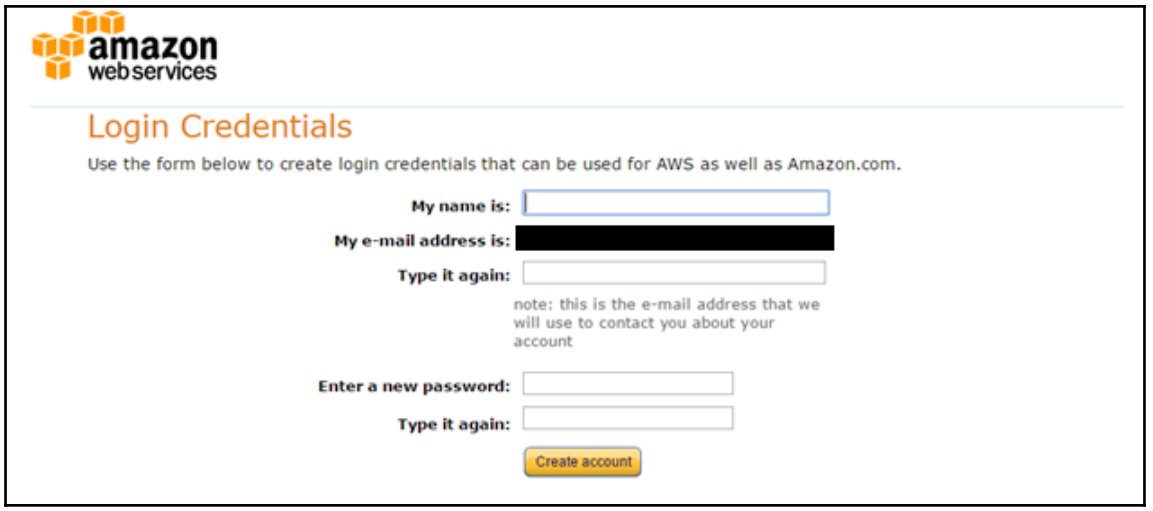
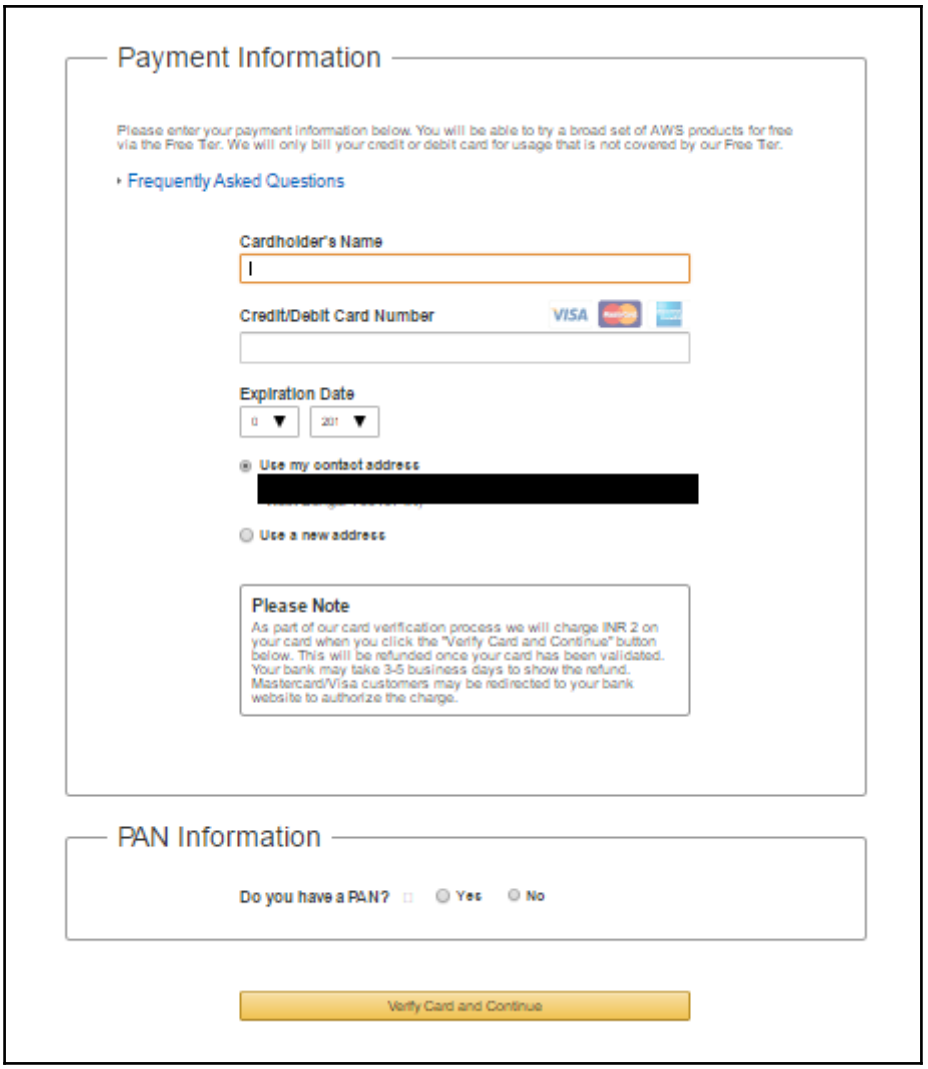
Chapter 1: Getting Started with AWS Networking Components

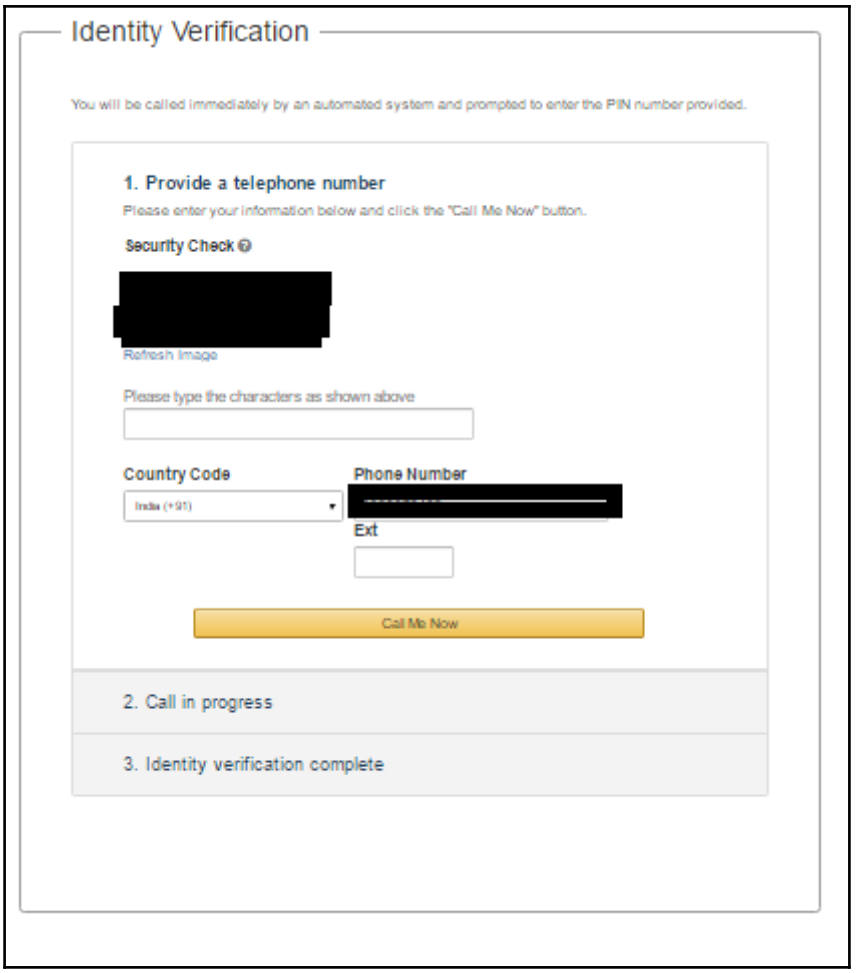


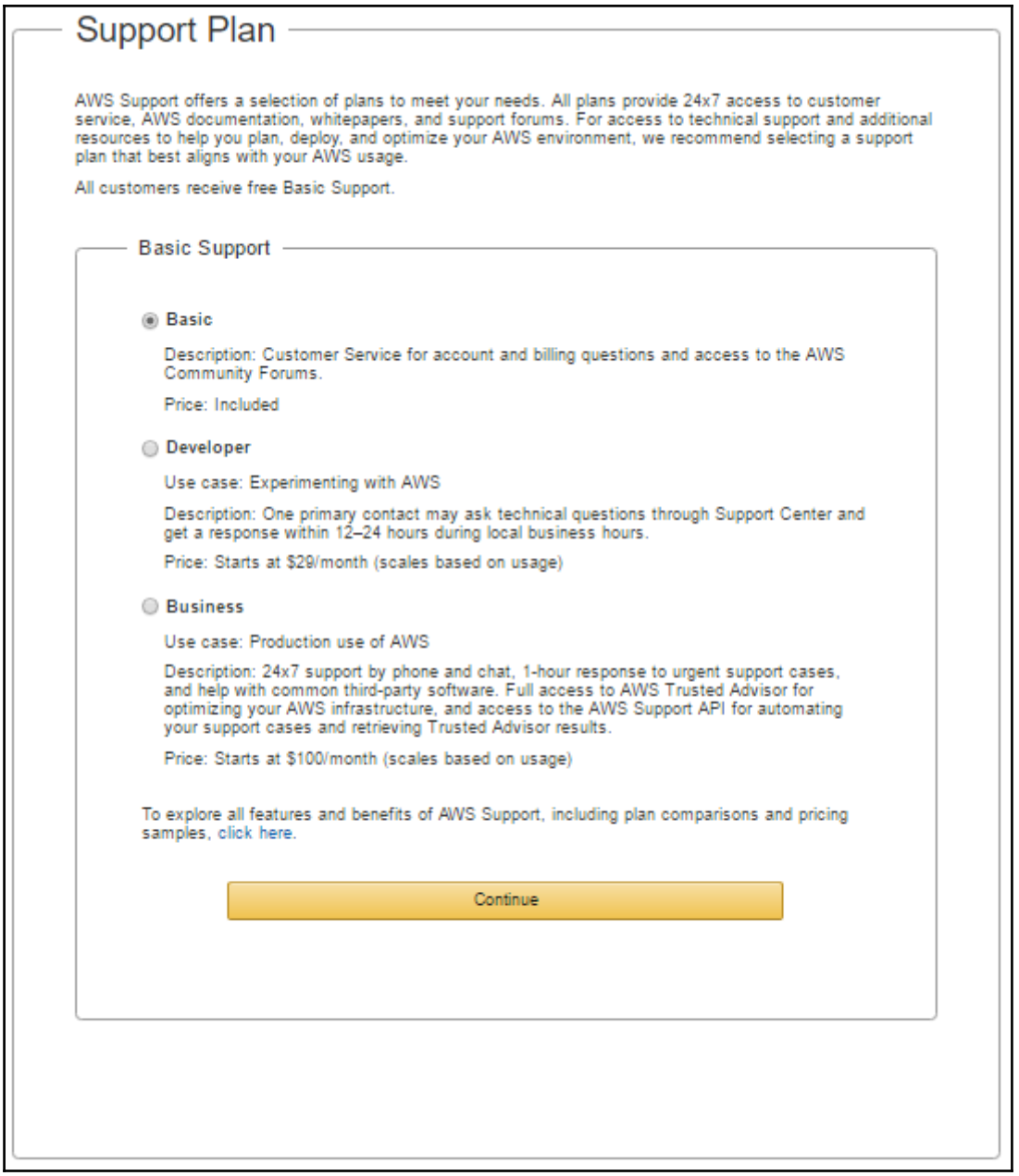
amazon
web services
Sign In or Create an AWS Account
What is your email (phone for mobile accounts)?
E-mail or mobile number:
I am a new user.
I am a returning user
and my password is:
Sign in using our secure server
Forgot your password?

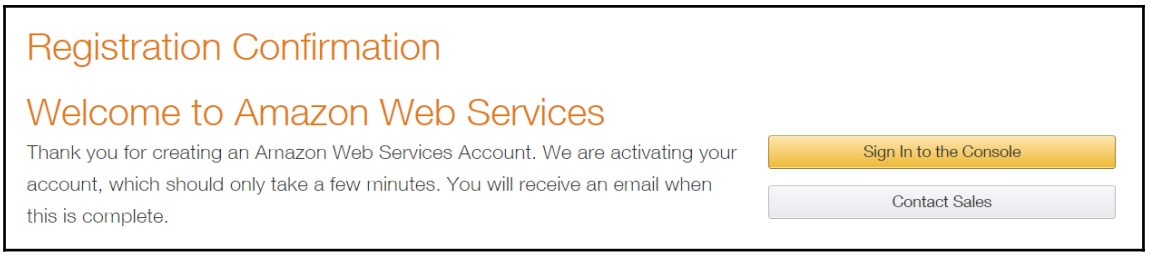

amazon
web services
Login Credentials
Use the form below to create login credentials that can be used for AWS as well as Amazon.com.
My name is:
My e-mail address is:
Type it again:
note: this is the e-mail address that we will use to contact you about your account
Enter a new password:
Type it again:
Create account

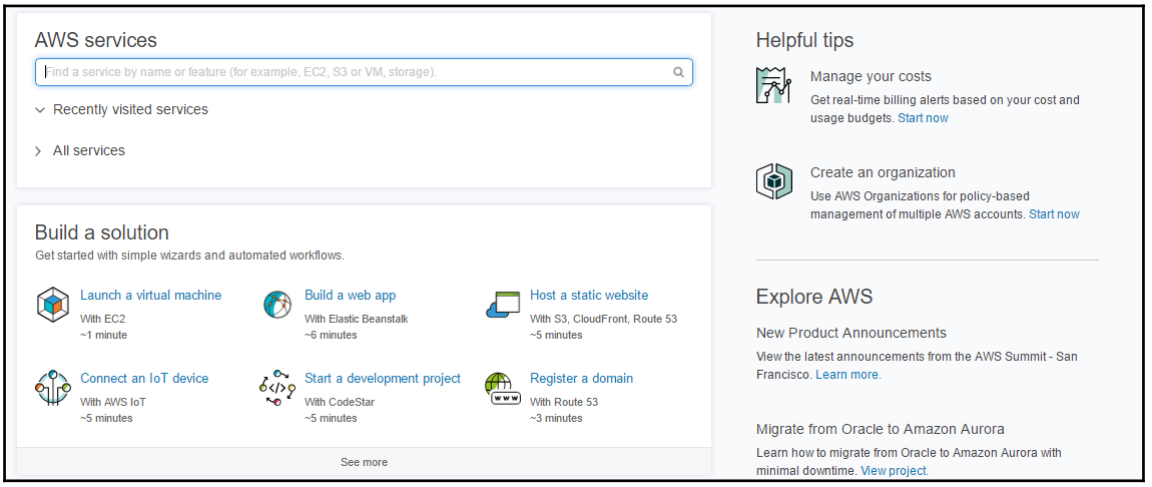
Contact Information
Company Account
Personal Account
* Required Fields
Full Name*
Company Name*
Country*
United States
Address*
Street, P.O. Box, Company Name, c/o
Apartment, suite, unit, building, floor, etc.
City*
State / Province or Region*
Postal Code*
Phone Number*
Security Check
Refresh Image
Please type the characters as shown above
AWS Customer Agreement
Check here to indicate that you have read and agree to the terms of the AWS Customer Agreement
Create Account and Continue

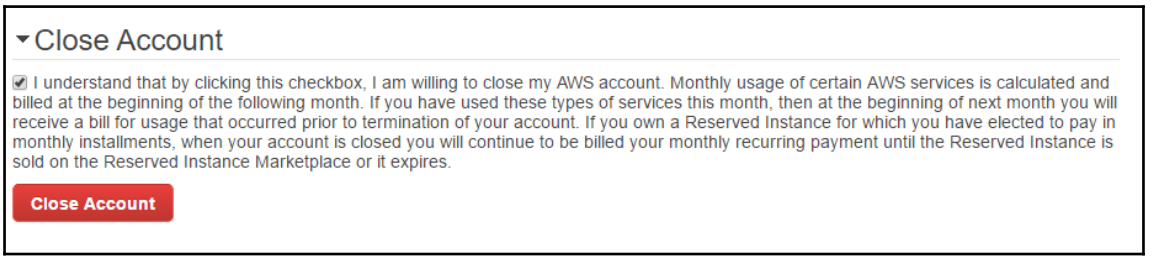

Payment Information
Please enter your payment information below. You will be able to try a broad set of AWS products for free via the Free Ter. We will only bill your credit or debit card for usage that is not covered by our Free Ter.
Frequently Asked Questions
Cardholder's Name
Credit/Debit Card Number
VISA
Expiration Date
Use my contact address
Use a new address
Please Note
As part of our card verification process we will charge INR 2 on your card when you click the "Verify Card and Continue" button below. This will be refunded once your card has been validated. Your bank may take 3-5 business days to show the refund. Mastercard/Visa customers may be redirected to your bank website to authorize the charge.
PAN Information
Do you have a PAN?
Yes
No
Verify Card and Continue


Identity Verification
You will be called immediately by an automated system and prompted to enter the PIN number provided.
1. Provide a telephone number
Please enter your information below and click the "Call Me Now" button.
Security Check
Refresh Image
Please type the characters as shown above
Country Code
India (+91)
Phone Number
Ext
Call Me Now
2. Call in progress
3. Identity verification complete


Support Plan
AWS Support offers a selection of plans to meet your needs. All plans provide 24x7 access to customer service, AWS documentation, whitepapers, and support forums. For access to technical support and additional resources to help you plan, deploy, and optimize your AWS environment, we recommend selecting a support plan that best aligns with your AWS usage.
All customers receive free Basic Support.
Basic Support
Basic
Description: Customer Service for account and billing questions and access to the AWS Community Forums.
Price: Included
Developer
Use case: Experimenting with AWS
Description: One primary contact may ask technical questions through Support Center and get a response within 12–24 hours during local business hours.
Price: Starts at $29/month (scales based on usage)
Business
Use case: Production use of AWS
Description: 24x7 support by phone and chat, 1-hour response to urgent support cases, and help with common third-party software. Full access to AWS Trusted Advisor for optimizing your AWS infrastructure, and access to the AWS Support API for automating your support cases and retrieving Trusted Advisor results.
Price: Starts at $100/month (scales based on usage)
To explore all features and benefits of AWS Support, including plan comparisons and pricing samples, click here.
Continue

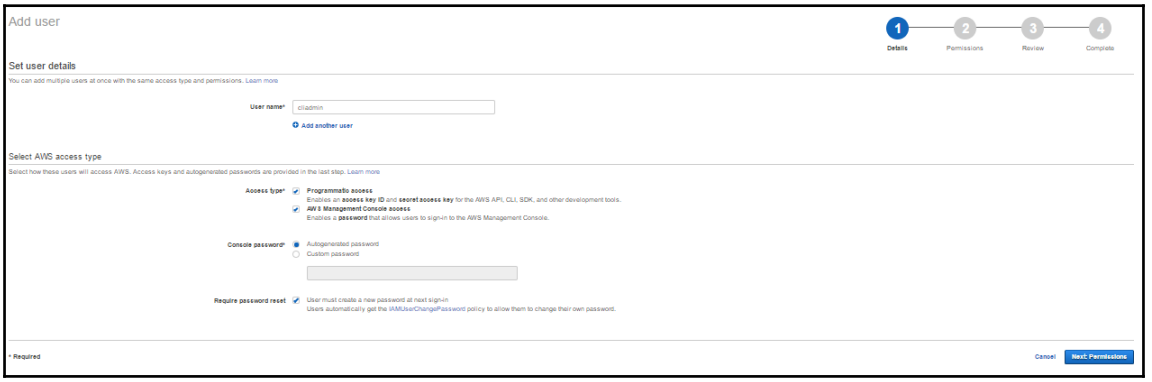

Registration Confirmation
Welcome to Amazon Web Services
Thank you for creating an Amazon Web Services Account. We are activating your account, which should only take a few minutes. You will receive an email when this is complete.
Sign In to the Console
Contact Sales

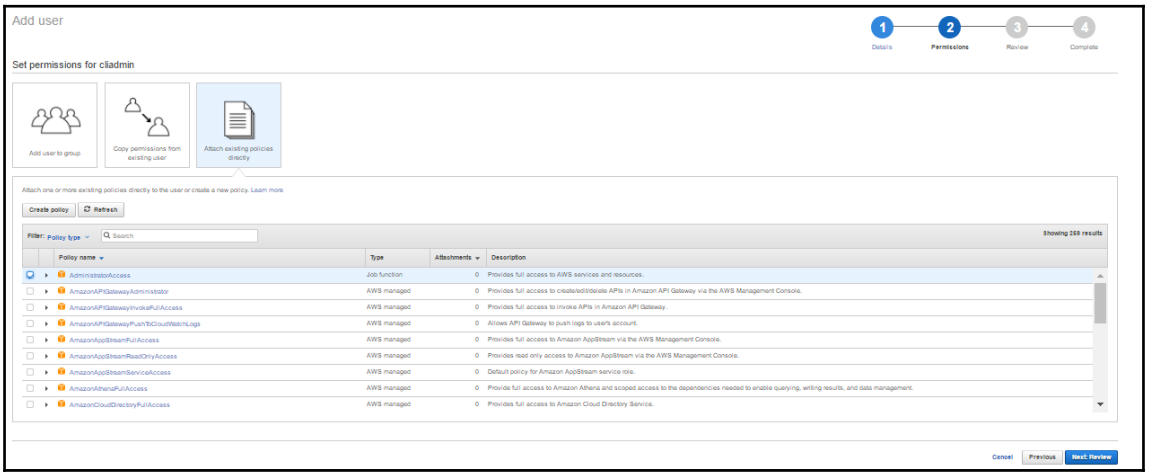

AWS services
Find a service by name or feature (for example, EC2, S3 or VM, storage).
Recently visited services
All services
Build a solution
Get started with simple wizards and automated workflows.
Launch a virtual machine
With EC2
~1 minute
Build a web app
With Elastic Beanstalk
~6 minutes
Host a static website
With S3, CloudFront, Route 53
~5 minutes
Connect an IoT device
With AWS IoT
~5 minutes
Start a development project
With CodeStar
~5 minutes
Register a domain
With Route 53
~3 minutes
See more
Helpful tips
Manage your costs
Get real-time billing alerts based on your cost and usage budgets. Start now
Create an organization
Use AWS Organizations for policy-based management of multiple AWS accounts. Start now
Explore AWS
New Product Announcements
View the latest announcements from the AWS Summit - San Francisco. Learn more.
Migrate from Oracle to Amazon Aurora
Learn how to migrate from Oracle to Amazon Aurora with minimal downtime. View project.


Close Account
I understand that by clicking this checkbox, I am willing to close my AWS account. Monthly usage of certain AWS services is calculated and billed at the beginning of the following month. If you have used these types of services this month, then at the beginning of next month you will receive a bill for usage that occurred prior to termination of your account. If you own a Reserved Instance for which you have elected to pay in monthly installments, when your account is closed you will continue to be billed your monthly recurring payment until the Reserved Instance is sold on the Reserved Instance Marketplace or it expires.
Close Account

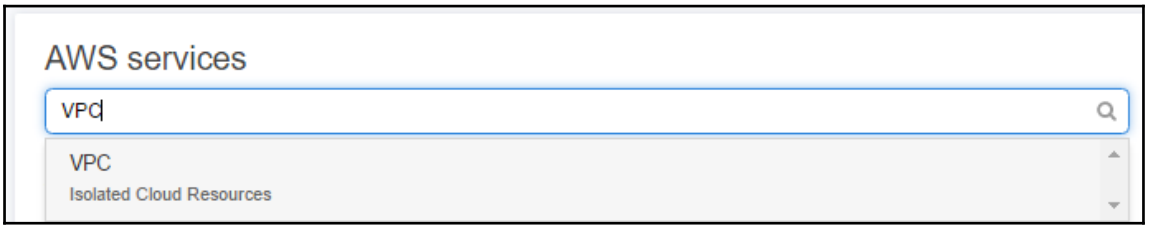
IAM users sign-in link:
https:/[redacted].signin.aws.amazon.com/console

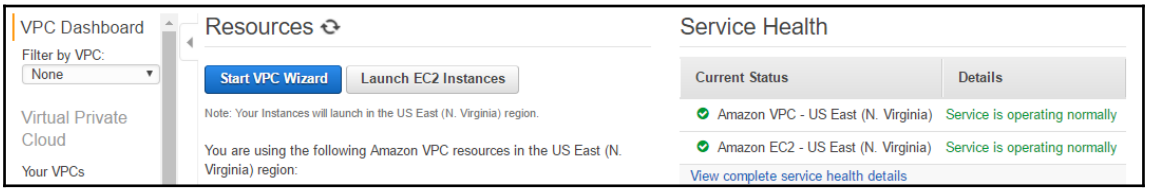
Search IAM
Add user
Delete user
Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Find users by username or access key
Showing 0 results
User name
Groups
Password
Last sign-in
Access keys
Creation time
No results

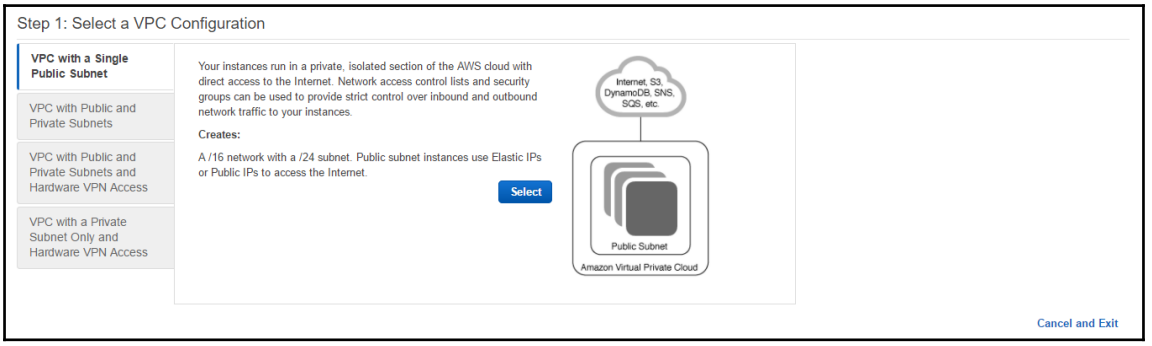

Add user
1 Details
2 Permissions
3 Review
4 Complete
Set user details
You can add multiple users at once with the same access type and permissions. Learn more
User name*
cliadmin
Add another user
Select AWS access type
Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more
Access type*
Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.
AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.
Console password*
Autogenerated password
Custom password
Require password reset
User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.
* Required
Cancel
Next: Permissions

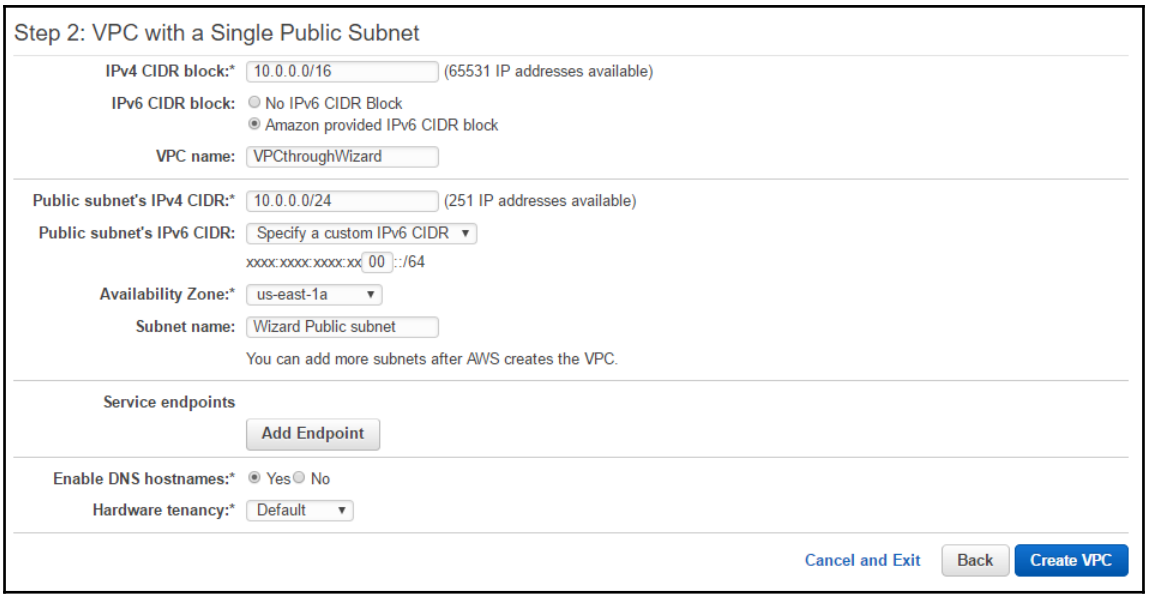

Add user
1 Details
2 Permissions
3 Review
4 Complete
Set permissions for cliadmin
Add user to group
Copy permissions from existing user
Attach existing policies directly
Attach one or more existing policies directly to the user or create a new policy. Learn more
Create policy
Refresh
Filter: Policy type
Search
Showing 269 results
Policy name
Type
Attachments
Description
AdministratorAccess
Job function
Provides full access to AWS services and resources.
AmazonAPIGatewayAdministrator
AWS managed
Provides full access to create/edit/delete APIs in Amazon API Gateway via the AWS Management Console.
AmazonAPIGatewayInvokeFullAccess
Provides full access to invoke APIs in Amazon API Gateway.
AmazonAPIGatewayPushToCloudWatchLogs
Allows API Gateway to push logs to user's account.
AmazonAppStreamFullAccess
Provides full access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamReadOnlyAccess
Provides read only access to Amazon AppStream via the AWS Management Console.
AmazonAppStreamServiceAccess
Default policy for Amazon AppStream service role.
AmazonAthenaFullAccess
Provide full access to Amazon Athena and scoped access to the dependencies needed to enable querying, writing results, and data management.
AmazonCloudDirectoryFullAccess
Provides full access to Amazon Cloud Directory Service.
Cancel
Previous
Next: Review

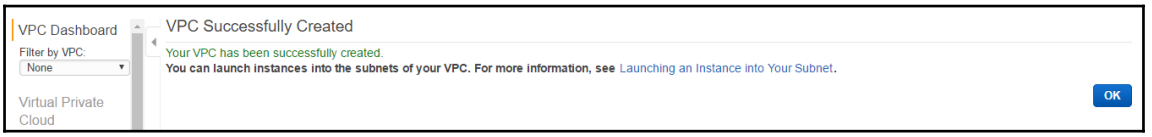
User name	Access key ID	Secret access key	Console login link

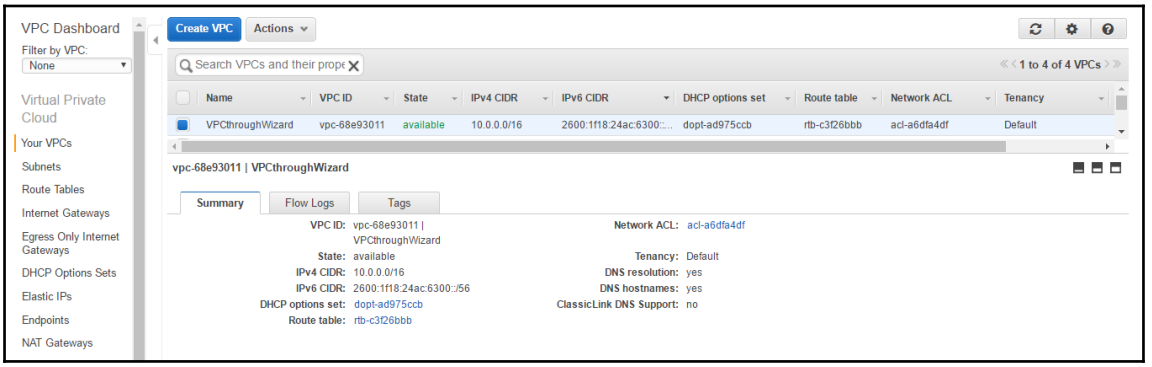


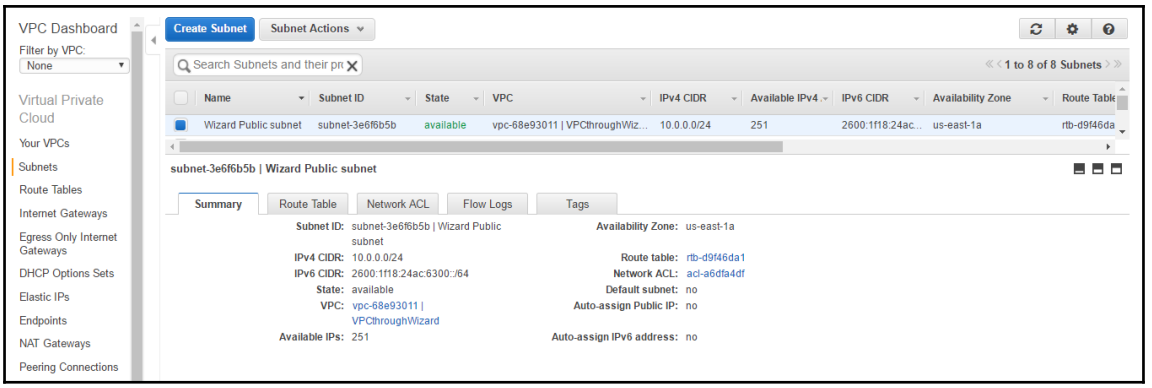


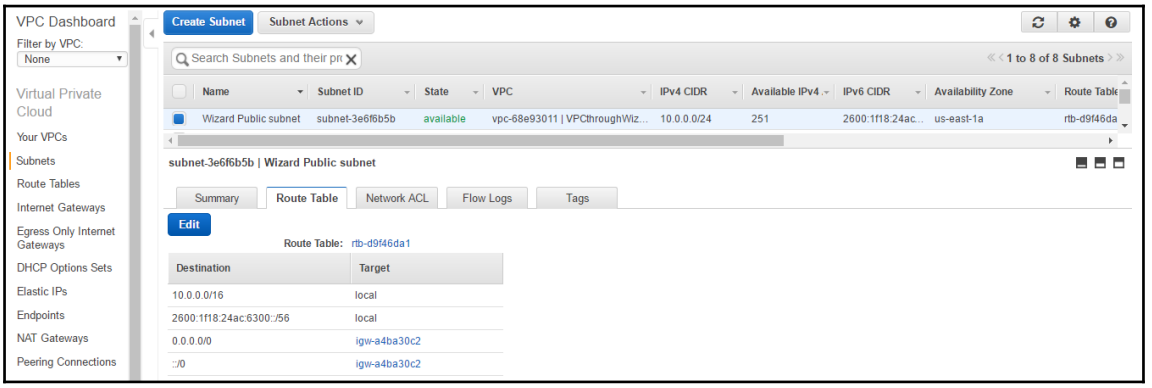


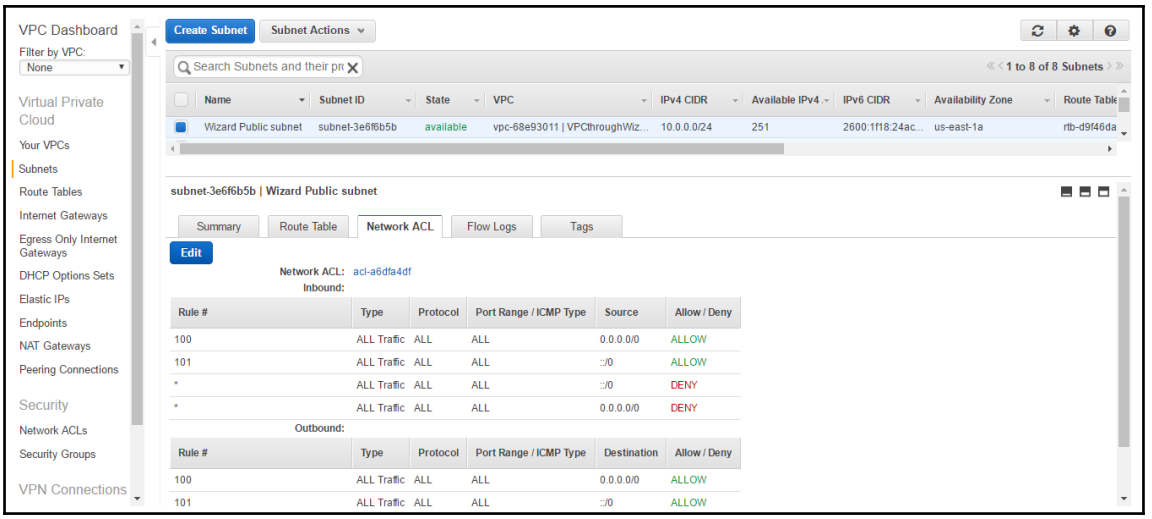

Step 2: VPC with a Single Public Subnet
IPv4 CIDR block:* 10.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
VPC name: VPCthroughWizard
Public subnet's IPv4 CIDR:* 10.0.0.0/24 (251 IP addresses available)
Public subnet's IPv6 CIDR: Specify a custom IPv6 CIDR
xxxx:xxxx:xxxx:xx 00 ::/64
Availability Zone:* us-east-1a
Subnet name: Wizard Public subnet
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Create VPC

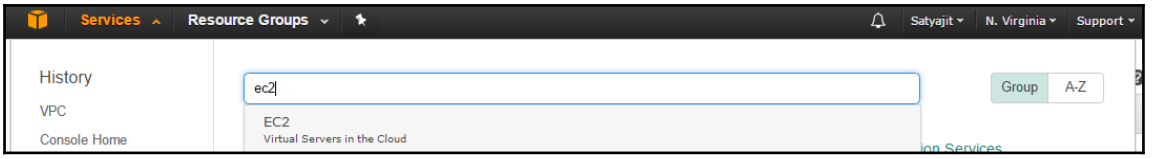

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
VPC Successfully Created
Your VPC has been successfully created.
You can launch instances into the subnets of your VPC. For more information, see Launching an Instance into Your Subnet.
OK

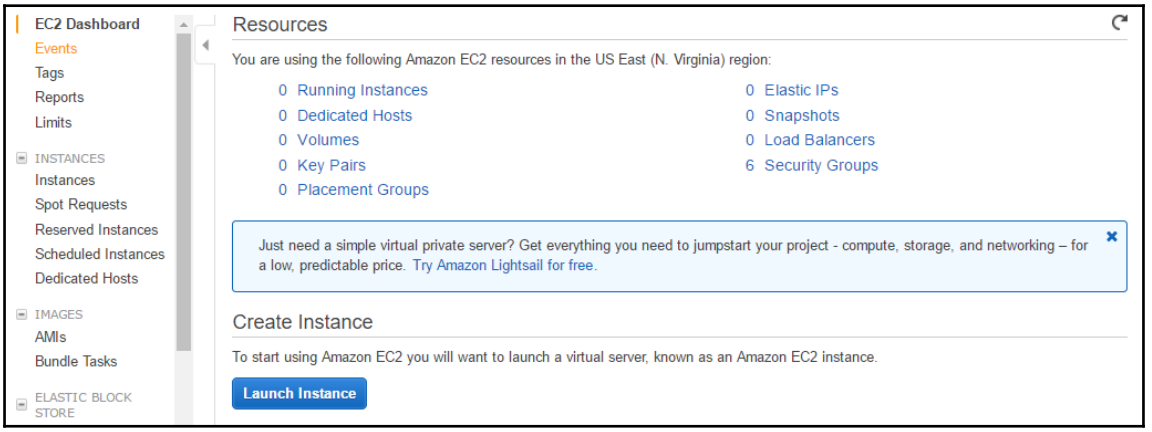

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create VPC
Actions
Search VPCs and their prop
1 to 4 of 4 VPCs
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCthroughWizard
vpc-68e93011
available
10.0.0.0/16
2600:1f18:24ac:6300:...
dopt-ad975ccb
rtb-c3f26bbb
acl-a6dfa4df
Default
vpc-68e93011 | VPCthroughWizard
Summary
Flow Logs
Tags
VPC ID: vpc-68e93011 | VPCthroughWizard
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR: 2600:1f18:24ac:6300::/56
DHCP options set: dopt-ad975ccb
Route table: rtb-c3f26bbb
Network ACL: acl-a6dfa4df
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

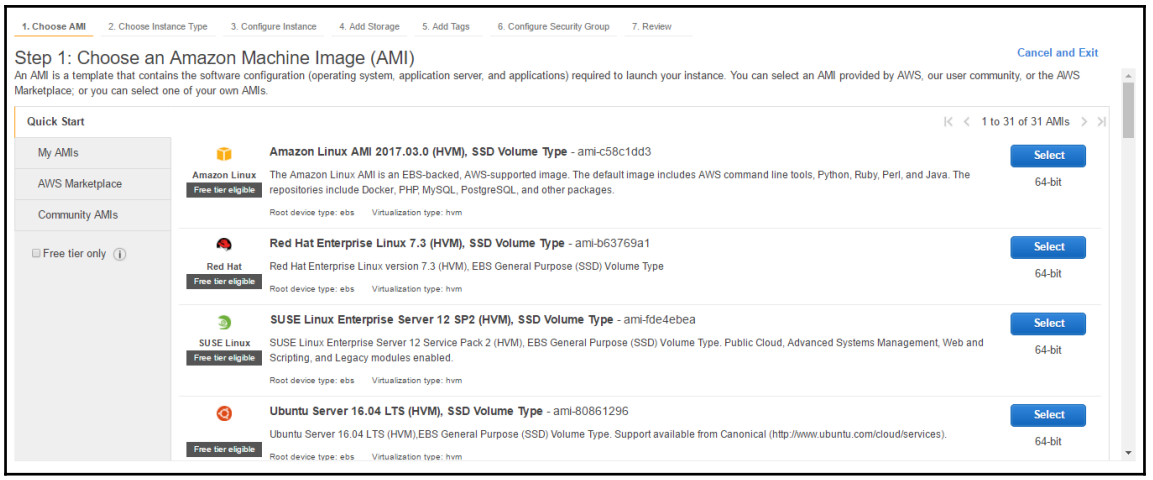

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Subnet
Subnet Actions
Search Subnets and their pr
1 to 8 of 8 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
Route Table
Wizard Public subnet
subnet-3e6f6b5b
available
vpc-68e93011 | VPCthroughWiz...
10.0.0.0/24
251
2600:1f18:24ac...
us-east-1a
rtb-d9f46da
subnet-3e6f6b5b | Wizard Public subnet
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-3e6f6b5b | Wizard Public subnet
IPv4 CIDR: 10.0.0.0/24
IPv6 CIDR: 2600:1f18:24ac:6300::/64
State: available
VPC: vpc-68e93011 | VPCthroughWizard
Available IPs: 251
Availability Zone: us-east-1a
Route table: rtb-d9f46da1
Network ACL: acl-a6dfa4df
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no

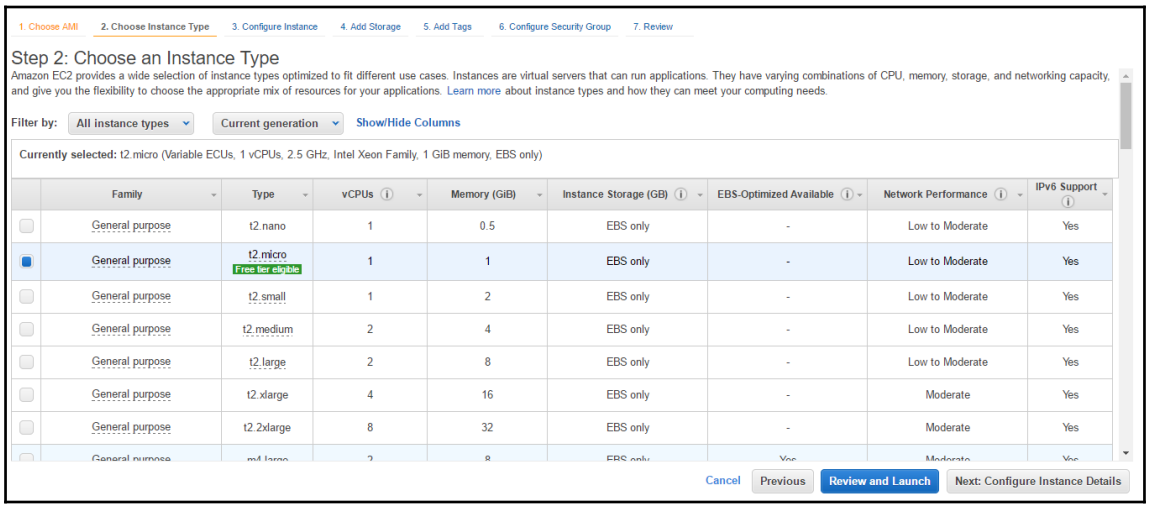

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Subnet
Subnet Actions
Search Subnets and their pr
1 to 8 of 8 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
Route Table
Wizard Public subnet
subnet-3e6f6b5b
available
vpc-68e93011 | VPCthroughWiz...
10.0.0.0/24
251
2600:1f18:24ac...
us-east-1a
rtb-d9f46da
subnet-3e6f6b5b | Wizard Public subnet
Summary
Route Table
Network ACL
Flow Logs
Tags
Edit
Route Table: rtb-d9f46da1
Destination
Target
10.0.0.0/16
local
2600:1f18:24ac:6300::/56
local
0.0.0.0/0
igw-a4ba30c2
::/0
igw-a4ba30c2

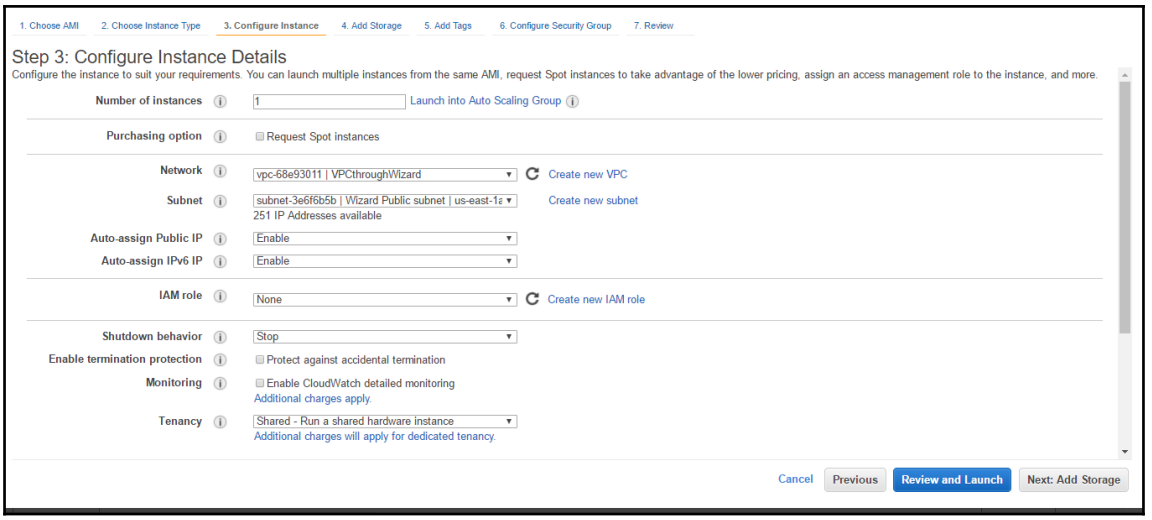

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
VPN Connections
Create Subnet
Subnet Actions
Search Subnets and their pr
1 to 8 of 8 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
Route Table
Wizard Public subnet
subnet-3e6f6b5b
available
vpc-68e93011 | VPCthroughWiz...
10.0.0.0/24
251
2600:1f18:24ac...
us-east-1a
rtb-d9f46da
subnet-3e6f6b5b | Wizard Public subnet
Summary
Route Table
Network ACL
Flow Logs
Tags
Edit
Network ACL: acl-a6dfa4df
Inbound:
Rule #
Type
Protocol
Port Range / ICMP Type
Source
Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
101 ALL Traffic ALL ALL ::/0 ALLOW
* ALL Traffic ALL ALL ::/0 DENY
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Outbound:
Rule #
Type
Protocol
Port Range / ICMP Type
Destination
Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
101 ALL Traffic ALL ALL ::/0 ALLOW

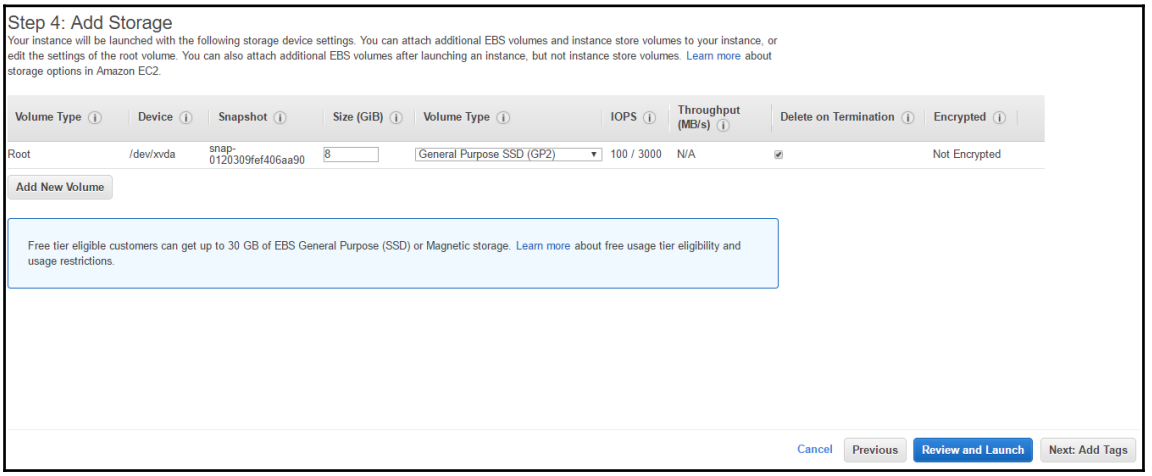

Services
Resource Groups
Satyajit
N. Virginia
Support
History
VPC
Console Home
ec2
EC2
Virtual Servers in the Cloud
Group
A-Z

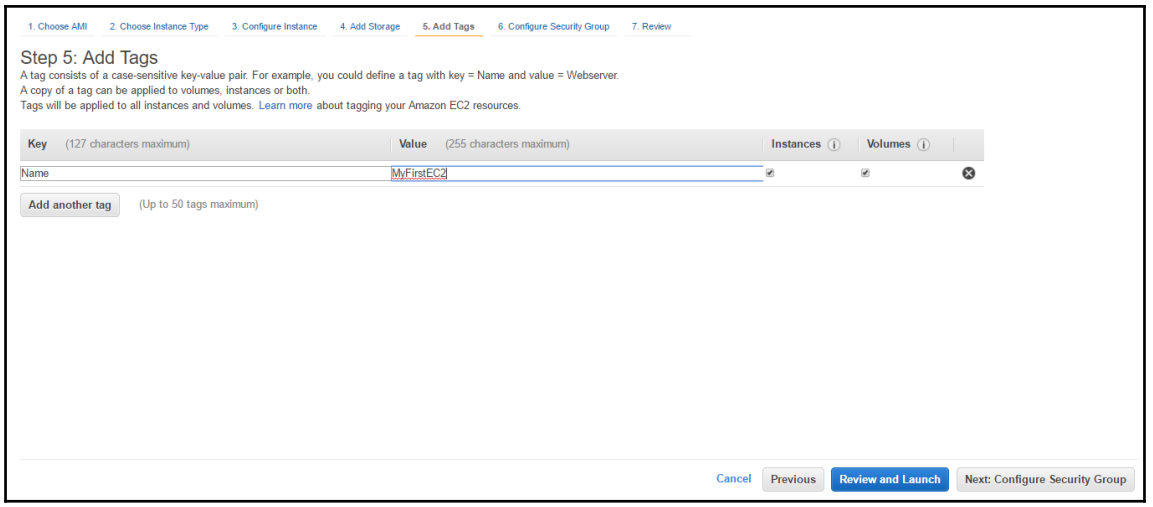

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Resources
You are using the following Amazon EC2 resources in the US East (N. Virginia) region:
0 Running Instances
0 Dedicated Hosts
0 Volumes
0 Key Pairs
0 Placement Groups
0 Elastic IPs
0 Snapshots
0 Load Balancers
6 Security Groups
Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance

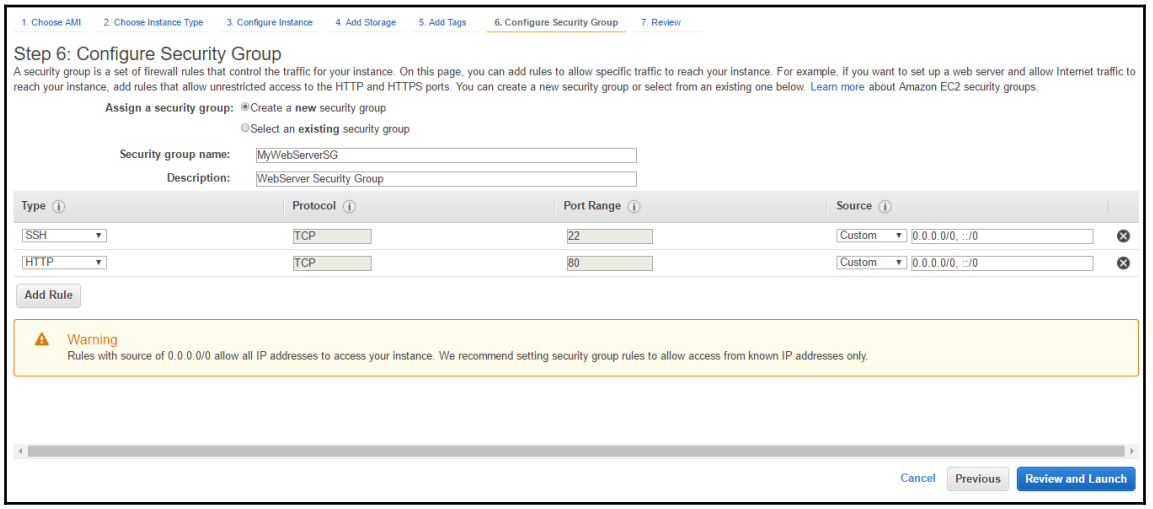

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Quick Start
1 to 31 of 31 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-c58c1dd3
Amazon Linux
Free tier eligible
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
Select
64-bit
Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-b63769a1
Red Hat
Free tier eligible
Red Hat Enterprise Linux version 7.3 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select
64-bit
SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-fde4ebea
SUSE Linux
Free tier eligible
SUSE Linux Enterprise Server 12 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
Select
64-bit
Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-80861296
Free tier eligible
Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm
Select
64-bit

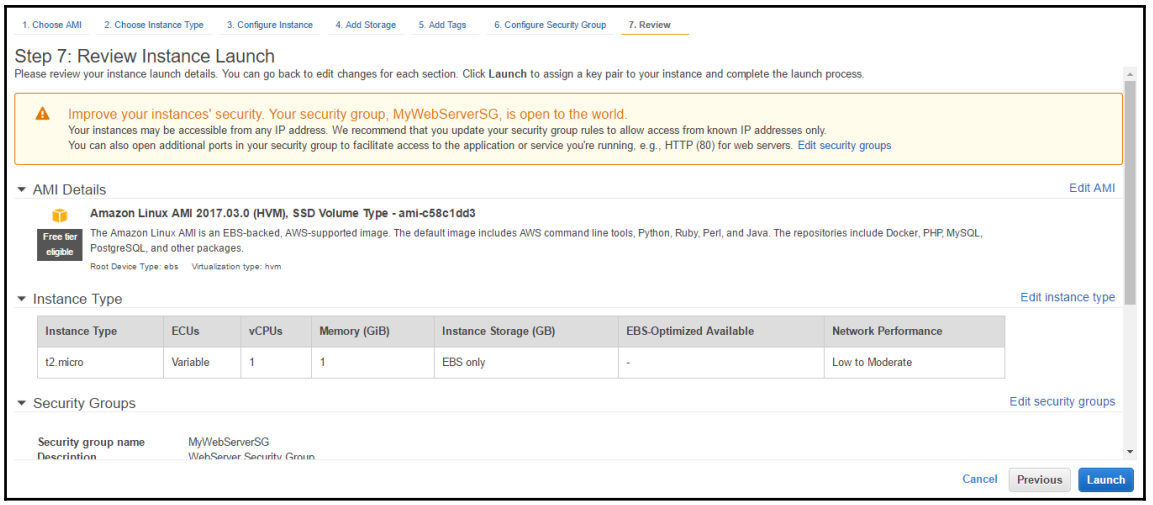

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
IPv6 Support
General purpose t2.nano 1 0.5 EBS only - Low to Moderate Yes
General purpose t2.micro Free tier eligible 1 1 EBS only - Low to Moderate Yes
General purpose t2.small 1 2 EBS only - Low to Moderate Yes
General purpose t2.medium 2 4 EBS only - Low to Moderate Yes
General purpose t2.large 2 8 EBS only - Low to Moderate Yes
General purpose t2.xlarge 4 16 EBS only - Moderate Yes
General purpose t2.2xlarge 8 32 EBS only - Moderate Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details

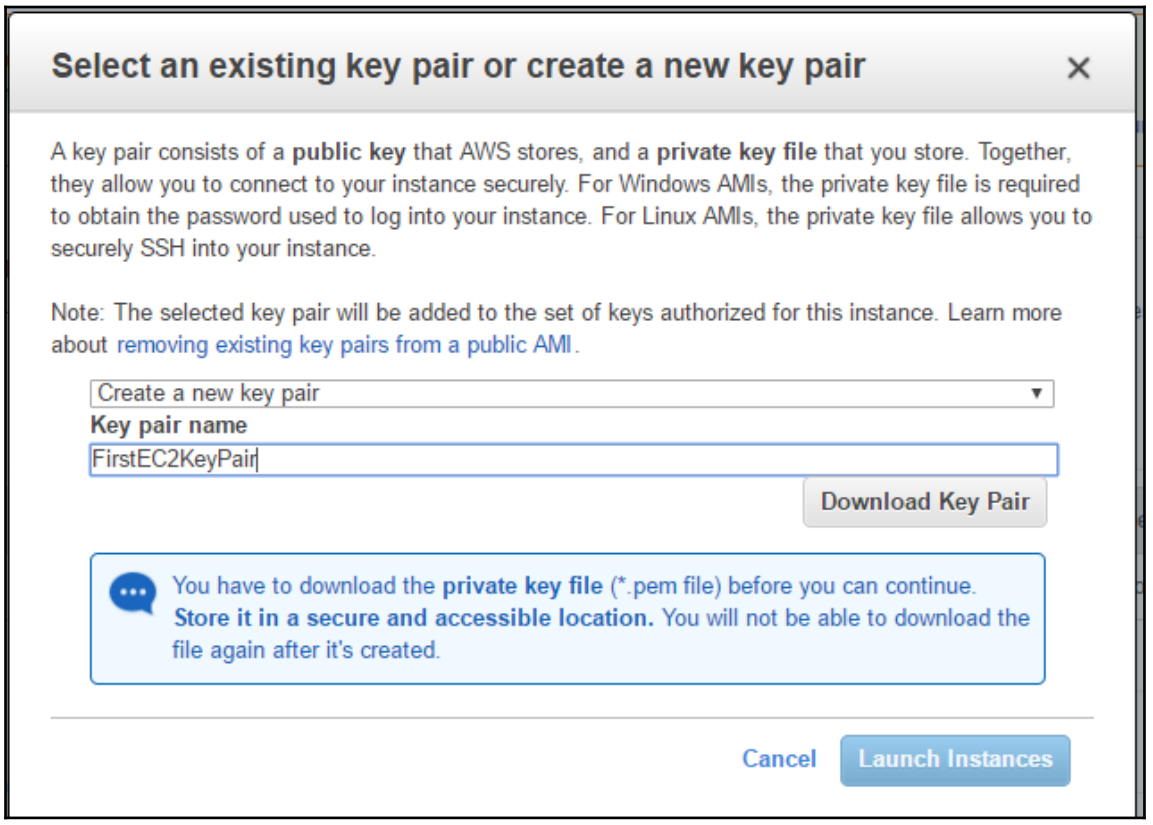

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-68e93011 | VPCthroughWizard
Create new VPC
Subnet
subnet-3e6f6b5b | Wizard Public subnet | us-east-1a
Create new subnet
251 IP Addresses available
Auto-assign Public IP
Enable
Auto-assign IPv6 IP
Enable
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Cancel
Previous
Review and Launch
Next: Add Storage

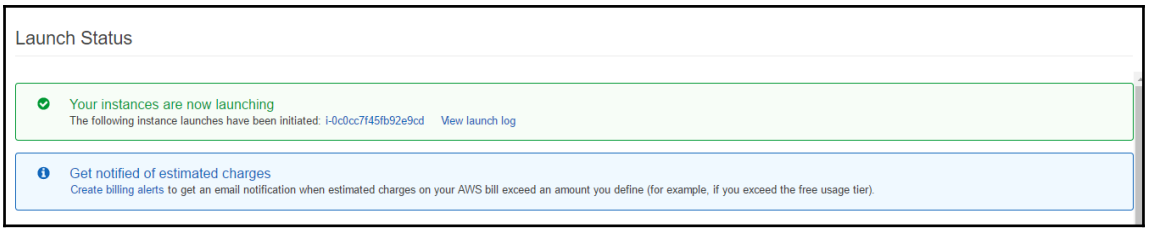

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encrypted
Root
/dev/xvda
snap-0120309fef406aa90
8
General Purpose SSD (GP2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags

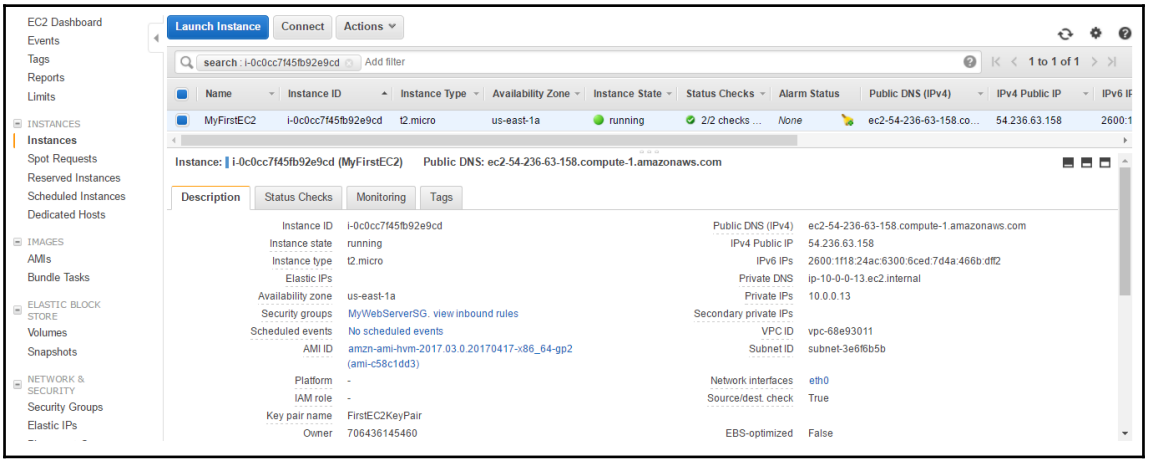

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.
Key (127 characters maximum)
Value (255 characters maximum)
Instances
Volumes
Name
MyFirstEC2
Add another tag
(Up to 50 tags maximum)
Cancel
Previous
Review and Launch
Next: Configure Security Group

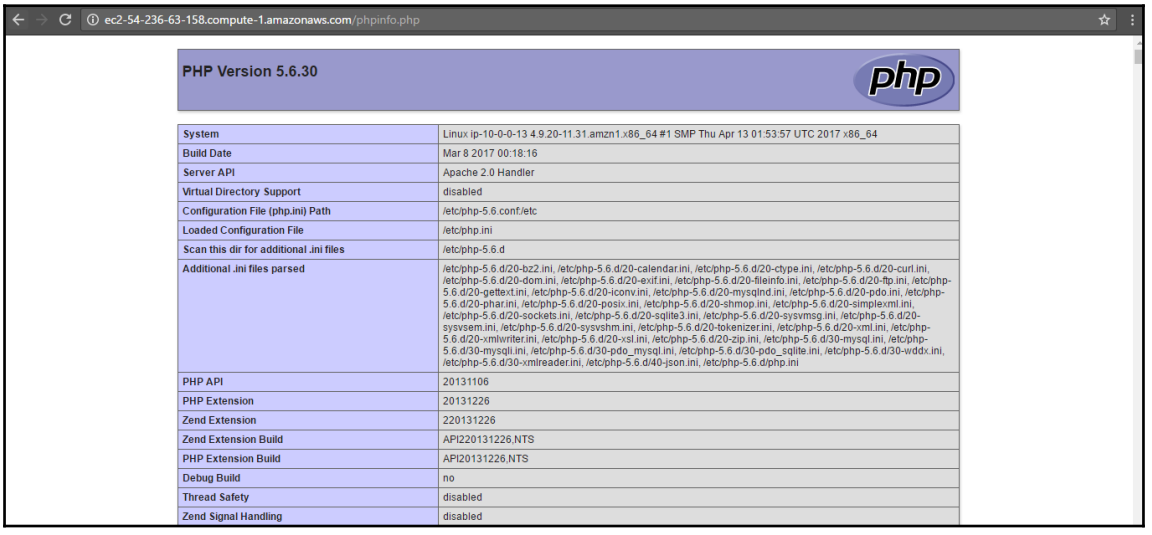

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
Security group name:
MyWebServerSG
Description:
WebServer Security Group
Type
Protocol
Port Range
Source
SSH
TCP
22
Custom
0.0.0.0/0, ::/0
HTTP
TCP
80
Custom
0.0.0.0/0, ::/0
Add Rule
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Cancel
Previous
Review and Launch


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, MyWebServerSG, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-c58c1dd3
Free tier eligible
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
t2.micro
Variable
1
1
EBS only
-
Low to Moderate
Security Groups
Edit security groups
Security group name
MyWebServerSG
Description
WebServer Security Group
Cancel
Previous
Launch


Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair name
FirstEC2KeyPair
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances

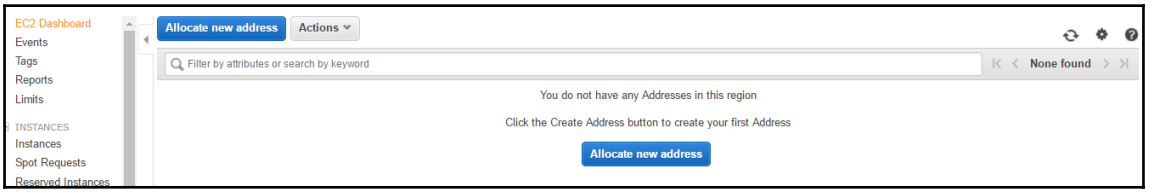




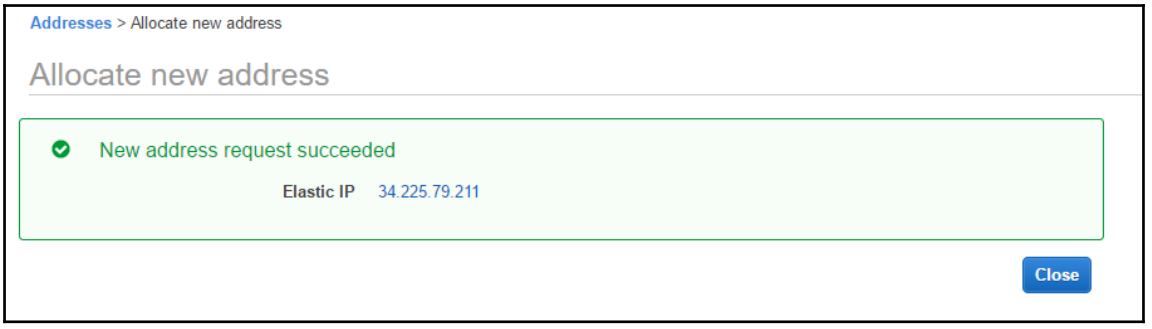


System	Linux ip-10-0-0-13 4.9.20-11.31.amzn1.x86_64 #1 SMP Thu Apr 13 01:53:57 UTC 2017 x86_64
Build Date	Mar 8 2017 00:18:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php-5.6.conf./etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php-5.6.d
Additional .ini files parsed	/etc/php-5.6.d/20-bz2.ini, /etc/php-5.6.d/20-calendar.ini, /etc/php-5.6.d/20-ctype.ini, /etc/php-5.6.d/20-curl.ini, /etc/php-5.6.d/20-dom.ini, /etc/php-5.6.d/20-exif.ini, /etc/php-5.6.d/20-fileinfo.ini, /etc/php-5.6.d/20-ftp.ini, /etc/php-5.6.d/20-gettext.ini, /etc/php-5.6.d/20-iconv.ini, /etc/php-5.6.d/20-mysqlnd.ini, /etc/php-5.6.d/20-pdo.ini, /etc/php-5.6.d/20-phar.ini, /etc/php-5.6.d/20-posix.ini, /etc/php-5.6.d/20-shmop.ini, /etc/php-5.6.d/20-simplexml.ini, /etc/php-5.6.d/20-sockets.ini, /etc/php-5.6.d/20-sqlite3.ini, /etc/php-5.6.d/20-sysvmsg.ini, /etc/php-5.6.d/20-sysvsem.ini, /etc/php-5.6.d/20-sysvshm.ini, /etc/php-5.6.d/20-tokenizer.ini, /etc/php-5.6.d/20-xml.ini, /etc/php-5.6.d/20-xmlwriter.ini, /etc/php-5.6.d/20-xsl.ini, /etc/php-5.6.d/20-zip.ini, /etc/php-5.6.d/30-mysql.ini, /etc/php-5.6.d/30-mysqli.ini, /etc/php-5.6.d/30-pdo_mysql.ini, /etc/php-5.6.d/30-pdo_sqlite.ini, /etc/php-5.6.d/30-wddx.ini, /etc/php-5.6.d/30-xmlreader.ini, /etc/php-5.6.d/40-json.ini, /etc/php-5.6.d/php.ini
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226
Zend Extension Build	API220131226,NTS
PHP Extension Build	API20131226,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

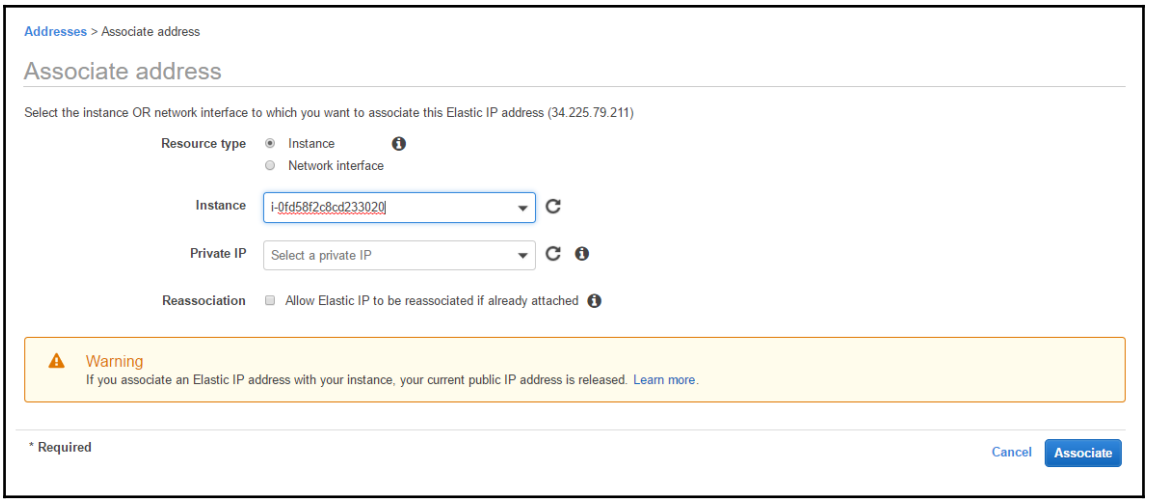
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
IPv6 IP
MyFirstEC2
i-0c0cc7f45fb92e9cd
t2.micro
us-east-1a
running
2/2 checks ...
None
ec2-54-236-63-158.co...
54.236.63.158
2600:1
Nat Instance
i-0fd58f2c8cd233020
t2.micro
us-east-1a
running
2/2 checks ...
None
ec2-34-205-26-14.com...
34.205.26.14
2600:1
Instance: i-0fd58f2c8cd233020 (Nat Instance)
Public DNS: ec2-34-205-26-14.compute-1.amazonaws.com
Description
Status Checks
Monitoring
Tags
Instance ID
i-0fd58f2c8cd233020
Instance state
running
Instance type
t2.micro
Elastic IPs
Availability zone
us-east-1a
Security groups
NATSG. view inbound rules
Scheduled events
No scheduled events
AMI ID
amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-c58c1dd3)
Platform
-
IAM role
-
Key pair name
FirstEC2KeyPair
Owner
706436145460
Public DNS (IPv4)
ec2-34-205-26-14.compute-1.amazonaws.com
IPv4 Public IP
34.205.26.14
IPv6 IPs
2600:1f18:24ac:6300:544a:2a15:347b:67d0
Private DNS
ip-10-0-0-25.ec2.internal
Private IPs
10.0.0.25
Secondary private IPs
VPC ID
vpc-68e93011
Subnet ID
subnet-3e6f6b5b
Network interfaces
eth0
Source/dest. check
True
EBS-optimized
False

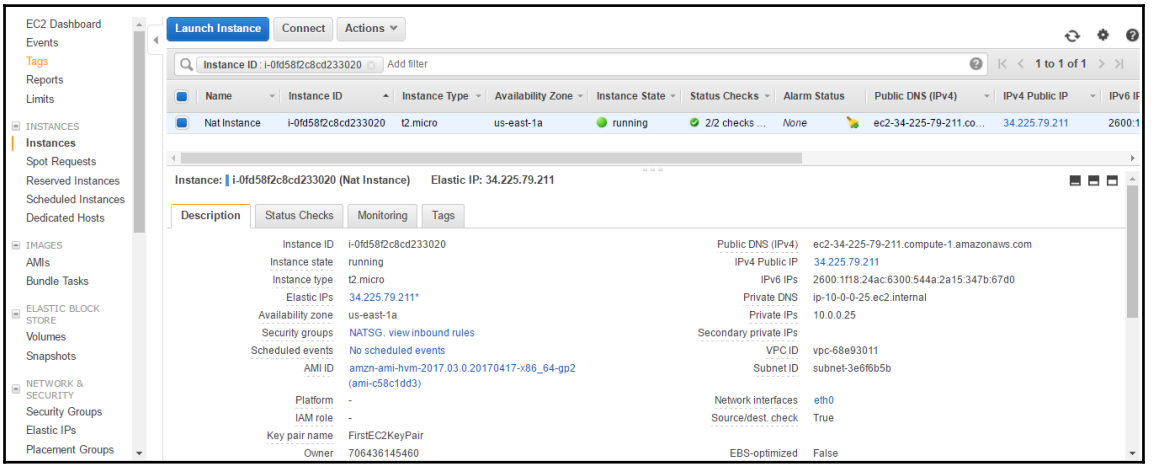

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Allocate new address
Actions
Filter by attributes or search by keyword
None found
You do not have any Addresses in this region
Click the Create Address button to create your first Address
Allocate new address

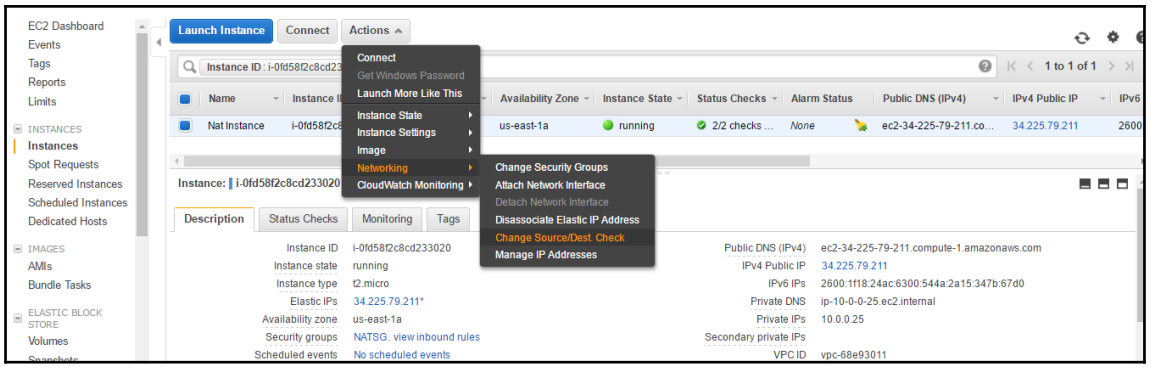
Allocate new address
Allocate a new Elastic IP address by selecting the scope in which it will be used
* Required
Cancel
Allocate

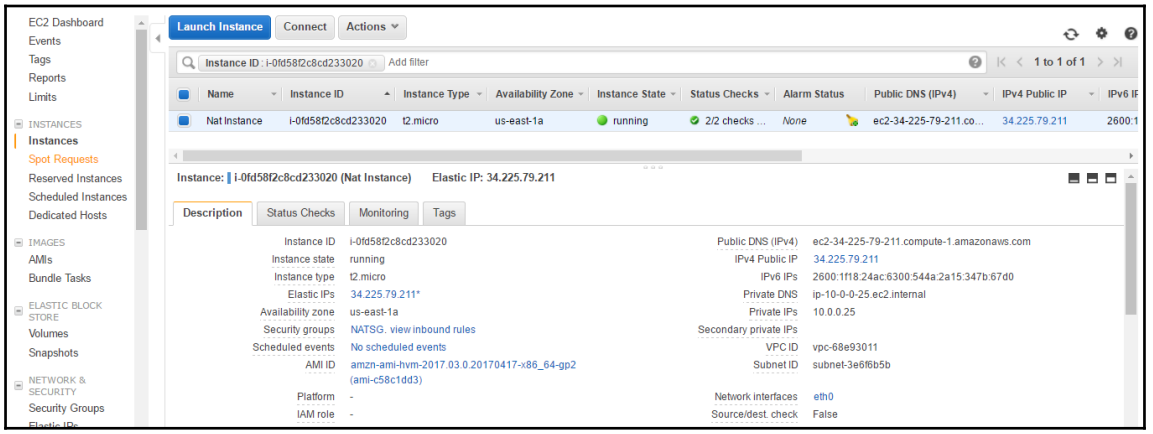

Addresses > Allocate new address
Allocate new address
New address request succeeded
Elastic IP
34.225.79.211
Close

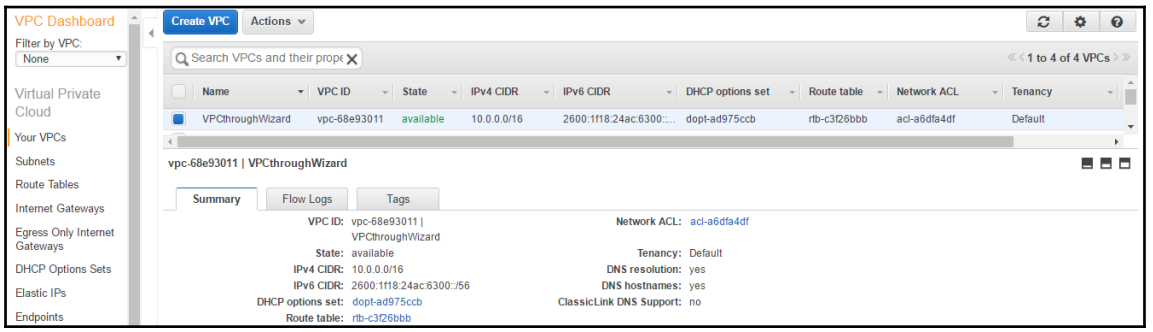
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Allocate new address
Actions
Release addresses
Associate address
Disassociate address
Move to VPC scope
Restore to EC2 scope
1 to 1 of 1
Elastic IP
Instance
Private IP address
Scope
Public DNS
Network Interface ID
34.225.79.211
vpc

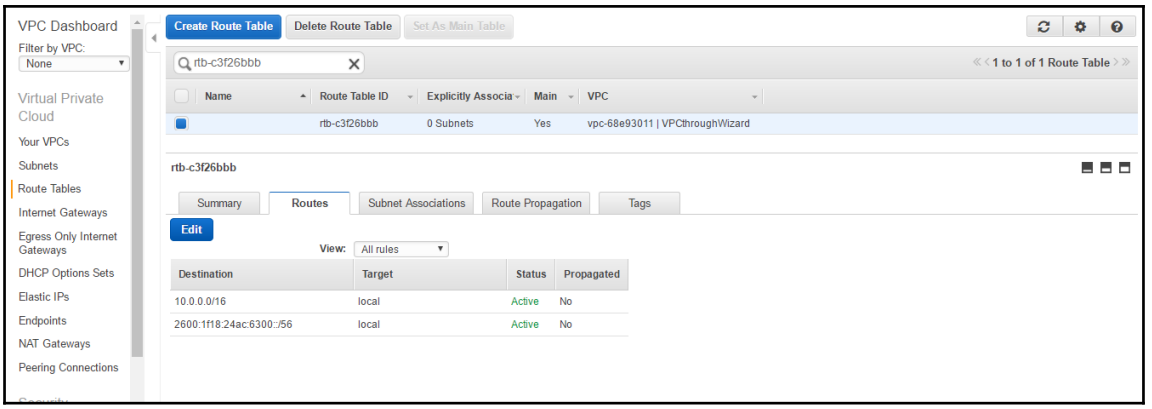

Addresses > Associate address
Associate address
Select the instance OR network interface to which you want to associate this Elastic IP address (34.225.79.211)
Resource type
Instance
Network interface
Instance
i-0fd58f2c8cd233020
Private IP
Select a private IP
Reassociation
Allow Elastic IP to be reassociated if already attached
Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.
* Required
Cancel
Associate

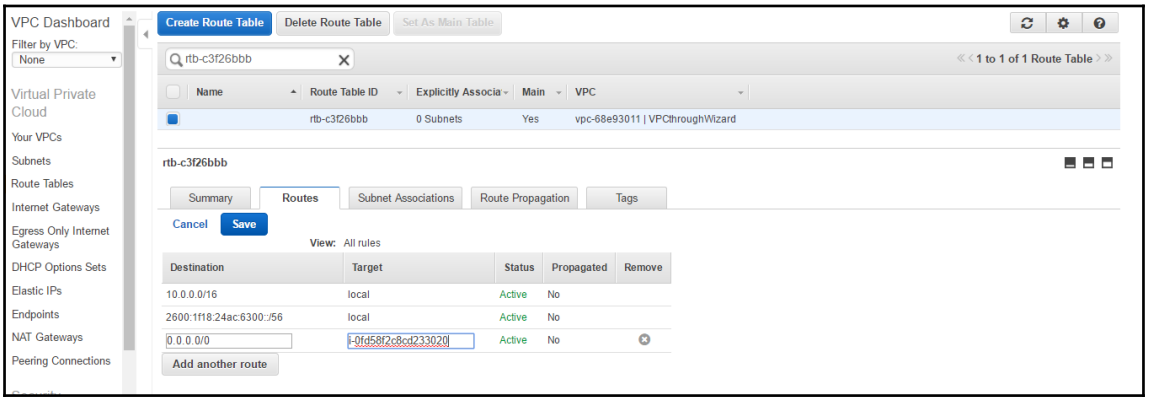

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Launch Instance
Connect
Actions
Instance ID : i-0fd58f2c8cd233020
Add filter
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
Nat Instance
i-0fd58f2c8cd233020
t2.micro
us-east-1a
running
2/2 checks ...
None
ec2-34-225-79-211.co...
34.225.79.211
Instance: i-0fd58f2c8cd233020 (Nat Instance)
Elastic IP: 34.225.79.211
Description
Status Checks
Monitoring
Tags
Instance ID
i-0fd58f2c8cd233020
Instance state
running
Instance type
t2.micro
Elastic IPs
34.225.79.211*
Availability zone
us-east-1a
Security groups
NATSG. view inbound rules
Scheduled events
No scheduled events
AMI ID
amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-c58c1dd3)
Platform
-
IAM role
-
Key pair name
FirstEC2KeyPair
Owner
706436145460
Public DNS (IPv4)
ec2-34-225-79-211.compute-1.amazonaws.com
IPv4 Public IP
34.225.79.211
IPv6 IPs
2600:1f18:24ac:6300:544a:2a15:347b:67d0
Private DNS
ip-10-0-0-25.ec2.internal
Private IPs
10.0.0.25
Secondary private IPs
VPC ID
vpc-68e93011
Subnet ID
subnet-3e6f6b5b
Network interfaces
eth0
Source/dest. check
True
EBS-optimized
False

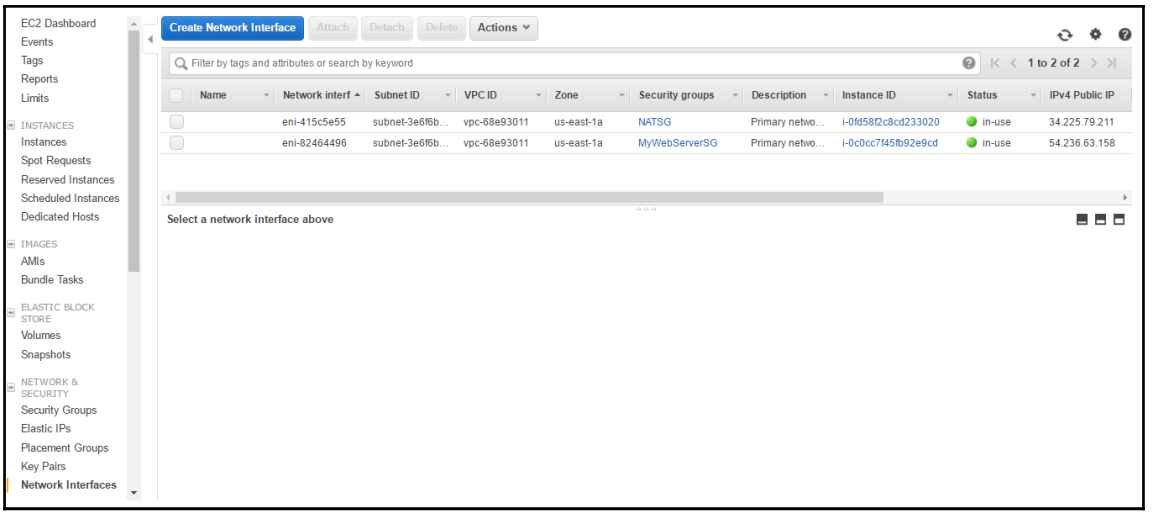

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Launch Instance
Connect
Actions
Connect
Get Windows Password
Launch More Like This
Instance State
Instance Settings
Image
Networking
CloudWatch Monitoring
Change Security Groups
Attach Network Interface
Detach Network Interface
Disassociate Elastic IP Address
Change Source/Dest. Check
Manage IP Addresses
Name
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
Nat Instance
us-east-1a
running
2/2 checks ...
None
34.225.79.211
Description
Status Checks
Monitoring
Tags
Instance ID i-0fd58f2c8cd233020
Instance state running
Instance type t2.micro
Elastic IPs 34.225.79.211*
Availability zone us-east-1a
Security groups NATSG. view inbound rules
Scheduled events No scheduled events
Public DNS (IPv4) ec2-34-225-79-211.compute-1.amazonaws.com
IPv4 Public IP 34.225.79.211
IPv6 IPs 2600:1f18:24ac:6300:544a:2a15:347b:67d0
Private DNS ip-10-0-0-25.ec2.internal
Private IPs 10.0.0.25
Secondary private IPs
VPC ID vpc-68e93011

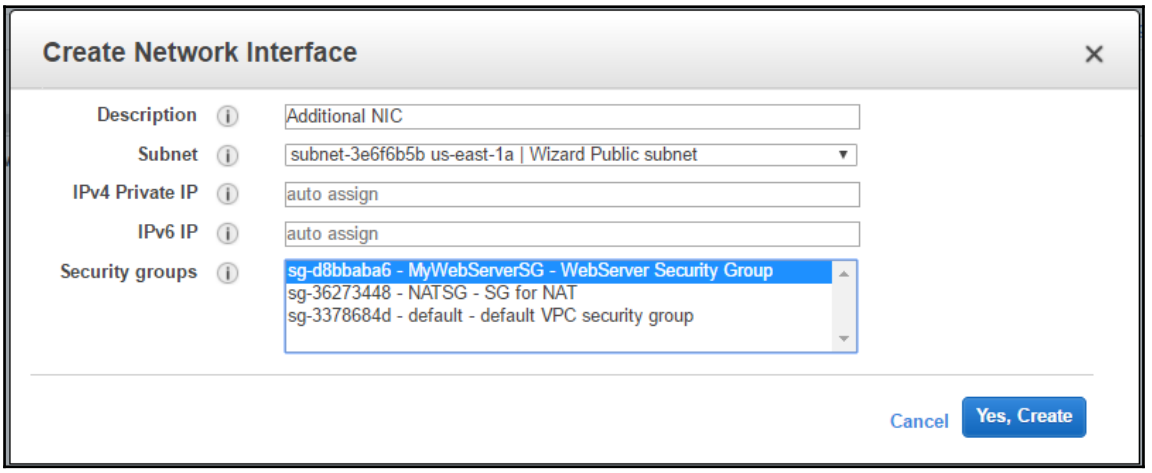

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Launch Instance
Connect
Actions
Add filter
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
Nat Instance
i-0fd58f2c8cd233020
t2.micro
us-east-1a
running
2/2 checks ...
None
34.225.79.211
Instance: i-0fd58f2c8cd233020 (Nat Instance) Elastic IP: 34.225.79.211
Description
Status Checks
Monitoring
Tags
Instance ID i-0fd58f2c8cd233020
Instance state running
Instance type t2.micro
Elastic IPs 34.225.79.211*
Availability zone us-east-1a
Security groups NATSG. view inbound rules
Scheduled events No scheduled events
AMI ID amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-c58c1dd3)
Platform -
IAM role -
Public DNS (IPv4) ec2-34-225-79-211.compute-1.amazonaws.com
IPv4 Public IP 34.225.79.211
IPv6 IPs 2600:1f18:24ac:6300:544a:2a15:347b:67d0
Private DNS ip-10-0-0-25.ec2.internal
Private IPs 10.0.0.25
Secondary private IPs
VPC ID vpc-68e93011
Subnet ID subnet-3e6f6b5b
Network interfaces eth0
Source/dest. check False

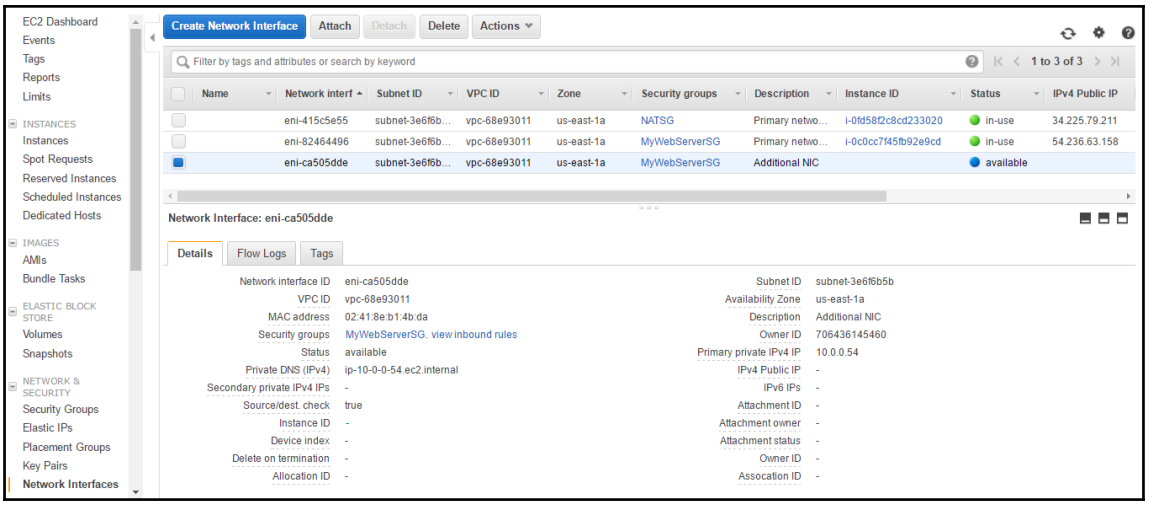

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create VPC
Actions
Search VPCs and their prope
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCthroughWizard
vpc-68e93011
available
10.0.0.0/16
2600:1f18:24ac:6300:...
dopt-ad975ccb
rtb-c3f26bbb
acl-a6dfa4df
Default
vpc-68e93011 | VPCthroughWizard
Summary
Flow Logs
Tags
VPC ID: vpc-68e93011 | VPCthroughWizard
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR: 2600:1f18:24ac:6300::/56
DHCP options set: dopt-ad975ccb
Route table: rtb-c3f26bbb
Network ACL: acl-a6dfa4df
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

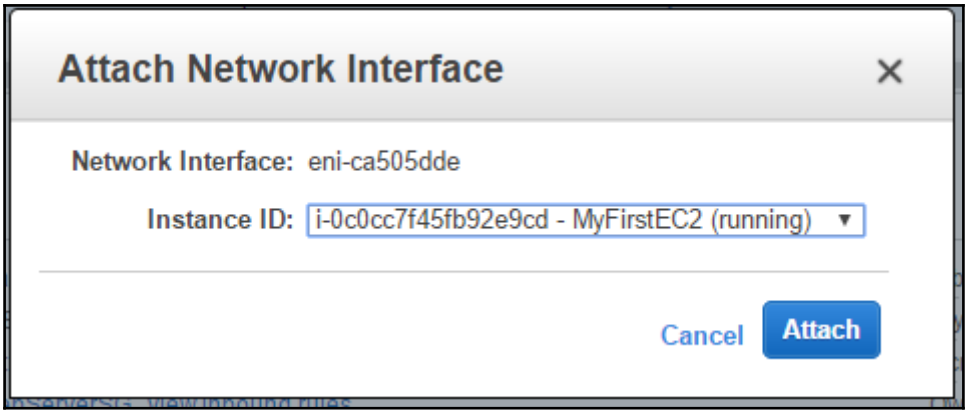

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
rtb-c3f26bbb
1 to 1 of 1 Route Table
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-c3f26bbb
0 Subnets
Yes
vpc-68e93011 | VPCthroughWizard
rtb-c3f26bbb
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
View:
All rules
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No
2600:1f18:24ac:6300::/56
local
Active
No

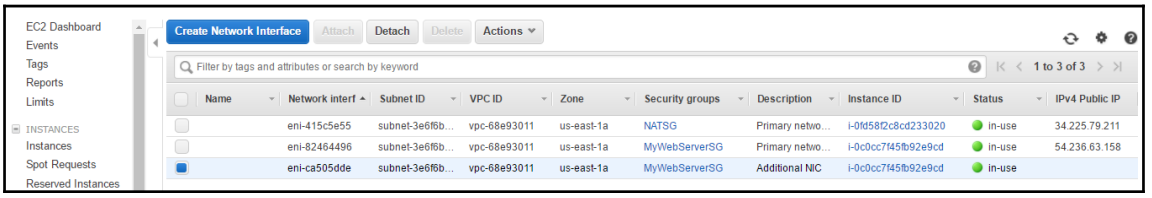

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
rtb-c3f26bbb
1 to 1 of 1 Route Table
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-c3f26bbb
0 Subnets
Yes
vpc-68e93011 | VPCthroughWizard
rtb-c3f26bbb
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View:
All rules
Destination
Target
Status
Propagated
Remove
10.0.0.0/16
local
Active
No
2600:1f18:24ac:6300::/56
local
Active
No
0.0.0.0/0
i-0fd58f2c8cd233020
Active
No
Add another route

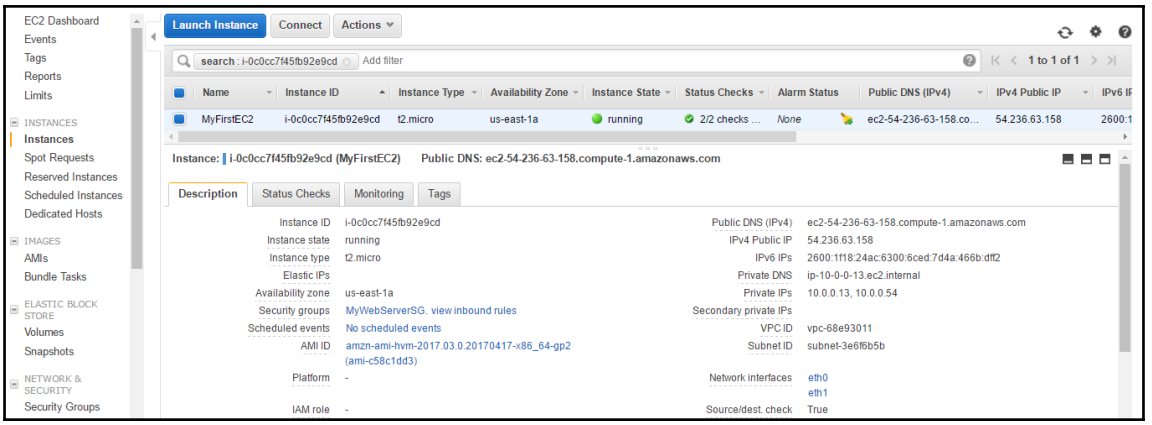

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Create Network Interface
Attach
Detach
Delete
Actions
Filter by tags and attributes or search by keyword
1 to 2 of 2
Name
Network interf
Subnet ID
VPC ID
Zone
Security groups
Description
Instance ID
Status
IPv4 Public IP
eni-415c5e55 subnet-3e6f6b... vpc-68e93011 us-east-1a NATSG Primary netwo... i-0fd58f2c8cd233020 in-use 34.225.79.211
eni-82464496 subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Primary netwo... i-0c0cc7f45fb92e9cd in-use 54.236.63.158
Select a network interface above


Create Network Interface
Description
Additional NIC
Subnet
subnet-3e6f6b5b us-east-1a | Wizard Public subnet
IPv4 Private IP
auto assign
IPv6 IP
auto assign
Security groups
sg-d8bbaba6 - MyWebServerSG - WebServer Security Group
sg-36273448 - NATSG - SG for NAT
sg-3378684d - default - default VPC security group
Cancel
Yes, Create


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Create Network Interface
Attach
Detach
Delete
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Network interf
Subnet ID
VPC ID
Zone
Security groups
Description
Instance ID
Status
IPv4 Public IP
eni-415c5e55 subnet-3e6f6b... vpc-68e93011 us-east-1a NATSG Primary netwo... i-0fd58f2c8cd233020 in-use 34.225.79.211
eni-82464496 subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Primary netwo... i-0c0cc7f45fb92e9cd in-use 54.236.63.158
eni-ca505dde subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Additional NIC available
Network Interface: eni-ca505dde
Details
Flow Logs
Tags
Network interface ID eni-ca505dde
VPC ID vpc-68e93011
MAC address 02:41:8e:b1:4b:da
Security groups MyWebServerSG. view inbound rules
Status available
Private DNS (IPv4) ip-10-0-0-54.ec2.internal
Secondary private IPv4 IPs -
Source/dest. check true
Instance ID -
Device index -
Delete on termination -
Allocation ID -
Subnet ID subnet-3e6f6b5b
Availability Zone us-east-1a
Description Additional NIC
Owner ID 706436145460
Primary private IPv4 IP 10.0.0.54
IPv4 Public IP -
IPv6 IPs -
Attachment ID -
Attachment owner -
Attachment status -
Owner ID -
Assocation ID -

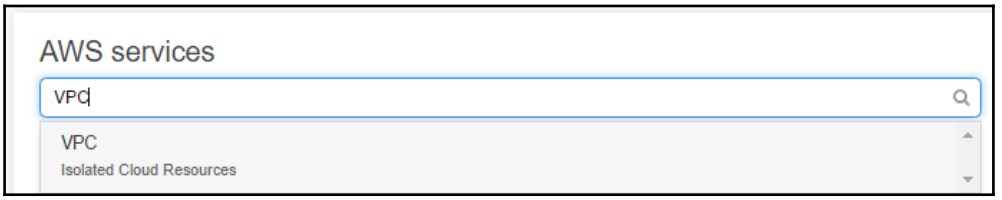

Attach Network Interface
Network Interface: eni-ca505dde
Instance ID: i-0c0cc7f45fb92e9cd - MyFirstEC2 (running)
Cancel
Attach

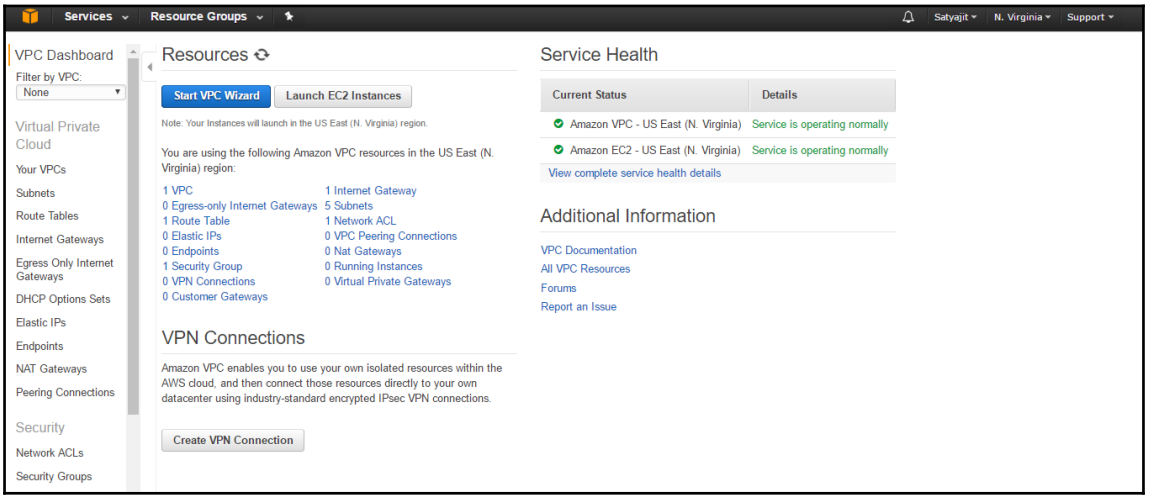

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Create Network Interface
Attach
Detach
Delete
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Network interf
Subnet ID
VPC ID
Zone
Security groups
Description
Instance ID
Status
IPv4 Public IP
eni-415c5e55 subnet-3e6f6b... vpc-68e93011 us-east-1a NATSG Primary netwo... i-0fd58f2c8cd233020 in-use 34.225.79.211
eni-82464496 subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Primary netwo... i-0c0cc7f45fb92e9cd in-use 54.236.63.158
eni-ca505dde subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Additional NIC i-0c0cc7f45fb92e9cd in-use

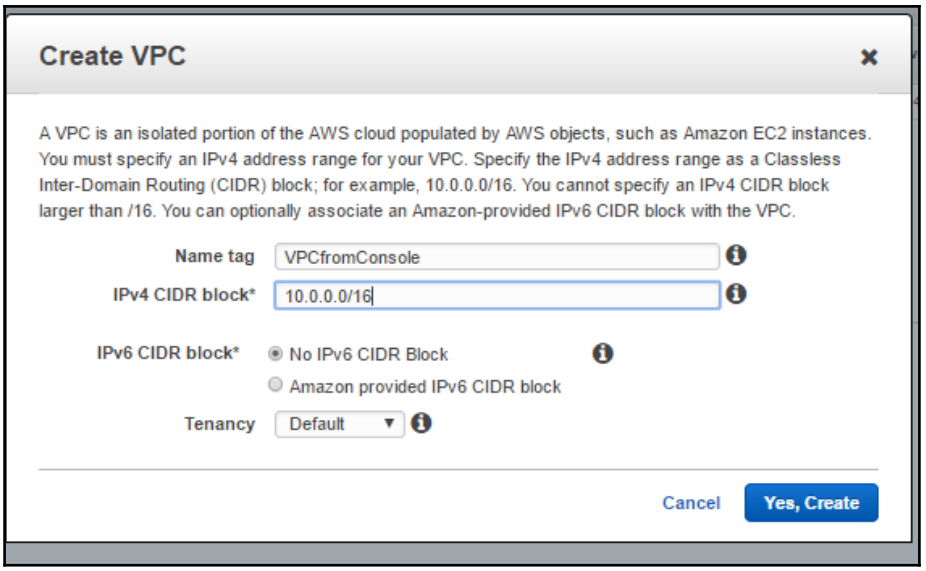


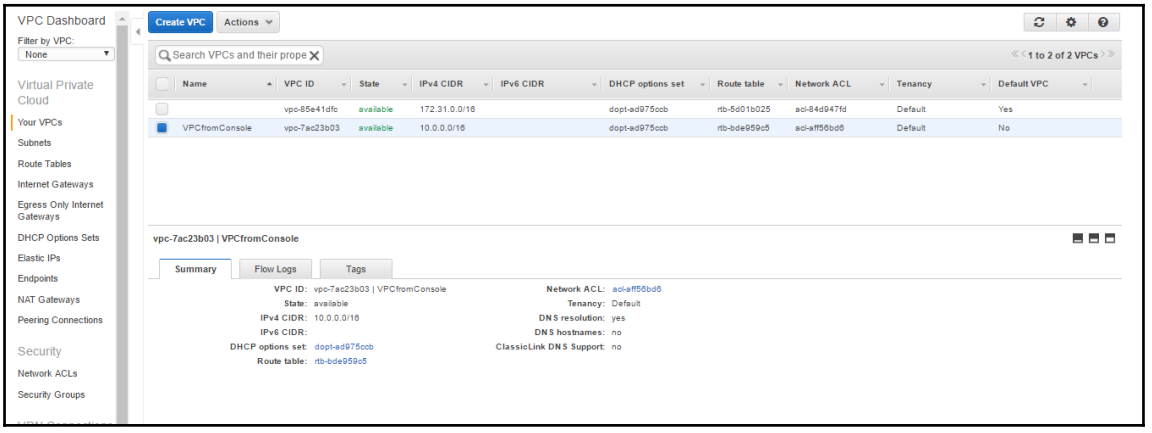

```
C:\>aws configure
AWS Access Key ID:
AWS Secret Access Key:
Default region name:
Default output format:
```

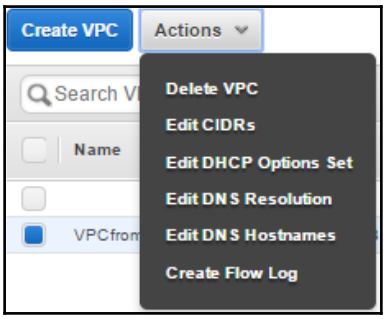
Chapter 2: Building Your Own Custom VPC

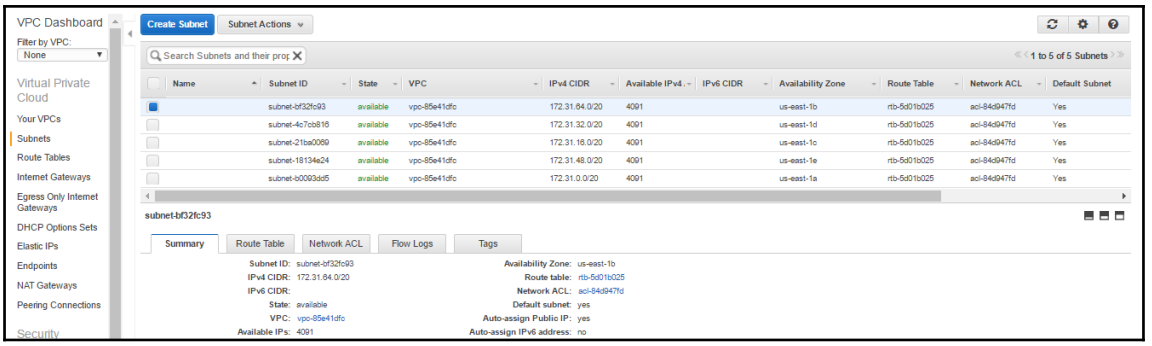


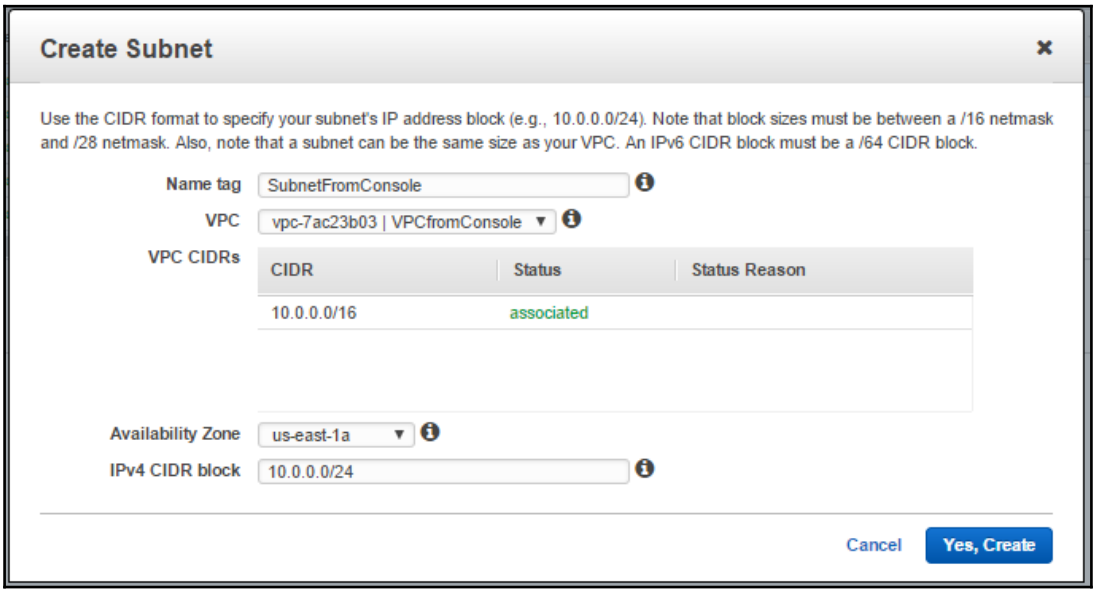


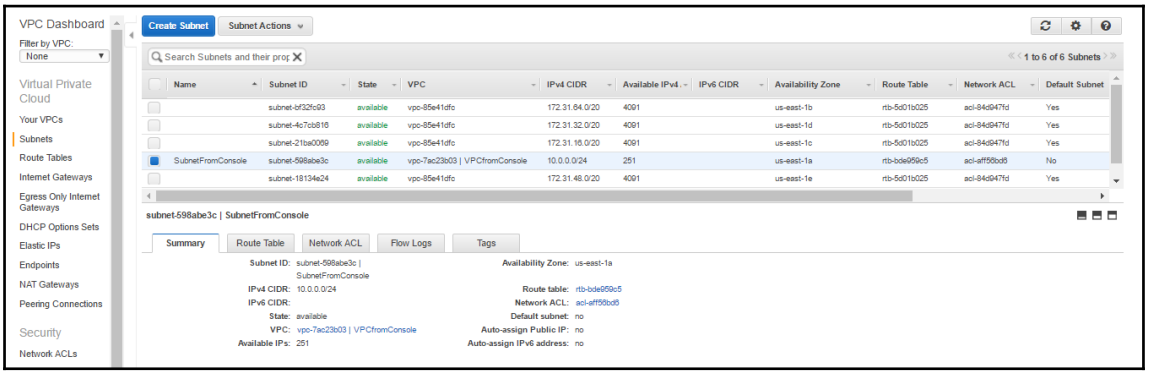

Create VPC
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an Amazon-provided IPv6 CIDR block with the VPC.
Name tag
VPCfromConsole
IPv4 CIDR block*
10.0.0.0/16
IPv6 CIDR block*
No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
Tenancy
Default
Cancel
Yes, Create

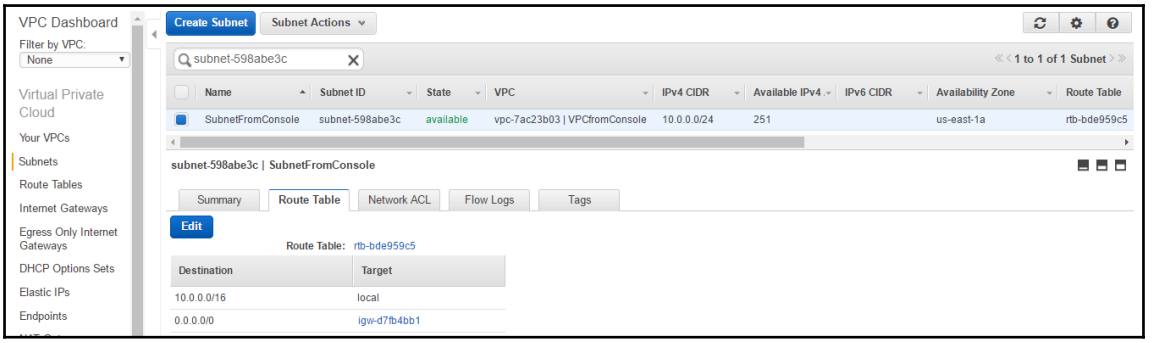

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create VPC
Actions
Search VPCs and their prope
1 to 2 of 2 VPCs
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
Default VPC
vpc-85e41dfc available 172.31.0.0/16 dopt-ad975ccb rtb-5d01b025 acl-84d947fd Default Yes
VPCfromConsole vpc-7ac23b03 available 10.0.0.0/16 dopt-ad975ccb rtb-bde959c5 acl-aff56bd6 Default No
vpc-7ac23b03 | VPCfromConsole
Summary
Flow Logs
Tags
VPC ID: vpc-7ac23b03 | VPCfromConsole
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR:
DHCP options set: dopt-ad975ccb
Route table: rtb-bde959c5
Network ACL: acl-aff56bd6
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
ClassicLink DNS Support: no

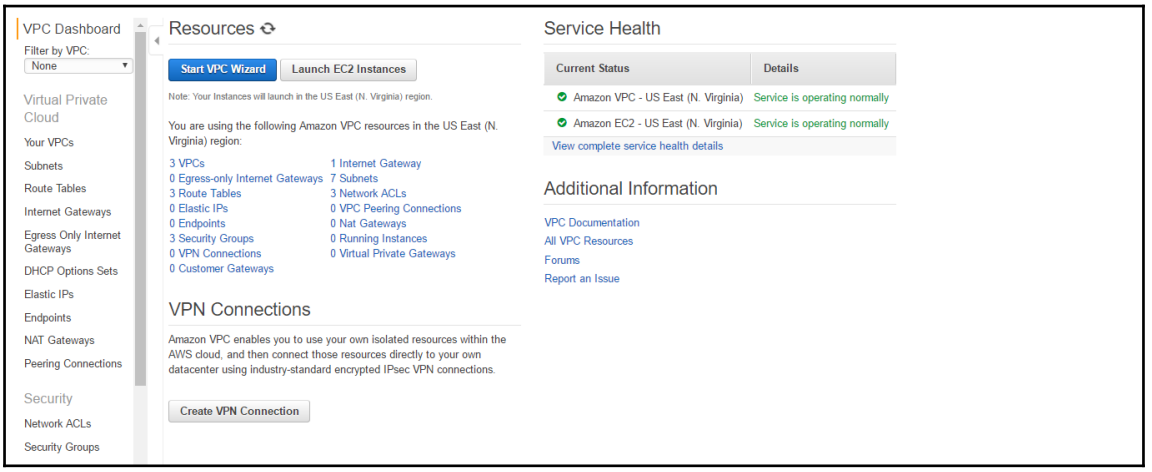

Create VPC
Actions
Search V
Name
VPCfrom
Delete VPC
Edit CIDRs
Edit DHCP Options Set
Edit DNS Resolution
Edit DNS Hostnames
Create Flow Log

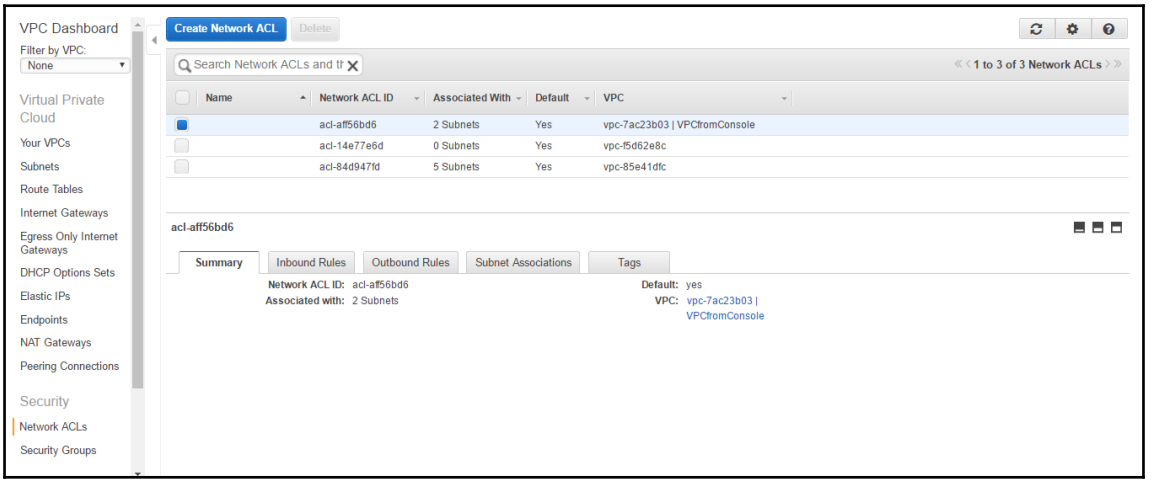

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 5 of 5 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4...
IPv6 CIDR
Availability Zone
Route Table
Network ACL
Default Subnet
subnet-bf32fc93 available vpc-85e41dfc 172.31.64.0/20 4091 us-east-1b rtb-5d01b025 acl-84d947fd Yes
subnet-4c7cb816 available vpc-85e41dfc 172.31.32.0/20 4091 us-east-1d rtb-5d01b025 acl-84d947fd Yes
subnet-21ba0069 available vpc-85e41dfc 172.31.16.0/20 4091 us-east-1c rtb-5d01b025 acl-84d947fd Yes
subnet-18134e24 available vpc-85e41dfc 172.31.48.0/20 4091 us-east-1e rtb-5d01b025 acl-84d947fd Yes
subnet-b0093dd5 available vpc-85e41dfc 172.31.0.0/20 4091 us-east-1a rtb-5d01b025 acl-84d947fd Yes
subnet-bf32fc93
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-bf32fc93
IPv4 CIDR: 172.31.64.0/20
IPv6 CIDR:
State: available
VPC: vpc-85e41dfc
Available IPs: 4091
Availability Zone: us-east-1b
Route table: rtb-5d01b025
Network ACL: acl-84d947fd
Default subnet: yes
Auto-assign Public IP: yes
Auto-assign IPv6 address: no

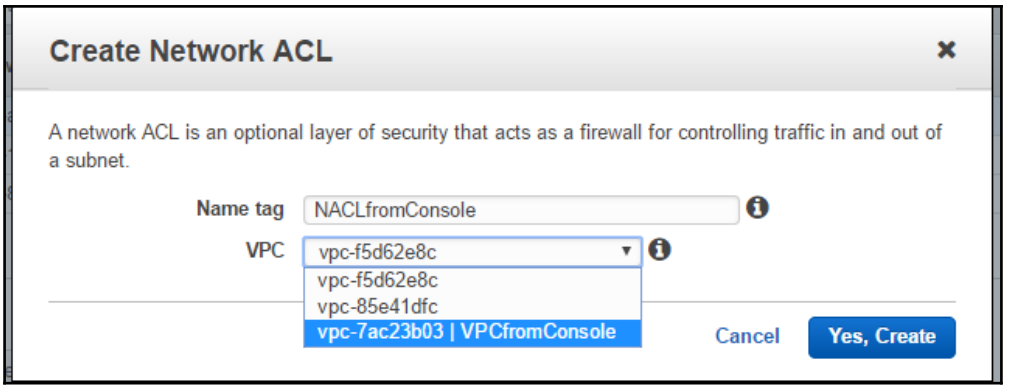

Create Subnet
Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.
Name tag
SubnetFromConsole
VPC
vpc-7ac23b03 | VPCfromConsole
VPC CIDRs
CIDR
Status
Status Reason
10.0.0.0/16
associated
Availability Zone
us-east-1a
IPv4 CIDR block
10.0.0.0/24
Cancel
Yes, Create

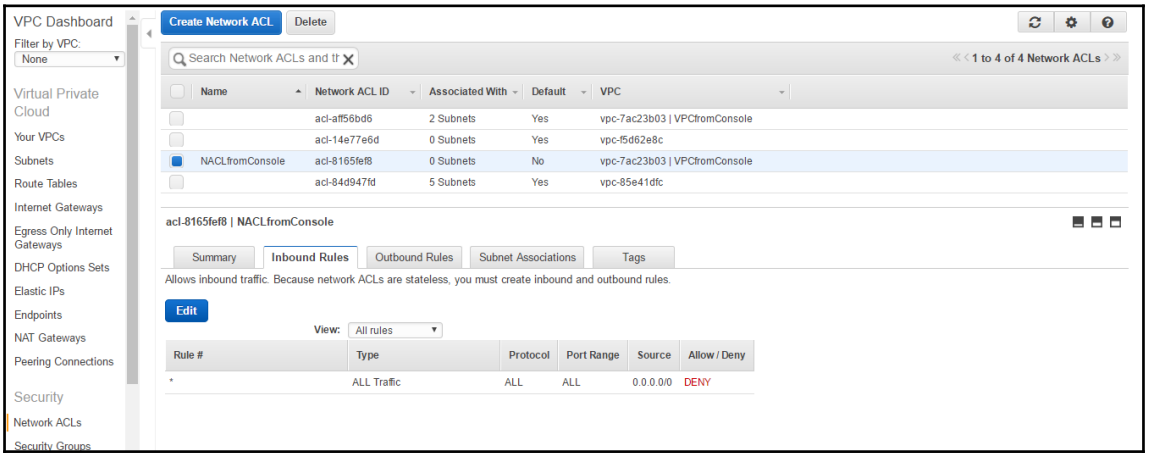

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 6 of 6 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4...
IPv6 CIDR
Availability Zone
Route Table
Network ACL
Default Subnet
subnet-bf32fc93 available vpc-85e41dfc 172.31.64.0/20 4091 us-east-1b rtb-5d01b025 acl-84d947fd Yes
subnet-4c7cb816 available vpc-85e41dfc 172.31.32.0/20 4091 us-east-1d rtb-5d01b025 acl-84d947fd Yes
subnet-21ba0069 available vpc-85e41dfc 172.31.16.0/20 4091 us-east-1c rtb-5d01b025 acl-84d947fd Yes
SubnetFromConsole subnet-598abe3c available vpc-7ac23b03 | VPCfromConsole 10.0.0.0/24 251 us-east-1a rtb-bde959c5 acl-aff56bd6 No
subnet-18134e24 available vpc-85e41dfc 172.31.48.0/20 4091 us-east-1e rtb-5d01b025 acl-84d947fd Yes
subnet-598abe3c | SubnetFromConsole
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-598abe3c | SubnetFromConsole
IPv4 CIDR: 10.0.0.0/24
IPv6 CIDR:
State: available
VPC: vpc-7ac23b03 | VPCfromConsole
Available IPs: 251
Availability Zone: us-east-1a
Route table: rtb-bde959c5
Network ACL: acl-aff56bd6
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no

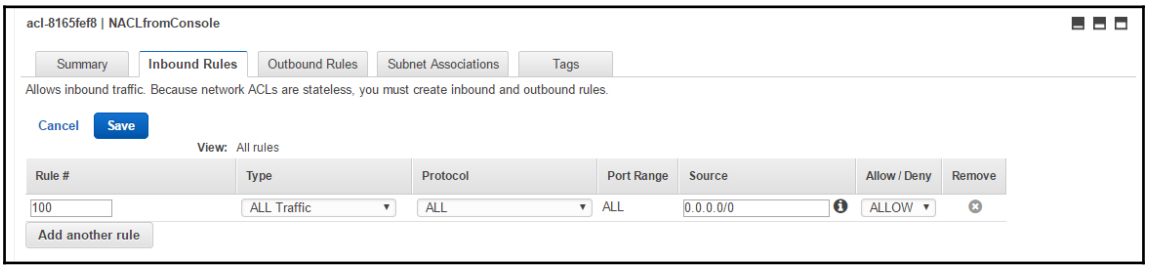

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create Subnet
Subnet Actions
subnet-598abe3c
1 to 1 of 1 Subnet
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
Route Table
SubnetFromConsole
subnet-598abe3c
available
vpc-7ac23b03 | VPCfromConsole
10.0.0.0/24
251
us-east-1a
rtb-bde959c5
subnet-598abe3c | SubnetFromConsole
Summary
Route Table
Network ACL
Flow Logs
Tags
Edit
Route Table: rtb-bde959c5
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-d7fb4bb1

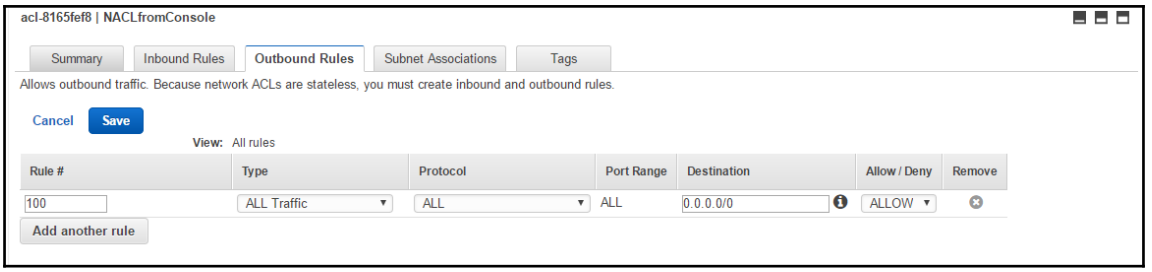

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Resources
Start VPC Wizard
Launch EC2 Instances
Note: Your Instances will launch in the US East (N. Virginia) region.
You are using the following Amazon VPC resources in the US East (N. Virginia) region:
3 VPCs
0 Egress-only Internet Gateways
3 Route Tables
0 Elastic IPs
0 Endpoints
3 Security Groups
0 VPN Connections
0 Customer Gateways
1 Internet Gateway
7 Subnets
3 Network ACLs
0 VPC Peering Connections
0 Nat Gateways
0 Running Instances
0 Virtual Private Gateways
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.
Create VPN Connection
Service Health
Current Status
Details
Amazon VPC - US East (N. Virginia)
Service is operating normally
Amazon EC2 - US East (N. Virginia)
Service is operating normally
View complete service health details
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue

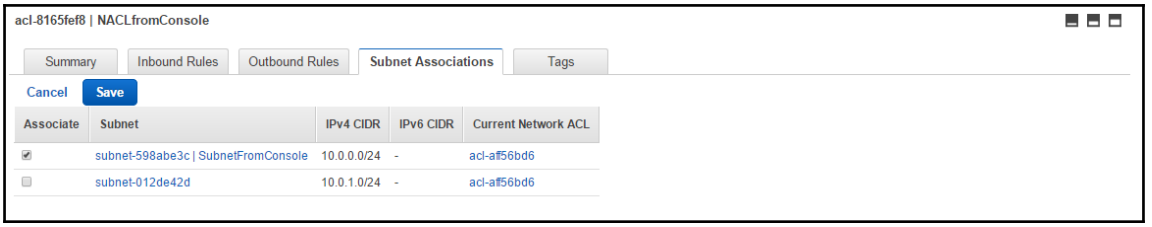

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Network ACL
Delete
Search Network ACLs and tf
1 to 3 of 3 Network ACLs
Name
Network ACL ID
Associated With
Default
VPC
acl-aff56bd6
2 Subnets
Yes
vpc-7ac23b03 | VPCfromConsole
acl-14e77e6d
0 Subnets
Yes
vpc-f5d62e8c
acl-84d947fd
5 Subnets
Yes
vpc-85e41dfc
acl-aff56bd6
Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags
Network ACL ID: acl-aff56bd6
Associated with: 2 Subnets
Default: yes
VPC: vpc-7ac23b03 | VPCfromConsole

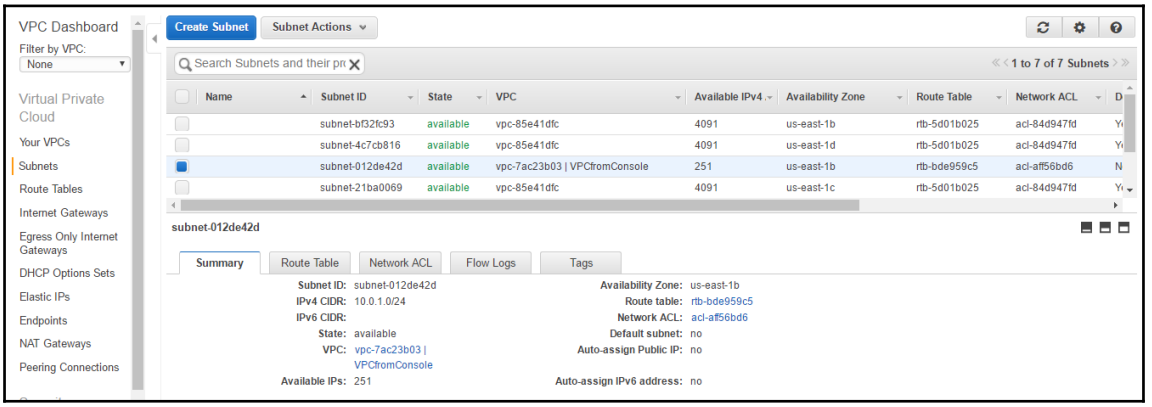

Create Network ACL
A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.
Name tag
NACLfromConsole
VPC
vpc-f5d62e8c
vpc-f5d62e8c
vpc-85e41dfc
vpc-7ac23b03 | VPCfromConsole
Cancel
Yes, Create

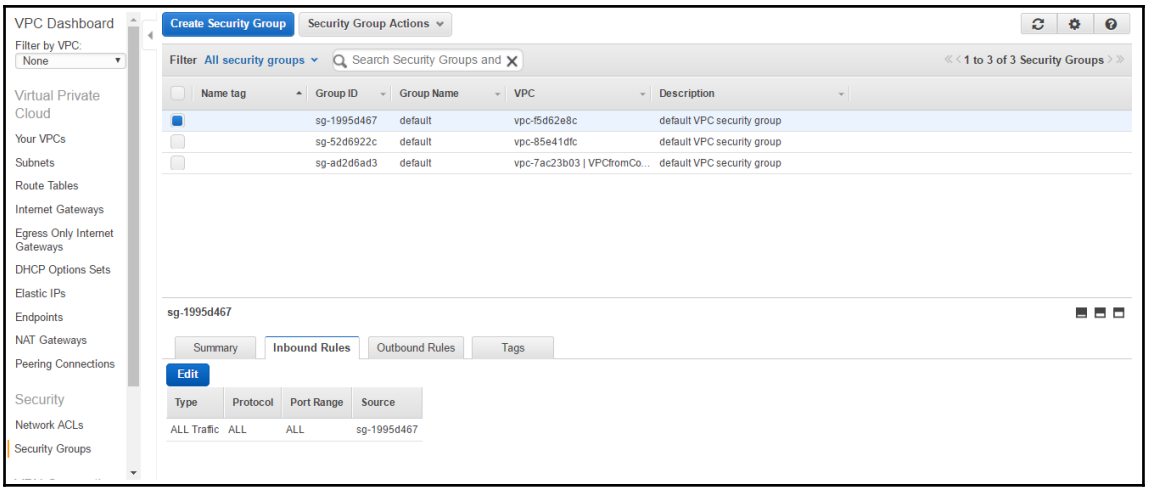

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Network ACL
Delete
Search Network ACLs and tr
1 to 4 of 4 Network ACLs
Name
Network ACL ID
Associated With
Default
VPC
acl-aff56bd6
2 Subnets
Yes
vpc-7ac23b03 | VPCfromConsole
acl-14e77e6d
0 Subnets
Yes
vpc-f5d62e8c
NACLfromConsole
acl-8165fef8
0 Subnets
No
vpc-7ac23b03 | VPCfromConsole
acl-84d947fd
5 Subnets
Yes
vpc-85e41dfc
acl-8165fef8 | NACLfromConsole
Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.
Edit
View:
All rules
Rule #
Type
Protocol
Port Range
Source
Allow / Deny
*
ALL Traffic
ALL
ALL
0.0.0.0/0
DENY

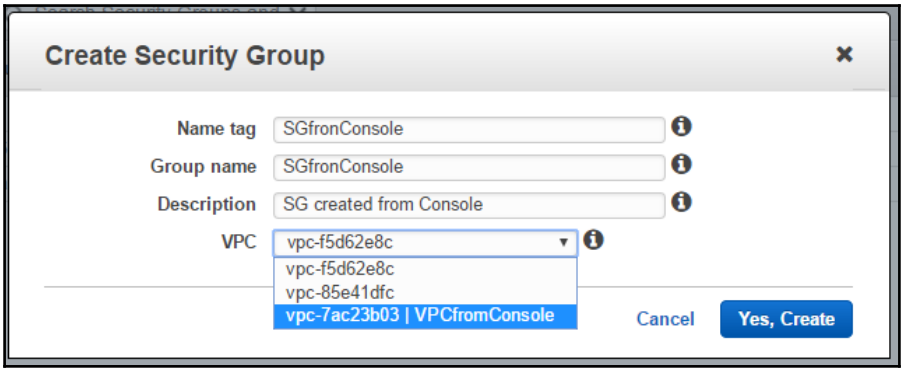

acl-8165fef8 | NACLfromConsole
Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags
Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.
Cancel
Save
View:
All rules
Rule #
Type
Protocol
Port Range
Source
Allow / Deny
Remove
100
ALL Traffic
ALL
ALL
0.0.0.0/0
ALLOW
Add another rule

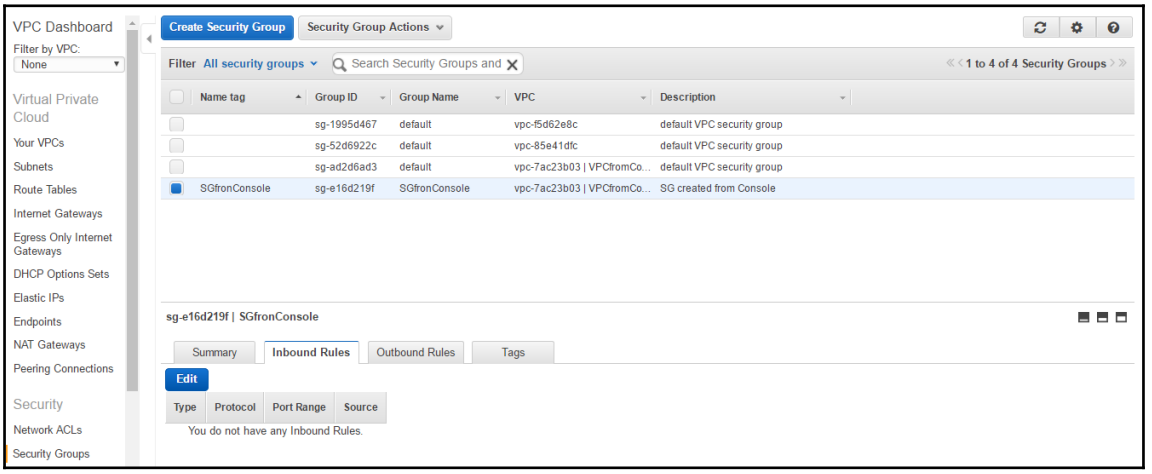

acl-8165fef8 | NACLfromConsole
Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags
Allows outbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.
Cancel
Save
View: All rules
Rule #
Type
Protocol
Port Range
Destination
Allow / Deny
Remove
100
ALL Traffic
ALL
ALL
0.0.0.0/0
ALLOW
Add another rule

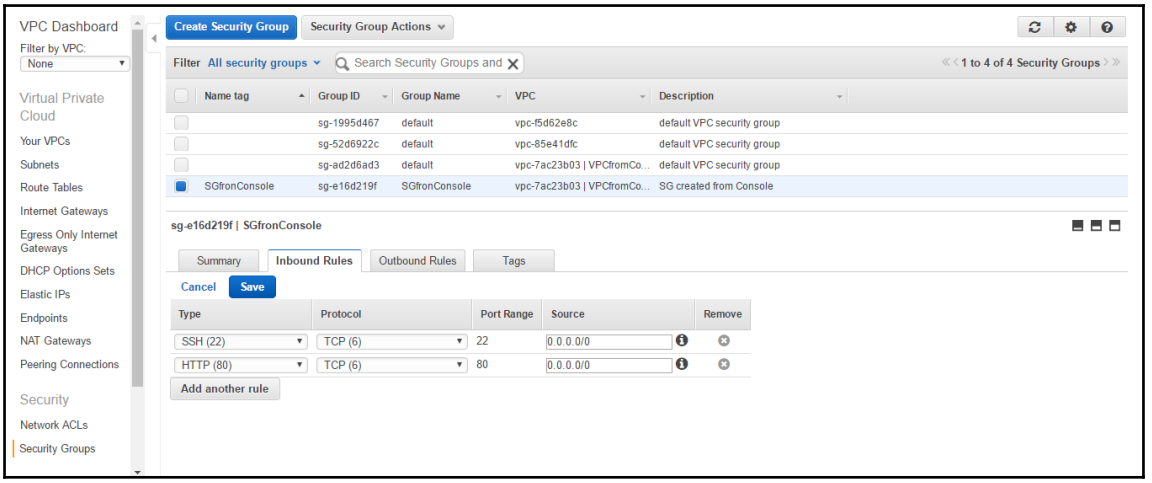

acl-8165fef8 | NACLfromConsole
Summary
Inbound Rules
Outbound Rules
Subnet Associations
Tags
Cancel
Save
Associate
Subnet
IPv4 CIDR
IPv6 CIDR
Current Network ACL
subnet-598abe3c | SubnetFromConsole
10.0.0.0/24
-
acl-aff56bd6
subnet-012de42d
10.0.1.0/24
-
acl-aff56bd6

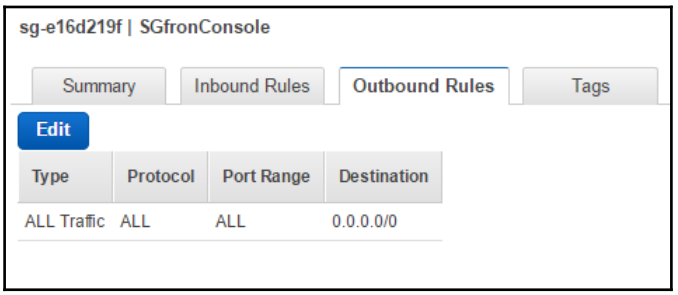

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Subnet
Subnet Actions
Search Subnets and their pr
1 to 7 of 7 Subnets
Name
Subnet ID
State
VPC
Available IPv4
Availability Zone
Route Table
Network ACL
subnet-bf32fc93 available vpc-85e41dfc 4091 us-east-1b rtb-5d01b025 acl-84d947fd
subnet-4c7cb816 available vpc-85e41dfc 4091 us-east-1d rtb-5d01b025 acl-84d947fd
subnet-012de42d available vpc-7ac23b03 | VPCfromConsole 251 us-east-1b rtb-bde959c5 acl-aff56bd6
subnet-21ba0069 available vpc-85e41dfc 4091 us-east-1c rtb-5d01b025 acl-84d947fd
subnet-012de42d
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-012de42d
IPv4 CIDR: 10.0.1.0/24
IPv6 CIDR:
State: available
VPC: vpc-7ac23b03 | VPCfromConsole
Available IPs: 251
Availability Zone: us-east-1b
Route table: rtb-bde959c5
Network ACL: acl-aff56bd6
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no

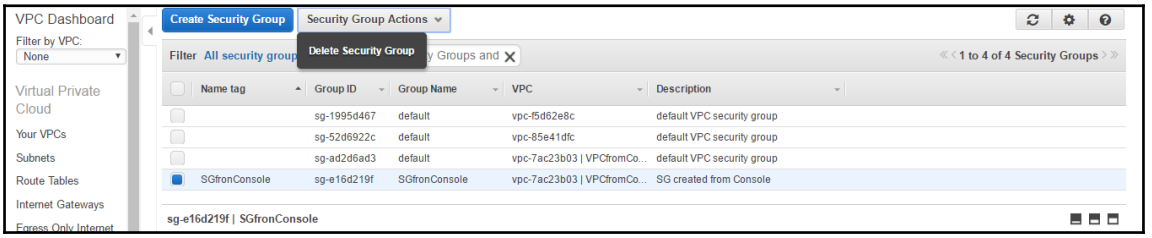

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Security Group
Security Group Actions
Filter All security groups
Search Security Groups and
1 to 3 of 3 Security Groups
Name tag
Group ID
Group Name
VPC
Description
sg-1995d467 default vpc-f5d62e8c default VPC security group
sg-52d6922c default vpc-85e41dfc default VPC security group
sg-ad2d6ad3 default vpc-7ac23b03 | VPCfromCo... default VPC security group
sg-1995d467
Summary
Inbound Rules
Outbound Rules
Tags
Edit
Type
Protocol
Port Range
Source
ALL Traffic ALL ALL sg-1995d467

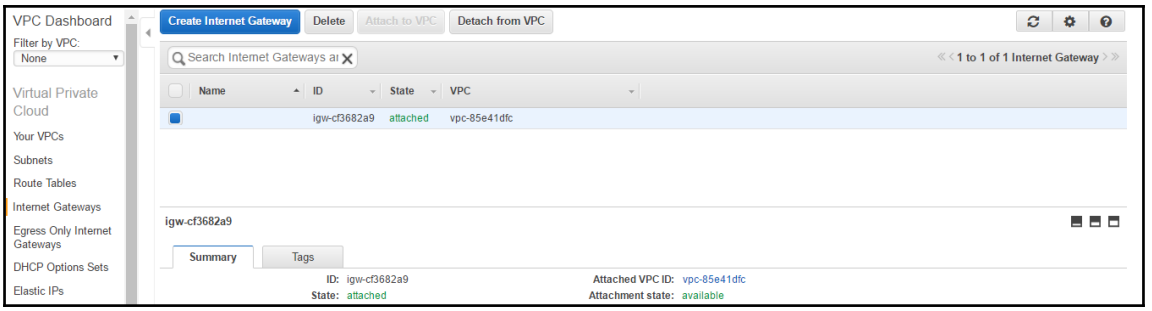

Create Security Group
Name tag
SGfronConsole
Group name
SGfronConsole
Description
SG created from Console
VPC
vpc-f5d62e8c
vpc-f5d62e8c
vpc-85e41dfc
vpc-7ac23b03 | VPCfromConsole
Cancel
Yes, Create

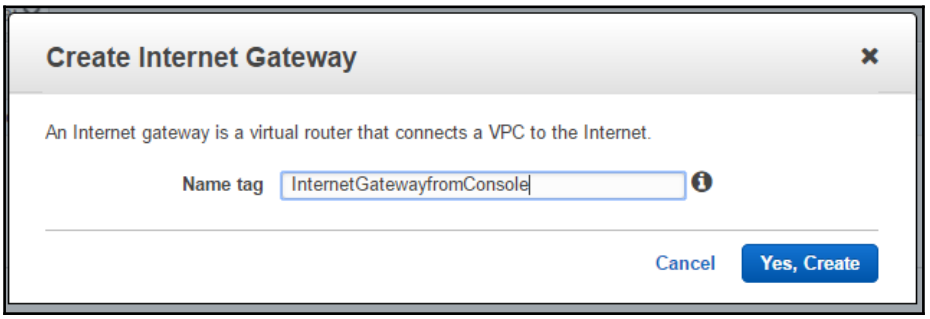

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Security Group
Security Group Actions
Filter All security groups
Search Security Groups and
1 to 4 of 4 Security Groups
Name tag
Group ID
Group Name
VPC
Description
sg-1995d467 default vpc-f5d62e8c default VPC security group
sg-52d6922c default vpc-85e41dfc default VPC security group
sg-ad2d6ad3 default vpc-7ac23b03 | VPCfromCo... default VPC security group
SGfronConsole sg-e16d219f SGfronConsole vpc-7ac23b03 | VPCfromCo... SG created from Console
sg-e16d219f | SGfronConsole
Summary
Inbound Rules
Outbound Rules
Tags
Edit
Type
Protocol
Port Range
Source
You do not have any Inbound Rules.

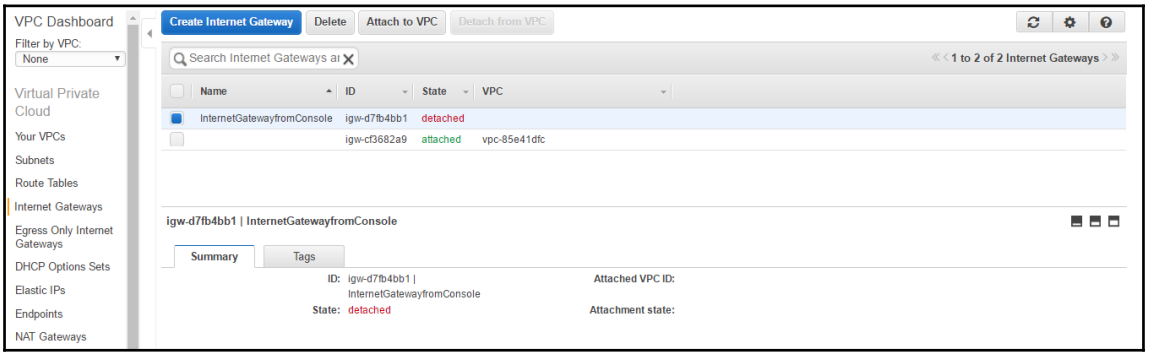

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Security Group
Security Group Actions
Filter All security groups
Search Security Groups and
1 to 4 of 4 Security Groups
Name tag
Group ID
Group Name
VPC
Description
sg-1995d467 default vpc-f5d62e8c default VPC security group
sg-52d6922c default vpc-85e41dfc default VPC security group
sg-ad2d6ad3 default vpc-7ac23b03 | VPCfromCo... default VPC security group
SGfronConsole sg-e16d219f SGfronConsole vpc-7ac23b03 | VPCfromCo... SG created from Console
sg-e16d219f | SGfronConsole
Summary
Inbound Rules
Outbound Rules
Tags
Cancel
Save
Type
Protocol
Port Range
Source
Remove
SSH (22) TCP (6) 22 0.0.0.0/0
HTTP (80) TCP (6) 80 0.0.0.0/0
Add another rule

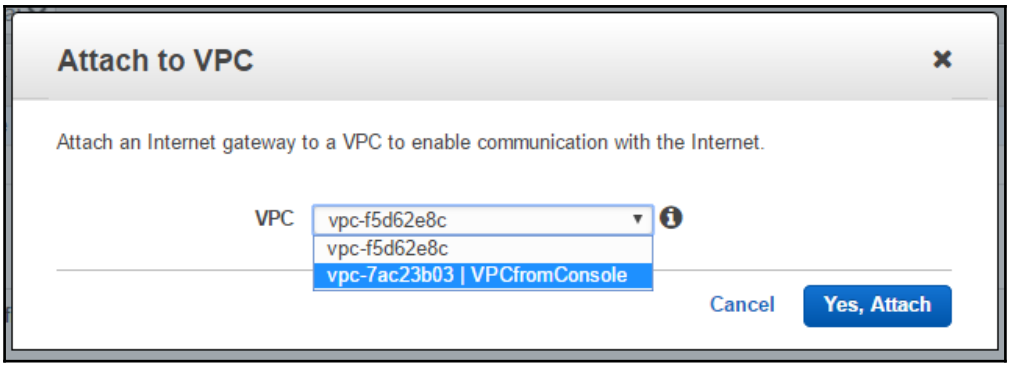

sg-e16d219f | SGfronConsole
Summary
Inbound Rules
Outbound Rules
Tags
Edit
Type
Protocol
Port Range
Destination
ALL Traffic ALL ALL 0.0.0.0/0

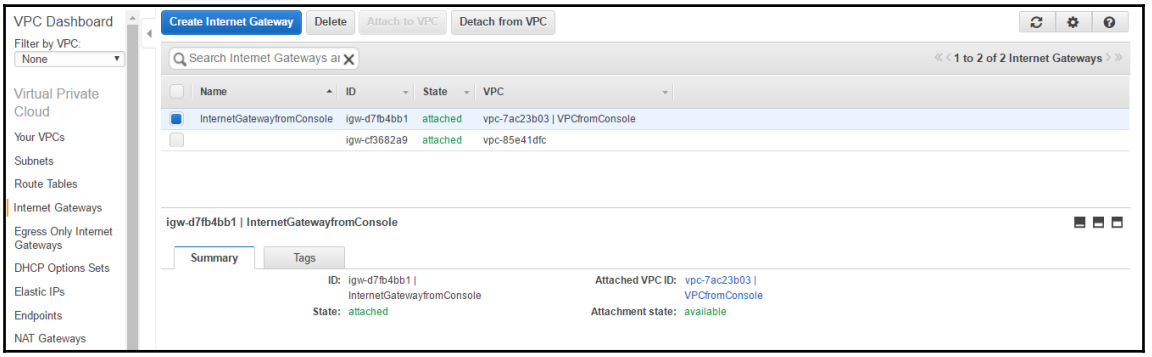

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Create Security Group
Security Group Actions
Delete Security Group
Filter All security group
Groups and
1 to 4 of 4 Security Groups
Name tag
Group ID
Group Name
VPC
Description
sg-1995d467 default vpc-f5d62e8c default VPC security group
sg-52d6922c default vpc-85e41dfc default VPC security group
sg-ad2d6ad3 default vpc-7ac23b03 | VPCfromCo... default VPC security group
SGfronConsole sg-e16d219f SGfronConsole vpc-7ac23b03 | VPCfromCo... SG created from Console
sg-e16d219f | SGfronConsole

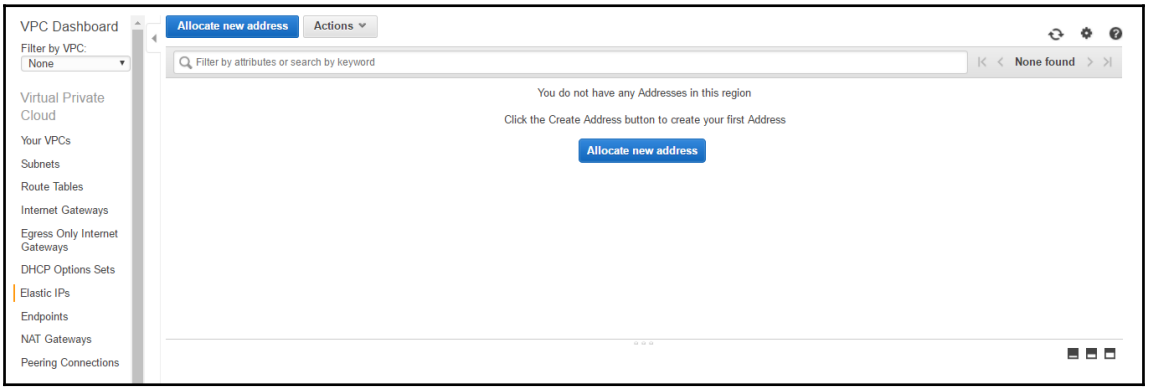

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create Internet Gateway
Delete
Attach to VPC
Detach from VPC
Search Internet Gateways a
1 to 1 of 1 Internet Gateway
Name
ID
State
VPC
igw-cf3682a9
attached
vpc-85e41dfc
igw-cf3682a9
Summary
Tags
ID: igw-cf3682a9
State: attached
Attached VPC ID: vpc-85e41dfc
Attachment state: available

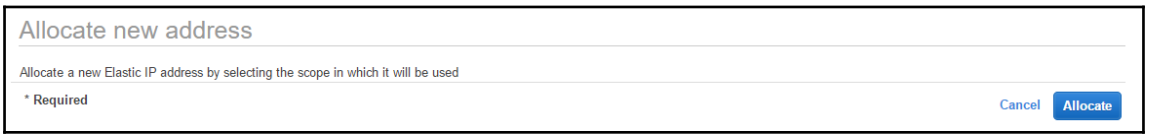

Create Internet Gateway
An Internet gateway is a virtual router that connects a VPC to the Internet.
Name tag
InternetGatewayfromConsole
Cancel
Yes, Create

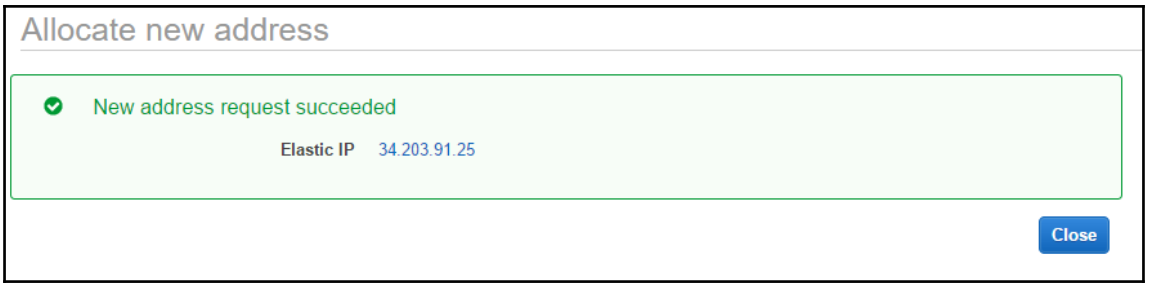

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create Internet Gateway
Delete
Attach to VPC
Detach from VPC
Search Internet Gateways a
1 to 2 of 2 Internet Gateways
Name
ID
State
VPC
InternetGatewayfromConsole
igw-d7fb4bb1
detached
igw-cf3682a9
attached
vpc-85e41dfc
igw-d7fb4bb1 | InternetGatewayfromConsole
Summary
Tags
ID: igw-d7fb4bb1 | InternetGatewayfromConsole
State: detached
Attached VPC ID:
Attachment state:

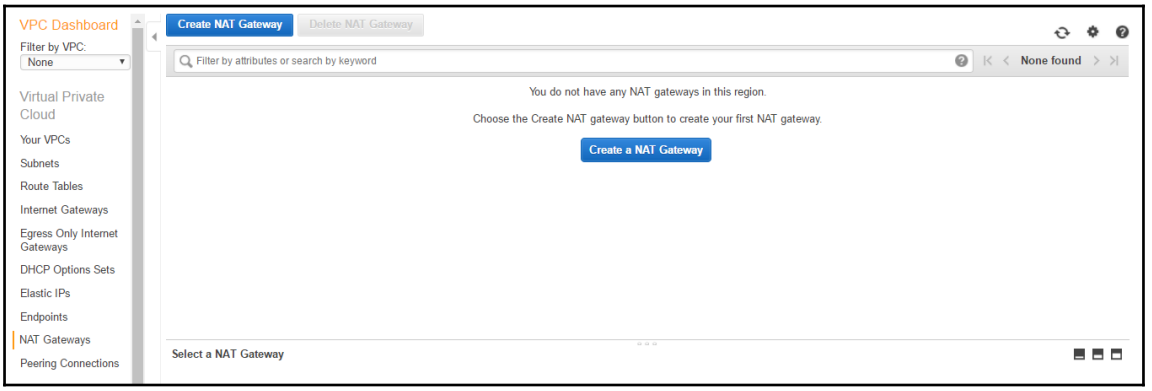

Attach to VPC
Attach an Internet gateway to a VPC to enable communication with the Internet.
VPC
vpc-f5d62e8c
vpc-f5d62e8c
vpc-7ac23b03 | VPCfromConsole
Cancel
Yes, Attach


VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create Internet Gateway
Delete
Attach to VPC
Detach from VPC
Search Internet Gateways a
1 to 2 of 2 Internet Gateways
Name
ID
State
VPC
InternetGatewayfromConsole
igw-d7fb4bb1
attached
vpc-7ac23b03 | VPCfromConsole
igw-cf3682a9
attached
vpc-85e41dfc
igw-d7fb4bb1 | InternetGatewayfromConsole
Summary
Tags
ID: igw-d7fb4bb1 | InternetGatewayfromConsole
State: attached
Attached VPC ID: vpc-7ac23b03 | VPCfromConsole
Attachment state: available

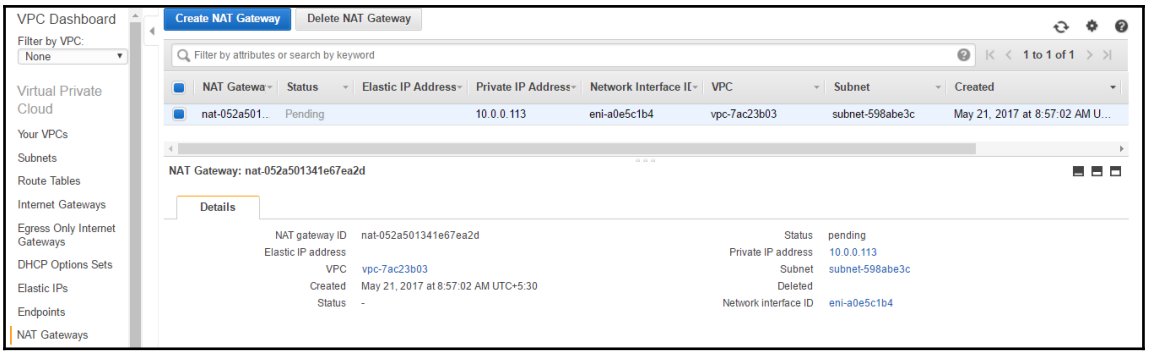

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Allocate new address
Actions
Filter by attributes or search by keyword
None found
You do not have any Addresses in this region
Click the Create Address button to create your first Address
Allocate new address

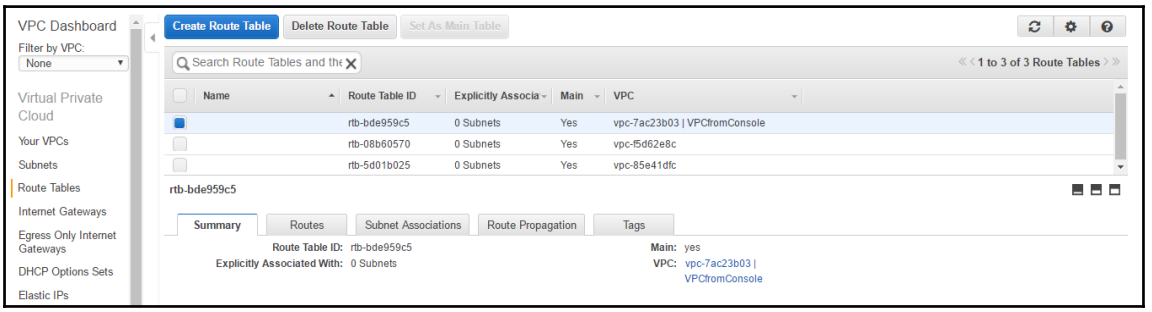

Allocate new address
Allocate a new Elastic IP address by selecting the scope in which it will be used
* Required
Cancel
Allocate

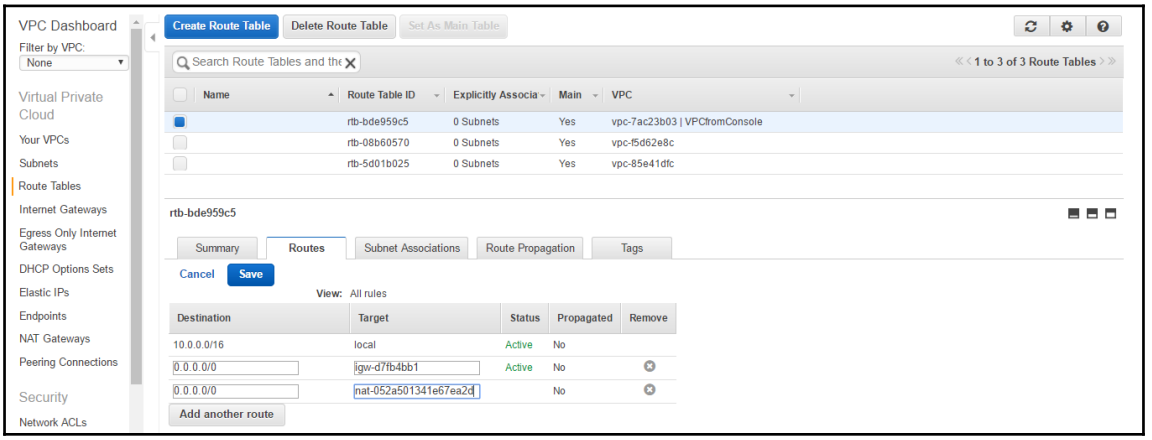

Allocate new address
New address request succeeded
Elastic IP
34.203.91.25
Close

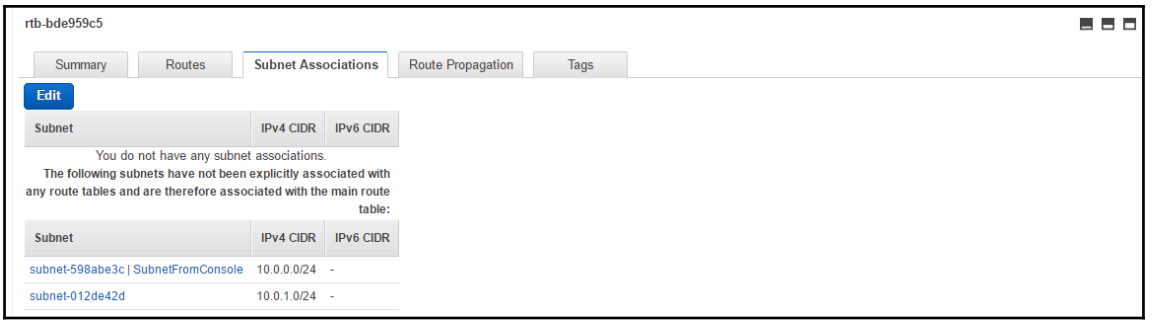

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create NAT Gateway
Delete NAT Gateway
Filter by attributes or search by keyword
None found
You do not have any NAT gateways in this region.
Choose the Create NAT gateway button to create your first NAT gateway.
Create a NAT Gateway
Select a NAT Gateway

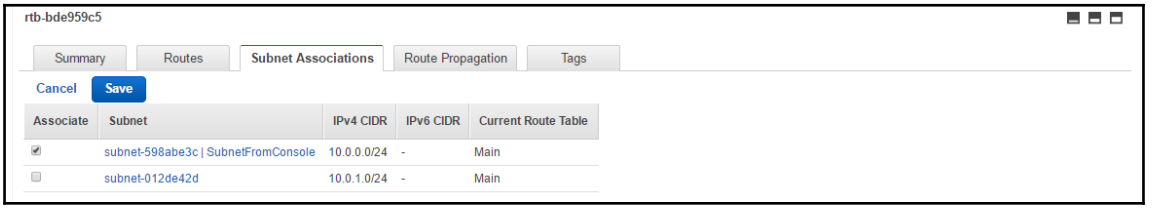
Create a NAT Gateway
Create a NAT gateway and assign it an Elastic IP address.
Learn more
Subnet*
subnet-598abe3c
Elastic IP Allocation ID*
eipalloc-f14b50c0
Create New EIP
Cancel
Create a NAT Gateway

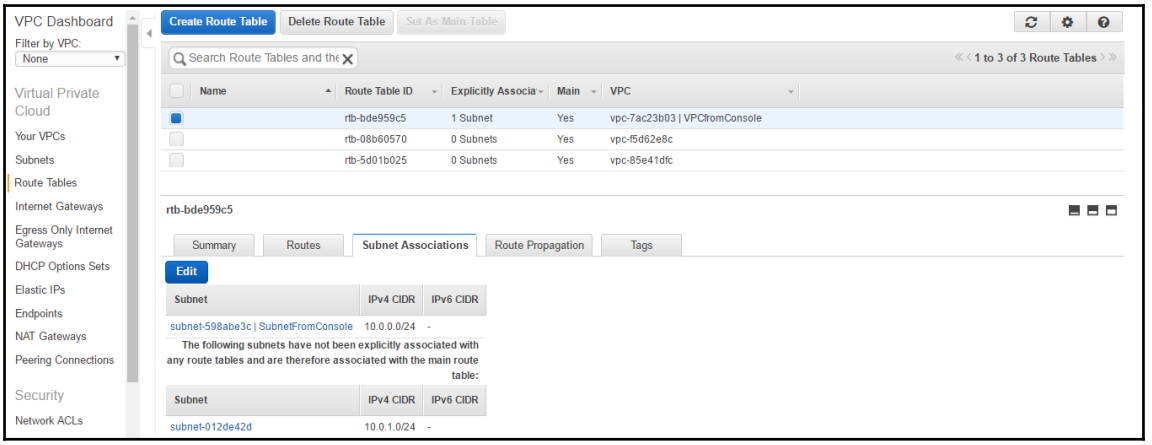

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create NAT Gateway
Delete NAT Gateway
Filter by attributes or search by keyword
1 to 1 of 1
NAT Gatewa
Status
Elastic IP Address
Private IP Address
Network Interface ID
VPC
Subnet
Created
nat-052a501..
Pending
10.0.0.113
eni-a0e5c1b4
vpc-7ac23b03
subnet-598abe3c
May 21, 2017 at 8:57:02 AM U...
NAT Gateway: nat-052a501341e67ea2d
Details
NAT gateway ID
nat-052a501341e67ea2d
Elastic IP address
VPC
vpc-7ac23b03
Created
May 21, 2017 at 8:57:02 AM UTC+5:30
Status
-
Status
pending
Private IP address
10.0.0.113
Subnet
subnet-598abe3c
Deleted
Network interface ID
eni-a0e5c1b4

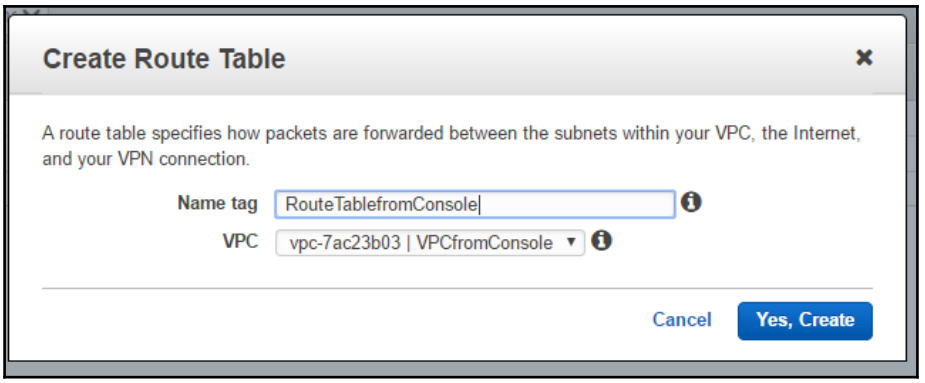

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and the
1 to 3 of 3 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-bde959c5
0 Subnets
Yes
vpc-7ac23b03 | VPCfromConsole
rtb-08b60570
0 Subnets
Yes
vpc-f5d62e8c
rtb-5d01b025
0 Subnets
Yes
vpc-85e41dfc
rtb-bde959c5
Summary
Routes
Subnet Associations
Route Propagation
Tags
Route Table ID: rtb-bde959c5
Explicitly Associated With: 0 Subnets
Main: yes
VPC: vpc-7ac23b03 | VPCfromConsole

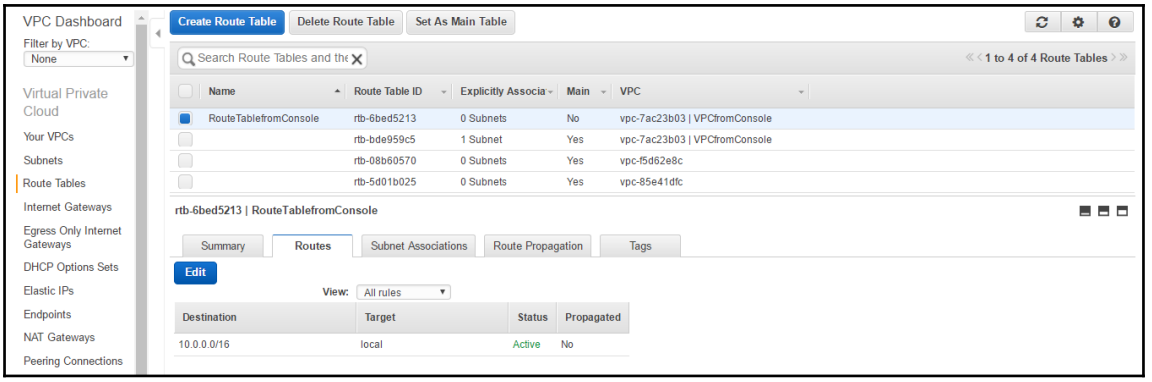

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and the
1 to 3 of 3 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-bde959c5
0 Subnets
Yes
vpc-7ac23b03 | VPCfromConsole
rtb-08b60570
0 Subnets
Yes
vpc-f5d62e8c
rtb-5d01b025
0 Subnets
Yes
vpc-85e41dfc
rtb-bde959c5
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
10.0.0.0/16
local
Active
No
0.0.0.0/0
igw-d7fb4bb1
Active
No
0.0.0.0/0
nat-052a501341e67ea2d
No
Add another route

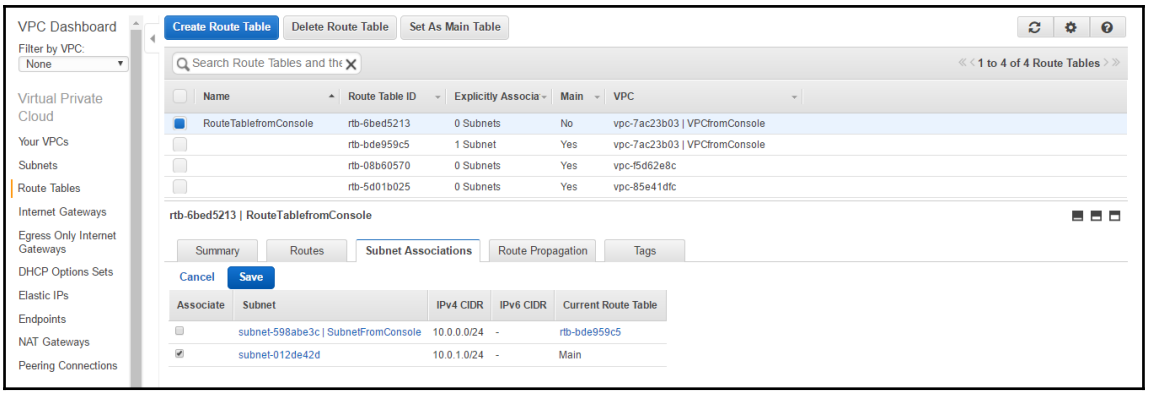

rtb-bde959c5
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
Subnet
IPv4 CIDR
IPv6 CIDR
You do not have any subnet associations.
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Subnet
IPv4 CIDR
IPv6 CIDR
subnet-598abe3c | SubnetFromConsole
10.0.0.0/24
-
subnet-012de42d
10.0.1.0/24
-

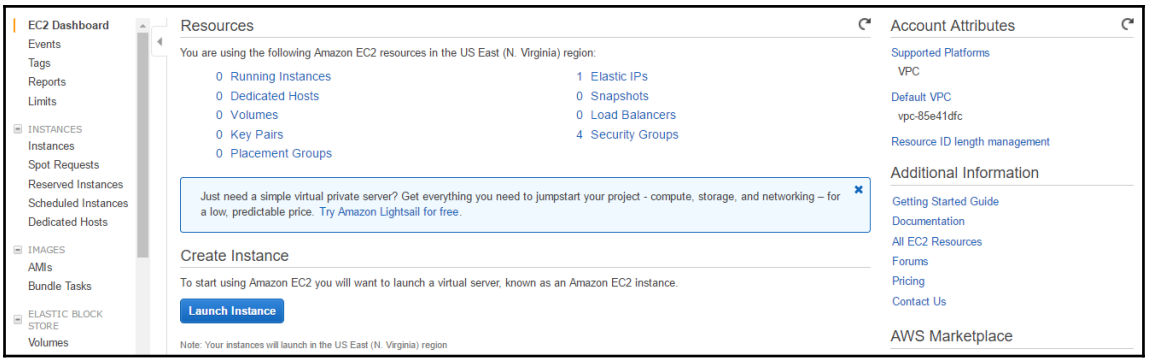

rtb-bde959c5
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
Associate
Subnet
IPv4 CIDR
IPv6 CIDR
Current Route Table
subnet-598abe3c | SubnetFromConsole
10.0.0.0/24
-
Main
subnet-012de42d
10.0.1.0/24
-
Main

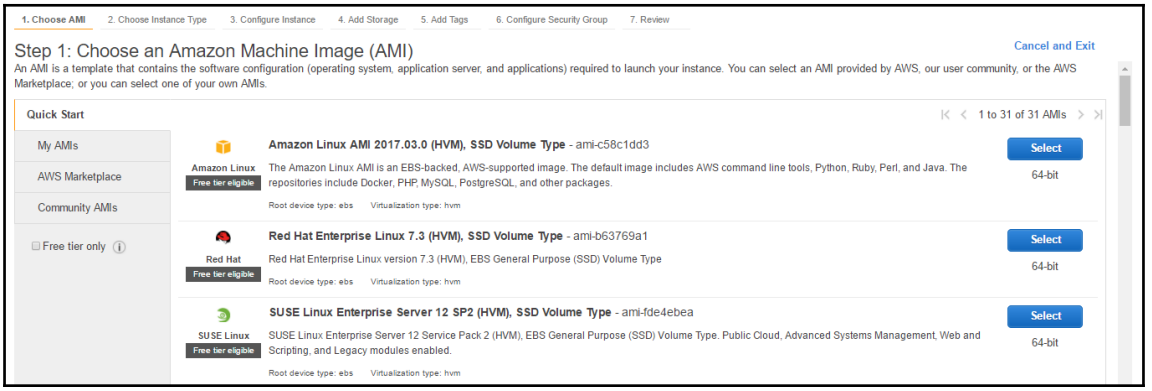

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and the
1 to 3 of 3 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-bde959c5
1 Subnet
Yes
vpc-7ac23b03 | VPCfromConsole
rtb-08b60570
0 Subnets
Yes
vpc-f5d62e8c
rtb-5d01b025
0 Subnets
Yes
vpc-85e41dfc
rtb-bde959c5
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
Subnet
IPv4 CIDR
IPv6 CIDR
subnet-598abe3c | SubnetFromConsole
10.0.0.0/24
-
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Subnet
IPv4 CIDR
IPv6 CIDR
subnet-012de42d
10.0.1.0/24
-

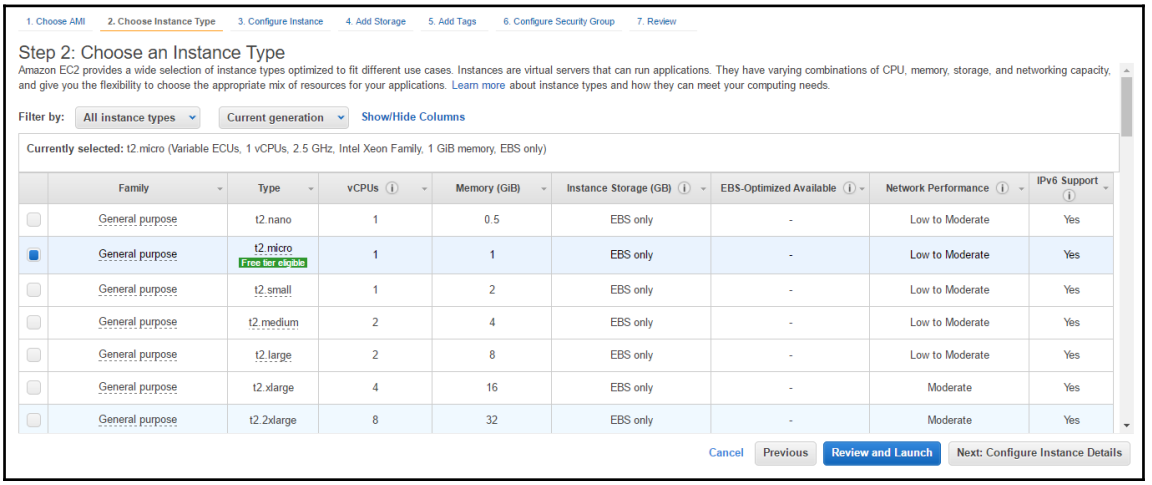

Create Route Table
A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.
Name tag
RouteTablefromConsole
VPC
vpc-7ac23b03 | VPCfromConsole
Cancel
Yes, Create

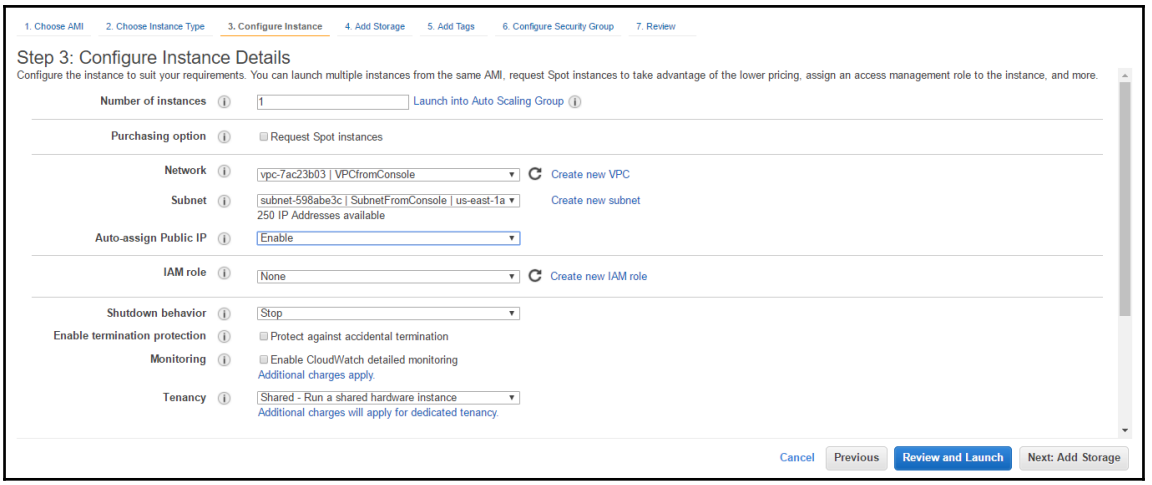

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and the
1 to 4 of 4 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
RouteTablefromConsole
rtb-6bed5213
0 Subnets
No
vpc-7ac23b03 | VPCfromConsole
rtb-bde959c5
1 Subnet
Yes
vpc-7ac23b03 | VPCfromConsole
rtb-08b60570
0 Subnets
Yes
vpc-f5d62e8c
rtb-5d01b025
0 Subnets
Yes
vpc-85e41dfc
rtb-6bed5213 | RouteTablefromConsole
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
View:
All rules
Destination
Target
Status
Propagated
10.0.0.0/16
local
Active
No

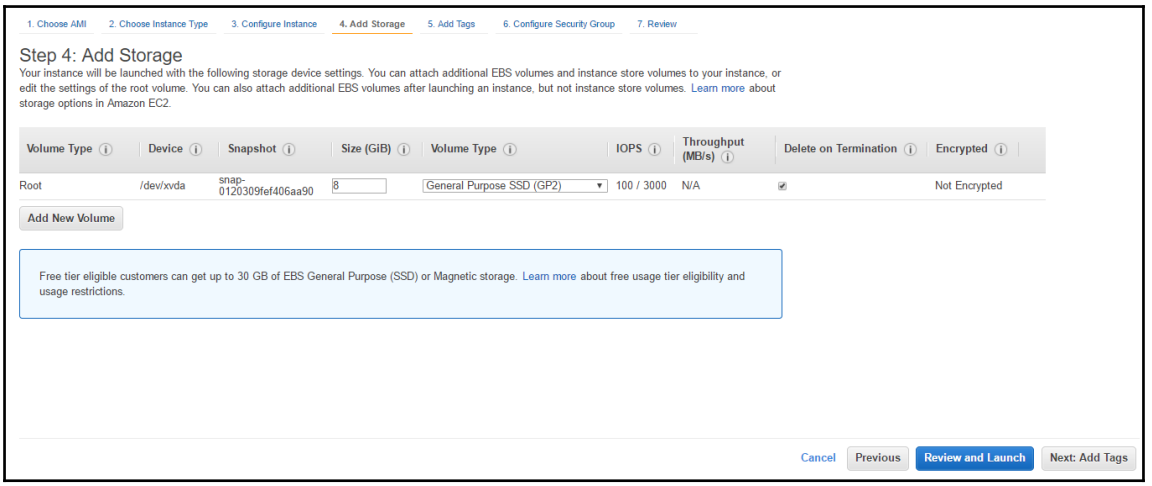

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and the
1 to 4 of 4 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
RouteTablefromConsole
rtb-6bed5213
0 Subnets
No
vpc-7ac23b03 | VPCfromConsole
rtb-bde959c5
1 Subnet
Yes
vpc-7ac23b03 | VPCfromConsole
rtb-08b60570
0 Subnets
Yes
vpc-f5d62e8c
rtb-5d01b025
0 Subnets
Yes
vpc-85e41dfc
rtb-6bed5213 | RouteTablefromConsole
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
Associate
Subnet
IPv4 CIDR
IPv6 CIDR
Current Route Table
subnet-598abe3c | SubnetFromConsole
10.0.0.0/24
-
rtb-bde959c5
subnet-012de42d
10.0.1.0/24
-
Main

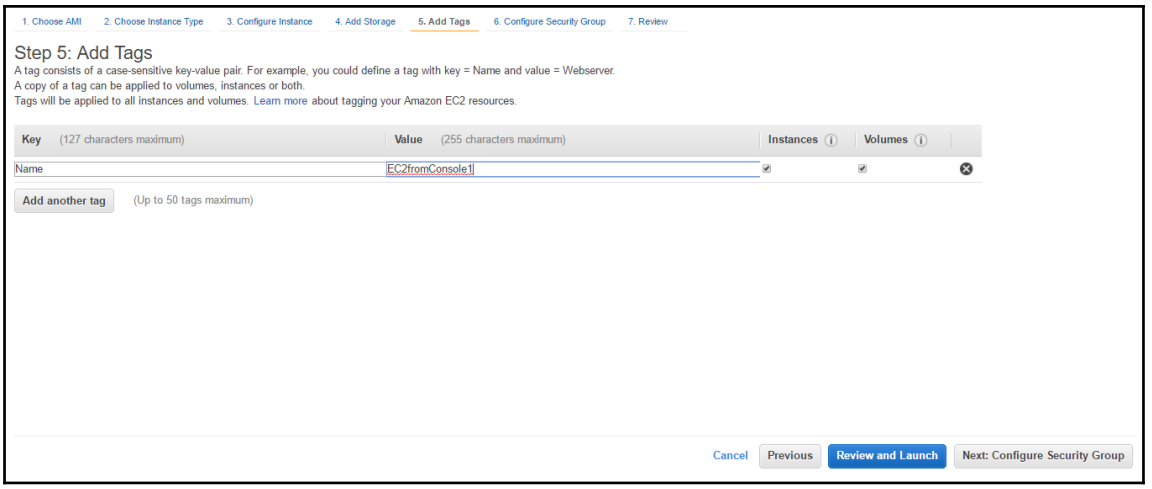

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Resources
You are using the following Amazon EC2 resources in the US East (N. Virginia) region:
0 Running Instances
0 Dedicated Hosts
0 Volumes
0 Key Pairs
0 Placement Groups
1 Elastic IPs
0 Snapshots
0 Load Balancers
4 Security Groups
Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.
Create Instance
To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.
Launch Instance
Note: Your instances will launch in the US East (N. Virginia) region
Account Attributes
Supported Platforms
VPC
Default VPC
vpc-85e41dfc
Resource ID length management
Additional Information
Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us
AWS Marketplace

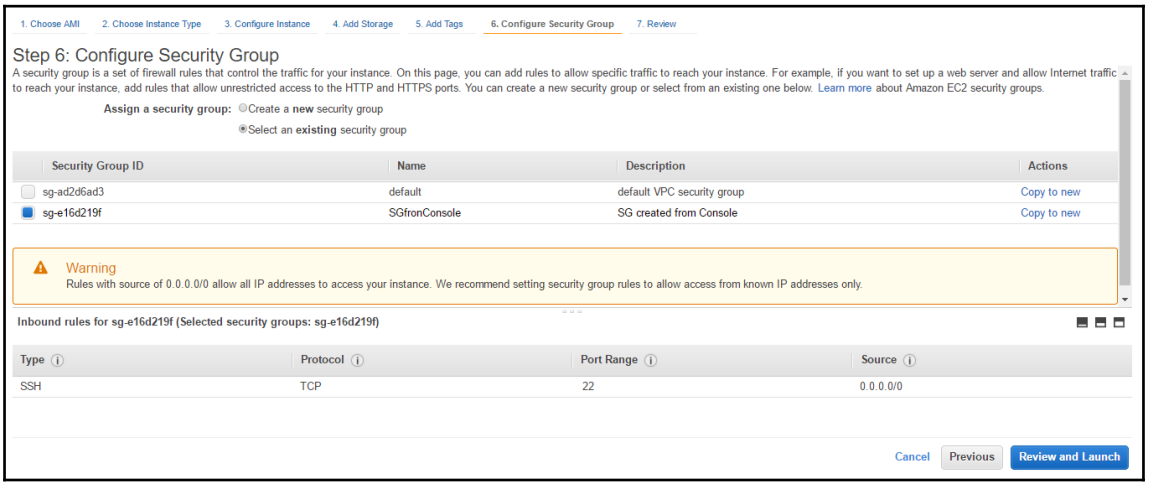

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Quick Start
1 to 31 of 31 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-c58c1dd3
Amazon Linux
Free tier eligible
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
Select
64-bit
Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-b63769a1
Red Hat
Free tier eligible
Red Hat Enterprise Linux version 7.3 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select
64-bit
SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-fde4ebea
SUSE Linux
Free tier eligible
SUSE Linux Enterprise Server 12 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
Select
64-bit

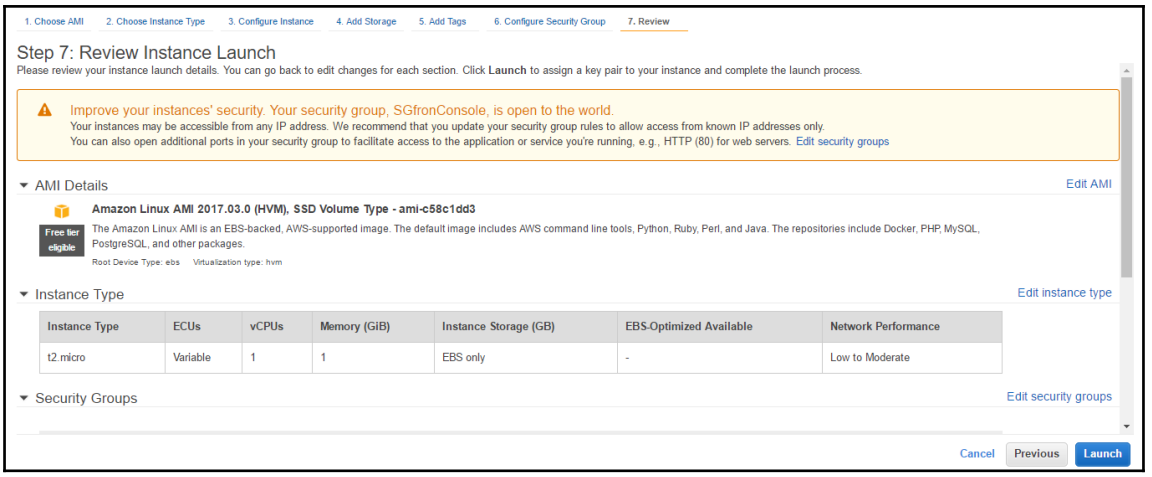

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by: All instance types Current generation Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family | Type | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance | IPv6 Support
General purpose | t2.nano | 1 | 0.5 | EBS only | - | Low to Moderate | Yes
General purpose | t2.micro Free tier eligible | 1 | 1 | EBS only | - | Low to Moderate | Yes
General purpose | t2.small | 1 | 2 | EBS only | - | Low to Moderate | Yes
General purpose | t2.medium | 2 | 4 | EBS only | - | Low to Moderate | Yes
General purpose | t2.large | 2 | 8 | EBS only | - | Low to Moderate | Yes
General purpose | t2.xlarge | 4 | 16 | EBS only | - | Moderate | Yes
General purpose | t2.2xlarge | 8 | 32 | EBS only | - | Moderate | Yes
Cancel
Previous
Review and Launch
Next: Configure Instance Details

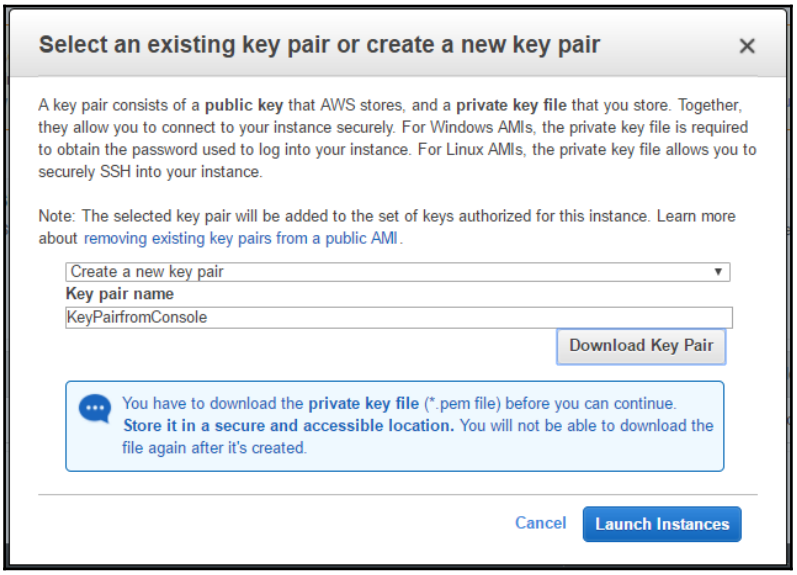

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-7ac23b03 | VPCfromConsole
Create new VPC
Subnet
subnet-598abe3c | SubnetFromConsole | us-east-1a
Create new subnet
250 IP Addresses available
Auto-assign Public IP
Enable
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Cancel
Previous
Review and Launch
Next: Add Storage

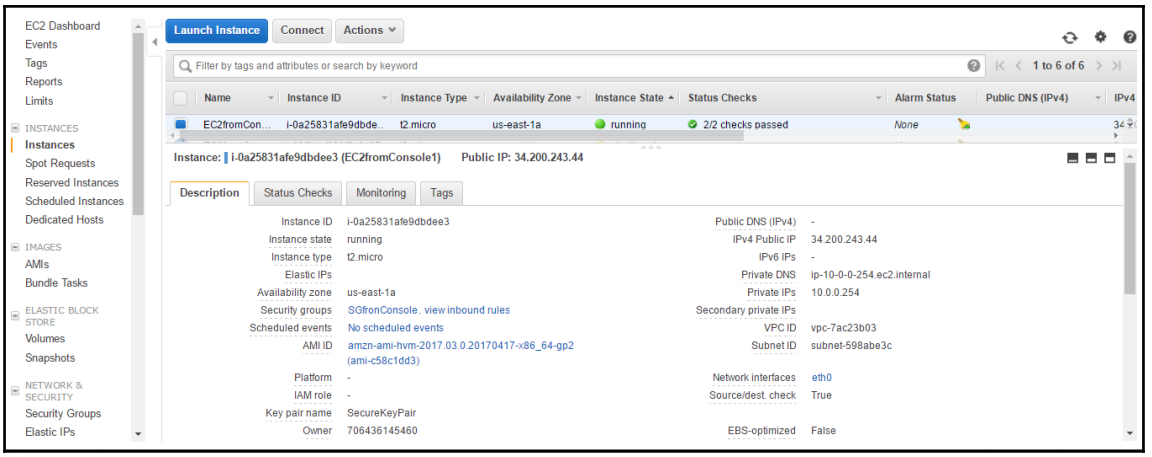

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.
Volume Type
Device
Snapshot
Size (GiB)
Volume Type
IOPS
Throughput (MB/s)
Delete on Termination
Encrypted
Root
/dev/xvda
snap-0120309fef406aa90
8
General Purpose SSD (GP2)
100 / 3000
N/A
Not Encrypted
Add New Volume
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.
Cancel
Previous
Review and Launch
Next: Add Tags

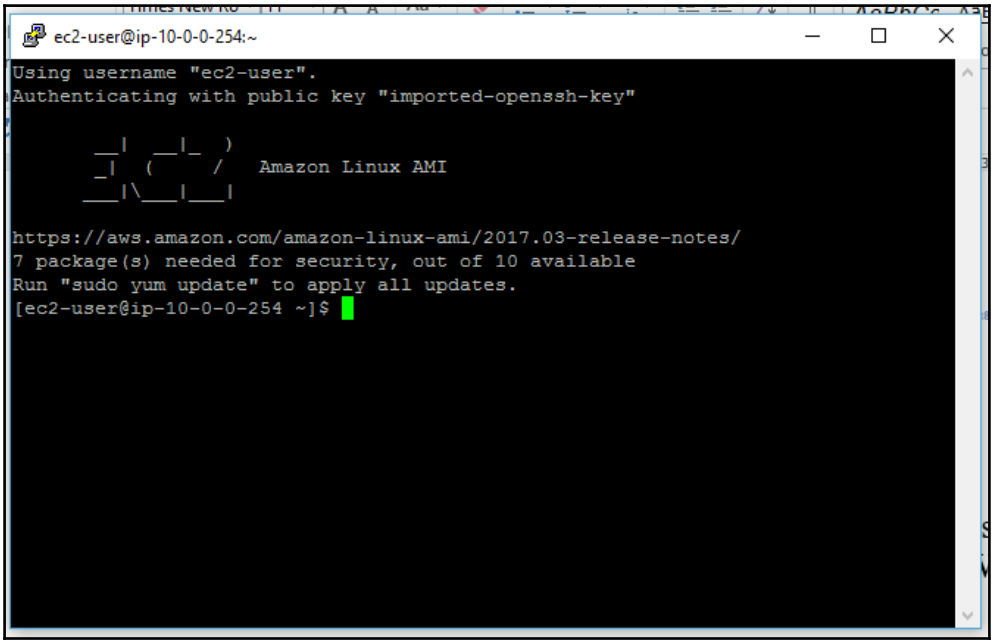

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.
Key (127 characters maximum)
Value (255 characters maximum)
Instances
Volumes
Name
EC2fromConsole1
Add another tag
(Up to 50 tags maximum)
Cancel
Previous
Review and Launch
Next: Configure Security Group


1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group: Create a new security group
Select an existing security group
Security Group ID
Name
Description
Actions
sg-ad2d6ad3
default
default VPC security group
Copy to new
sg-e16d219f
SGfronConsole
SG created from Console
Copy to new
Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.
Inbound rules for sg-e16d219f (Selected security groups: sg-e16d219f)
Type
Protocol
Port Range
Source
SSH
TCP
22
0.0.0.0/0
Cancel
Previous
Review and Launch

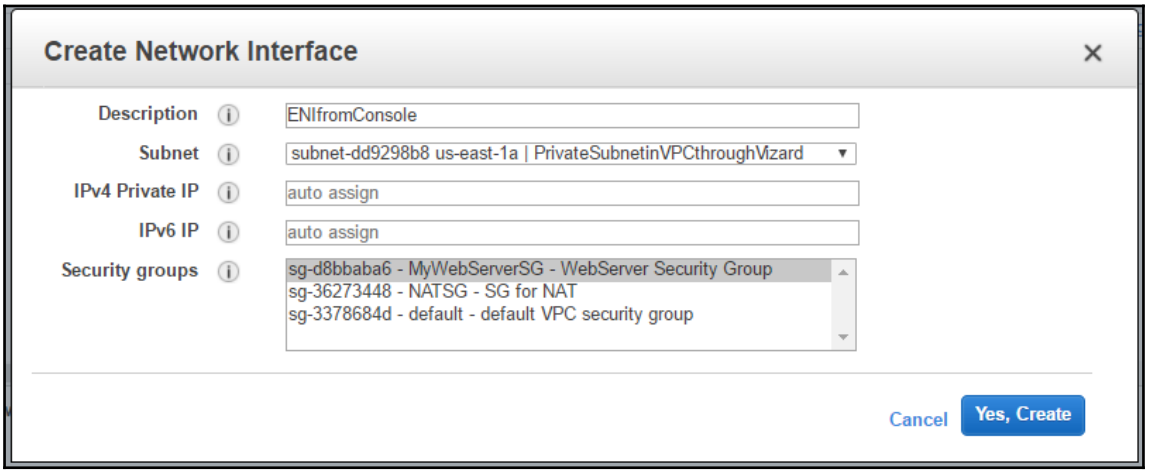

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, SGfronConsole, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
Amazon Linux AMI 2017.03.0 (HVM), SSD Volume Type - ami-c58c1dd3
Free tier eligible
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
t2.micro
Variable
1
1
EBS only
-
Low to Moderate
Security Groups
Edit security groups
Cancel
Previous
Launch

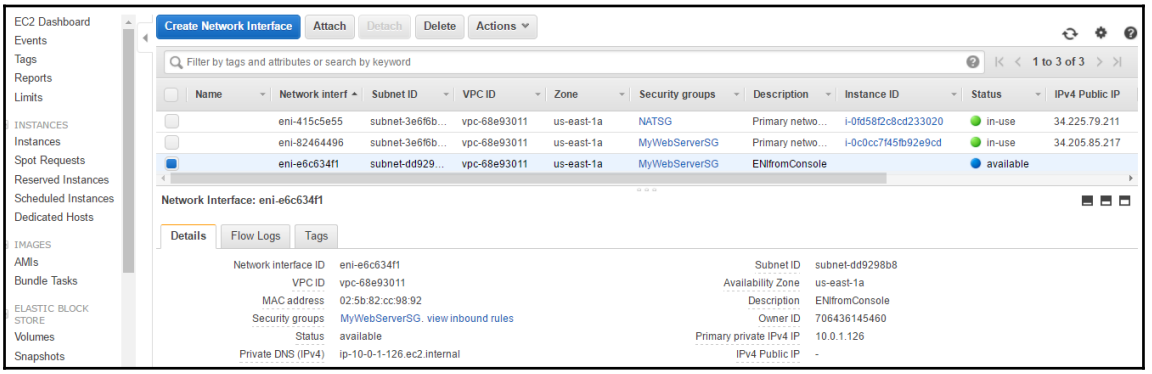

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Create a new key pair
Key pair name
KeyPairfromConsole
Download Key Pair
You have to download the private key file (*.pem file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.
Cancel
Launch Instances

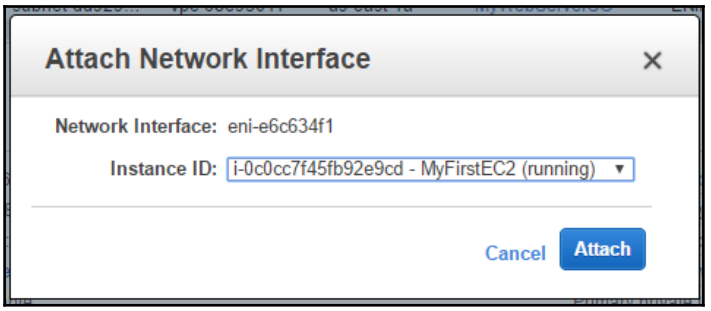

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 6 of 6
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4
EC2fromCon...
i-0a25831afe9dbde...
t2.micro
us-east-1a
running
2/2 checks passed
None
Instance: i-0a25831afe9dbdee3 (EC2fromConsole1)
Public IP: 34.200.243.44
Description
Status Checks
Monitoring
Tags
Instance ID
i-0a25831afe9dbdee3
Instance state
running
Instance type
t2.micro
Elastic IPs
Availability zone
us-east-1a
Security groups
SGfronConsole. view inbound rules
Scheduled events
No scheduled events
AMI ID
amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 (ami-c58c1dd3)
Platform
-
IAM role
-
Key pair name
SecureKeyPair
Owner
706436145460
Public DNS (IPv4)
-
IPv4 Public IP
34.200.243.44
IPv6 IPs
-
Private DNS
ip-10-0-0-254.ec2.internal
Private IPs
10.0.0.254
Secondary private IPs
VPC ID
vpc-7ac23b03
Subnet ID
subnet-598abe3c
Network interfaces
eth0
Source/dest. check
True
EBS-optimized
False

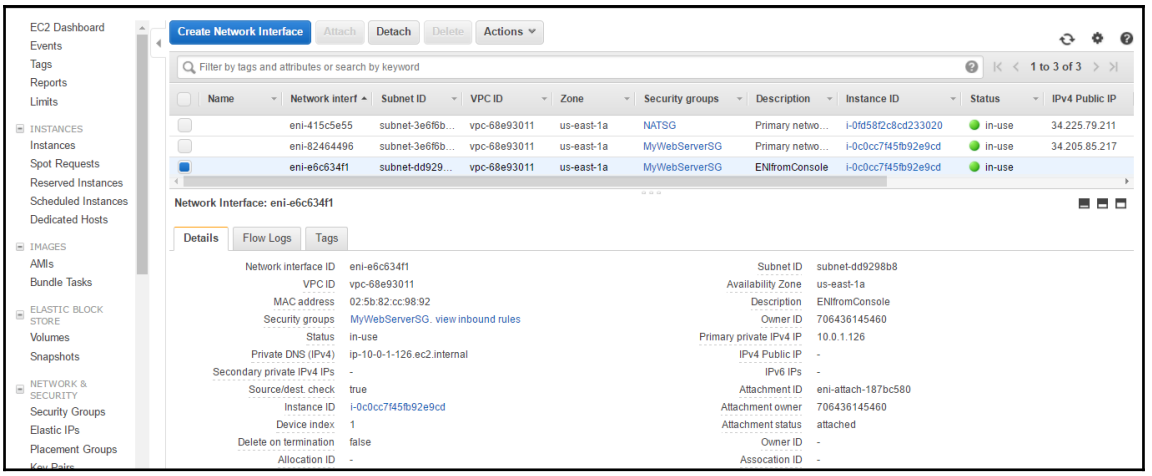

ec2-user@ip-10-0-0-254:~
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/ Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
7 package(s) needed for security, out of 10 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-254 ~]$

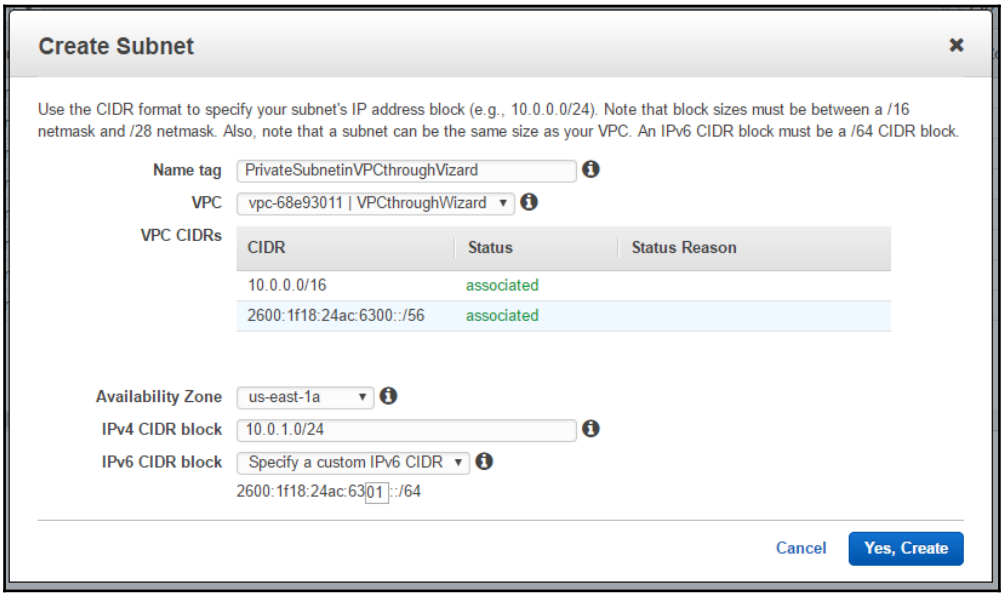
Chapter 3: VPC Advanced Components

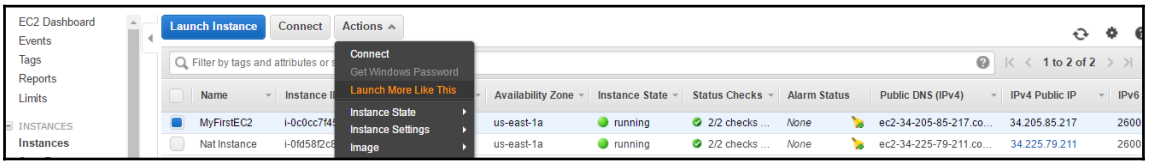


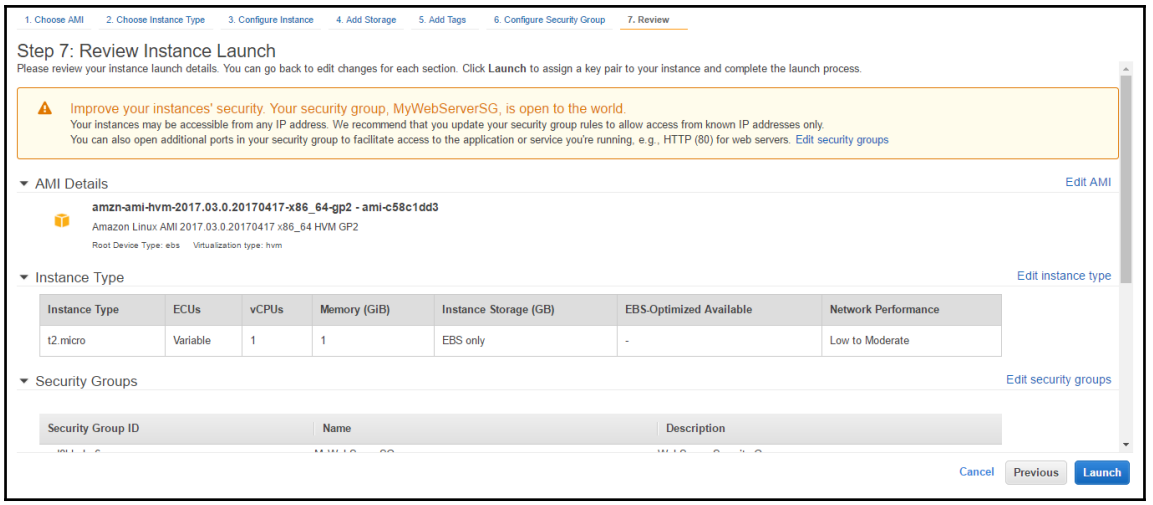


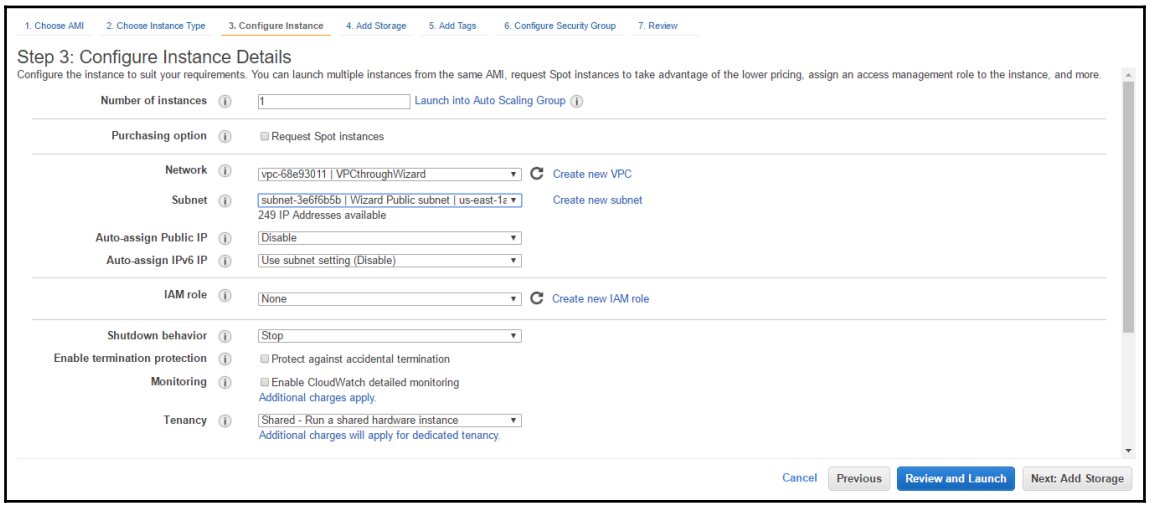


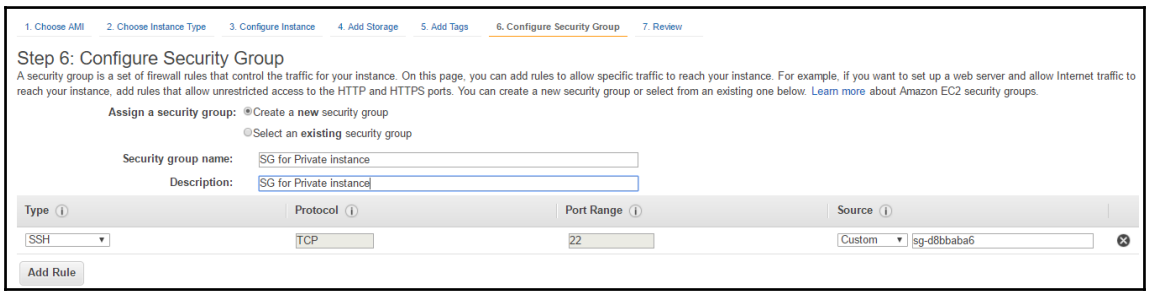

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Create Network Interface
Attach
Detach
Delete
Actions
Filter by tags and attributes or search by keyword
1 to 3 of 3
Name
Network interf
Subnet ID
VPC ID
Zone
Security groups
Description
Instance ID
Status
IPv4 Public IP
eni-415c5e55 subnet-3e6f6b... vpc-68e93011 us-east-1a NATSG Primary netwo... i-0fd58f2c8cd233020 in-use 34.225.79.211
eni-82464496 subnet-3e6f6b... vpc-68e93011 us-east-1a MyWebServerSG Primary netwo... i-0c0cc7f45fb92e9cd in-use 34.205.85.217
eni-e6c634f1 subnet-dd929... vpc-68e93011 us-east-1a MyWebServerSG ENIfromConsole i-0c0cc7f45fb92e9cd in-use
Network Interface: eni-e6c634f1
Details
Flow Logs
Tags
Network interface ID eni-e6c634f1
VPC ID vpc-68e93011
MAC address 02:5b:82:cc:98:92
Security groups MyWebServerSG. view inbound rules
Status in-use
Private DNS (IPv4) ip-10-0-1-126.ec2.internal
Secondary private IPv4 IPs -
Source/dest. check true
Instance ID i-0c0cc7f45fb92e9cd
Device index 1
Delete on termination false
Allocation ID -
Subnet ID subnet-dd9298b8
Availability Zone us-east-1a
Description ENIfromConsole
Owner ID 706436145460
Primary private IPv4 IP 10.0.1.126
IPv4 Public IP -
IPv6 IPs -
Attachment ID eni-attach-187bc580
Attachment owner 706436145460
Attachment status attached
Owner ID -
Assocation ID -

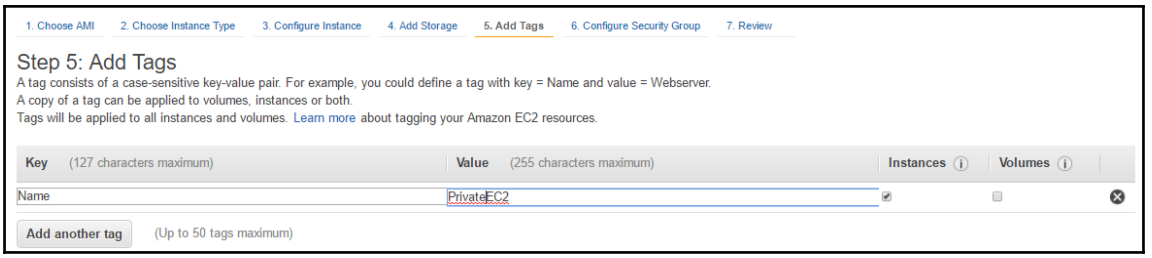

Create Subnet
Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.
Name tag PrivateSubnetinVPCthroughVizard
VPC vpc-68e93011 | VPCthroughWizard
VPC CIDRs
CIDR
Status
Status Reason
10.0.0.0/16 associated
2600:1f18:24ac:6300::/56 associated
Availability Zone us-east-1a
IPv4 CIDR block 10.0.1.0/24
IPv6 CIDR block Specify a custom IPv6 CIDR
2600:1f18:24ac:6301::/64
Cancel
Yes, Create

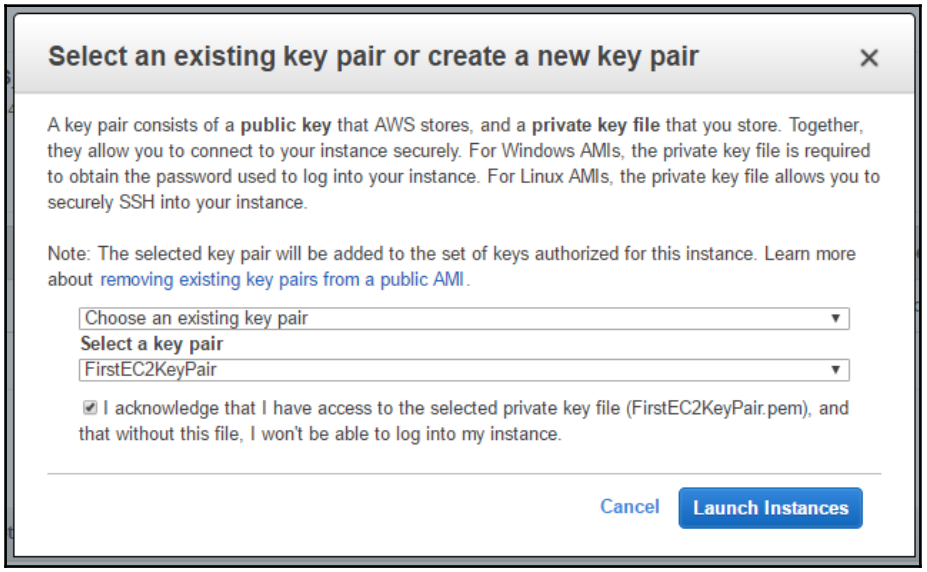

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Instance
Connect
Actions
Connect
Get Windows Password
Launch More Like This
Instance State
Instance Settings
Image
1 to 2 of 2
Name
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
MyFirstEC2 us-east-1a running 2/2 checks ... None ec2-34-205-85-217.co... 34.205.85.217
Nat Instance us-east-1a running 2/2 checks ... None ec2-34-225-79-211.co... 34.225.79.211

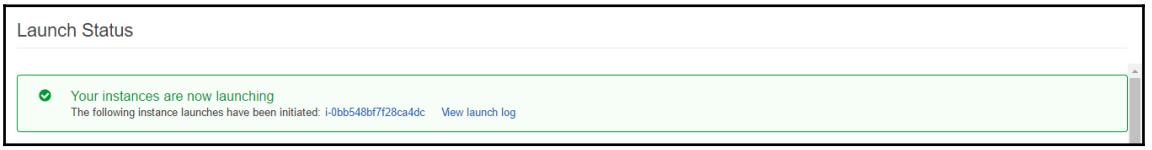

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 7: Review Instance Launch
Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.
Improve your instances' security. Your security group, MyWebServerSG, is open to the world.
Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
AMI Details
Edit AMI
amzn-ami-hvm-2017.03.0.20170417-x86_64-gp2 - ami-c58c1dd3
Amazon Linux AMI 2017.03.0.20170417 x86_64 HVM GP2
Root Device Type: ebs Virtualization type: hvm
Instance Type
Edit instance type
Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance
t2.micro | Variable | 1 | 1 | EBS only | - | Low to Moderate
Security Groups
Edit security groups
Security Group ID | Name | Description
Cancel
Previous
Launch

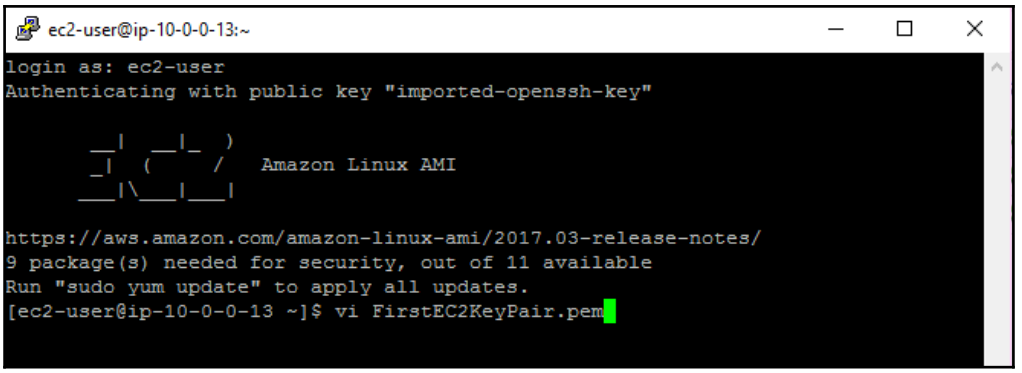

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-68e93011 | VPCthroughWizard
Create new VPC
Subnet
subnet-3e6f6b5b | Wizard Public subnet | us-east-1a
Create new subnet
249 IP Addresses available
Auto-assign Public IP
Disable
Auto-assign IPv6 IP
Use subnet setting (Disable)
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Cancel
Previous
Review and Launch
Next: Add Storage

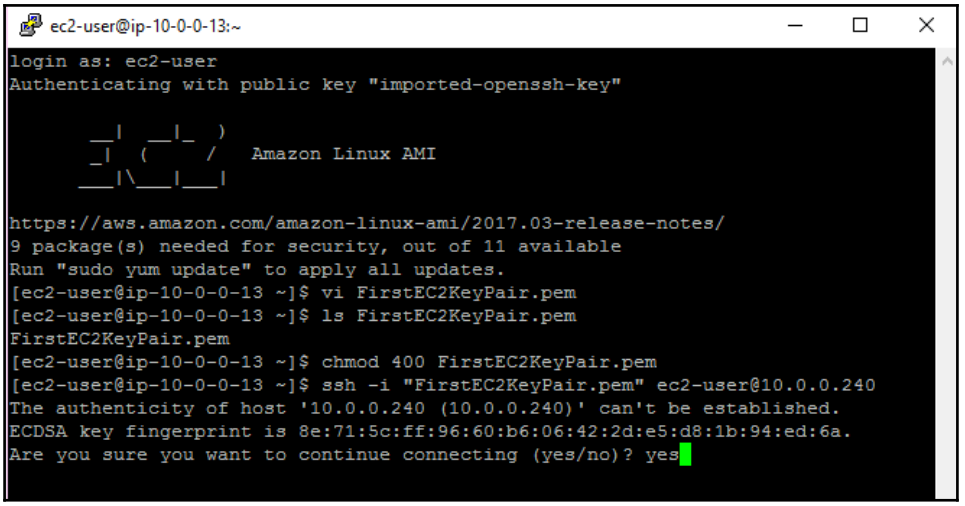

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
Security group name:
SG for Private instance
Description:
SG for Private instance
Type | Protocol | Port Range | Source
SSH | TCP | 22 | Custom | sg-d8bbaba6
Add Rule

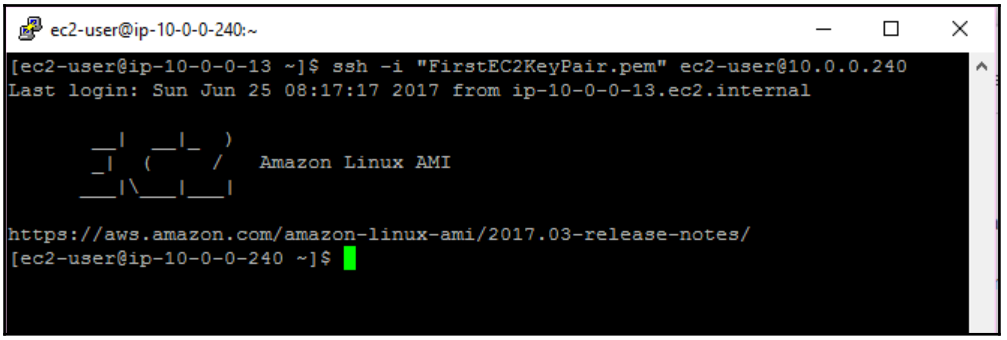

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.
Key (127 characters maximum)
Value (255 characters maximum)
Instances
Volumes
Name
PrivateEC2
Add another tag
(Up to 50 tags maximum)

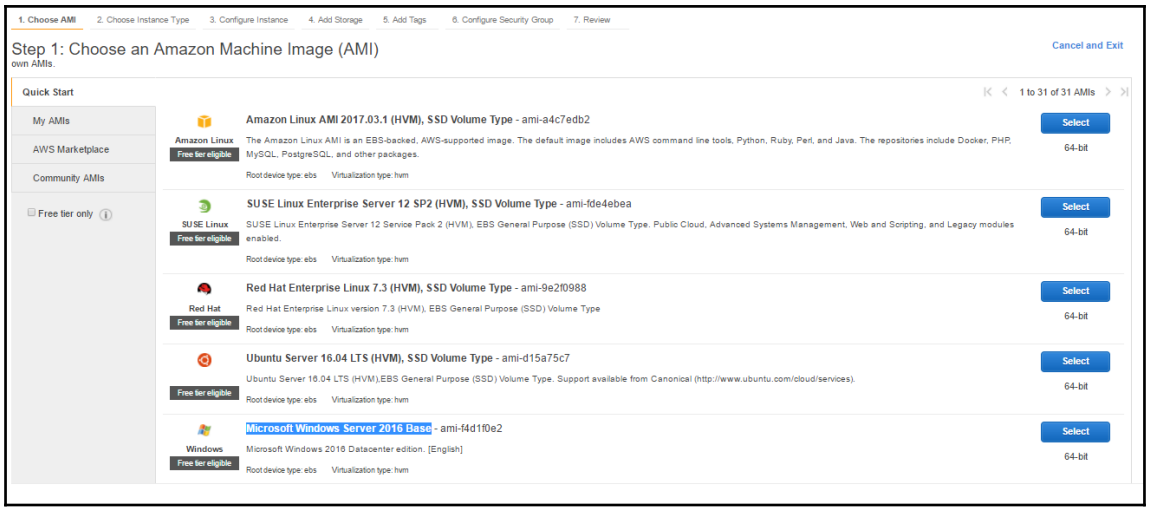

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
FirstEC2KeyPair
I acknowledge that I have access to the selected private key file (FirstEC2KeyPair.pem), and that without this file, I won't be able to log into my instance.
Cancel
Launch Instances

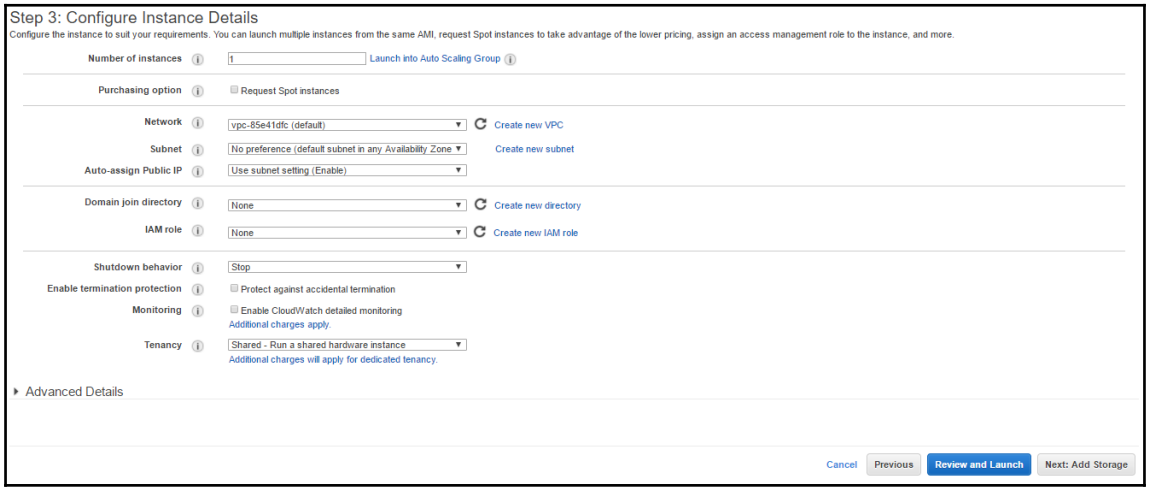

Launch Status
Your instances are now launching
The following instance launches have been initiated: i-0bb548bf7f28ca4dc
View launch log

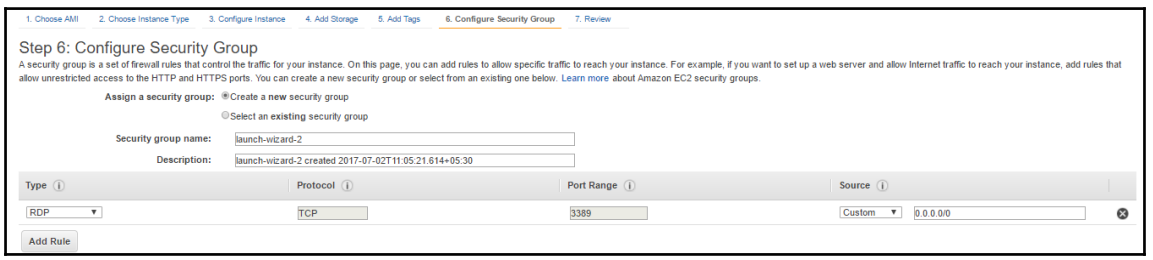

ec2-user@ip-10-0-0-13:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
9 package(s) needed for security, out of 11 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-13 ~]$ vi FirstEC2KeyPair.pem

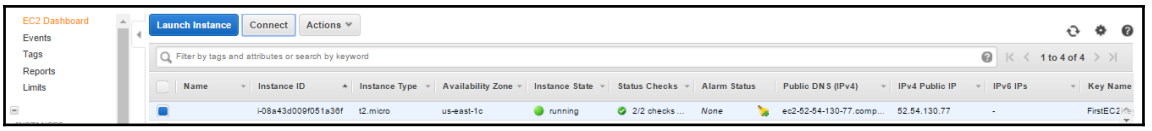

ec2-user@ip-10-0-0-13:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
9 package(s) needed for security, out of 11 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-0-13 ~]$ vi FirstEC2KeyPair.pem
[ec2-user@ip-10-0-0-13 ~]$ ls FirstEC2KeyPair.pem
FirstEC2KeyPair.pem
[ec2-user@ip-10-0-0-13 ~]$ chmod 400 FirstEC2KeyPair.pem
[ec2-user@ip-10-0-0-13 ~]$ ssh -i "FirstEC2KeyPair.pem" ec2-user@10.0.0.240
The authenticity of host '10.0.0.240 (10.0.0.240)' can't be established.
ECDSA key fingerprint is 8e:71:5c:ff:96:60:b6:06:42:2d:e5:d8:1b:94:ed:6a.
Are you sure you want to continue connecting (yes/no)? yes

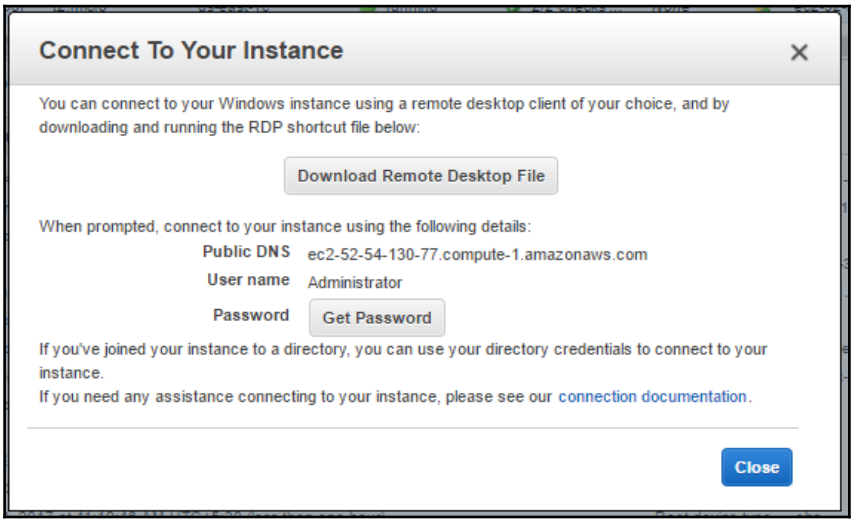

ec2-user@ip-10-0-0-240:~
[ec2-user@ip-10-0-0-13 ~]$ ssh -i "FirstEC2KeyPair.pem" ec2-user@10.0.0.240
Last login: Sun Jun 25 08:17:17 2017 from ip-10-0-0-13.ec2.internal
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
[ec2-user@ip-10-0-0-240 ~]$

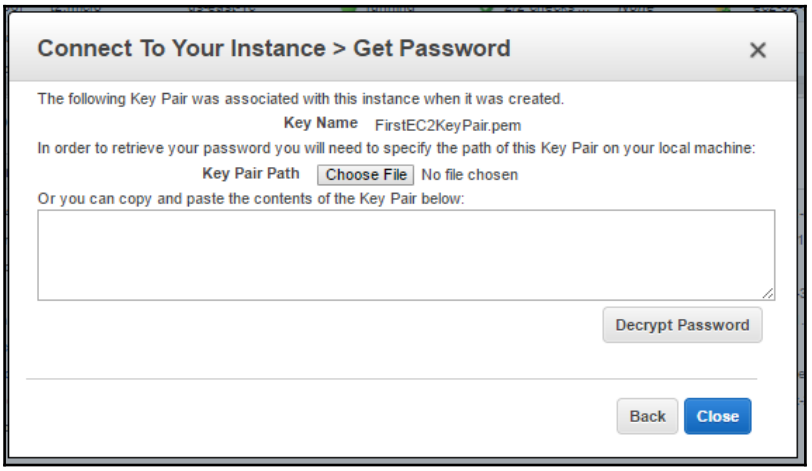

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 1: Choose an Amazon Machine Image (AMI)
own AMIs.
Cancel and Exit
Quick Start
1 to 31 of 31 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-a4c7edb2
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
Select
64-bit
SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-fde4ebea
SUSE Linux Enterprise Server 12 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
Select
64-bit
Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-9e2f0988
Red Hat Enterprise Linux version 7.3 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select
64-bit
Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-d15a75c7
Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm
Select
64-bit
Microsoft Windows Server 2016 Base - ami-f4d1f0e2
Microsoft Windows 2016 Datacenter edition. [English]
Root device type: ebs Virtualization type: hvm
Select
64-bit
Free tier eligible

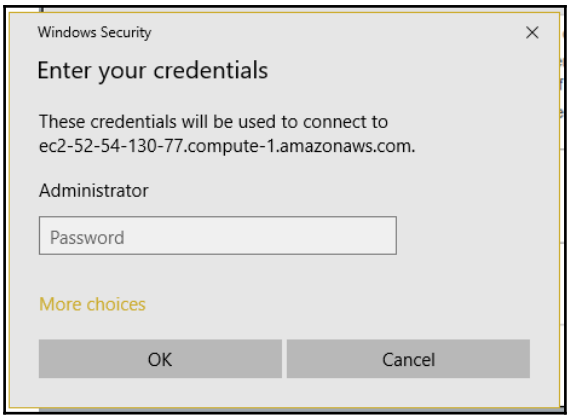

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.
Number of instances
1
Launch into Auto Scaling Group
Purchasing option
Request Spot instances
Network
vpc-85e41dfc (default)
Create new VPC
Subnet
No preference (default subnet in any Availability Zone
Create new subnet
Auto-assign Public IP
Use subnet setting (Enable)
Domain join directory
None
Create new directory
IAM role
None
Create new IAM role
Shutdown behavior
Stop
Enable termination protection
Protect against accidental termination
Monitoring
Enable CloudWatch detailed monitoring
Additional charges apply.
Tenancy
Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.
Advanced Details
Cancel
Previous
Review and Launch
Next: Add Storage

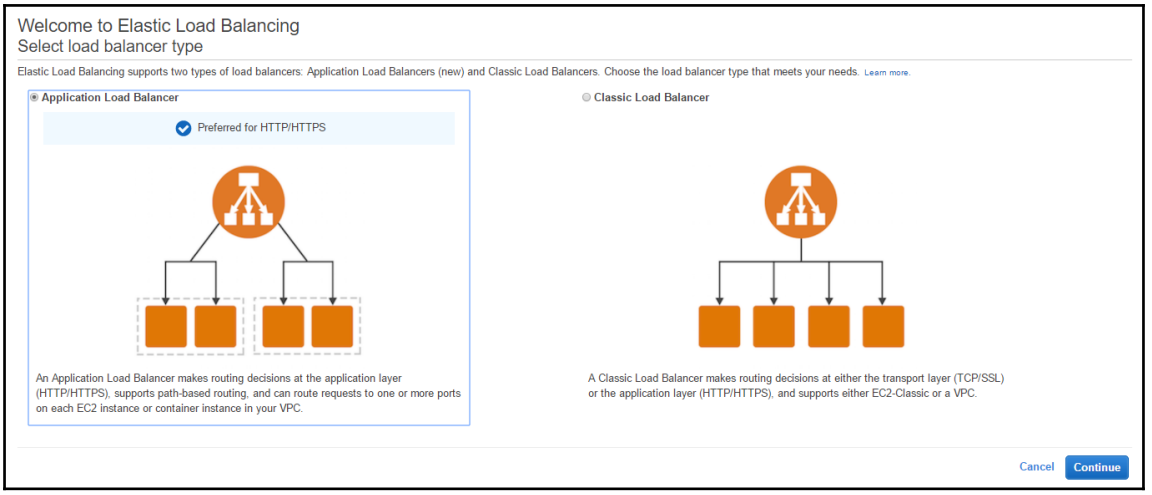

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review
Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
Security group name:
launch-wizard-2
Description:
launch-wizard-2 created 2017-07-02T11:05:21.614+05:30
Type
Protocol
Port Range
Source
RDP
TCP
3389
Custom
0.0.0.0/0
Add Rule

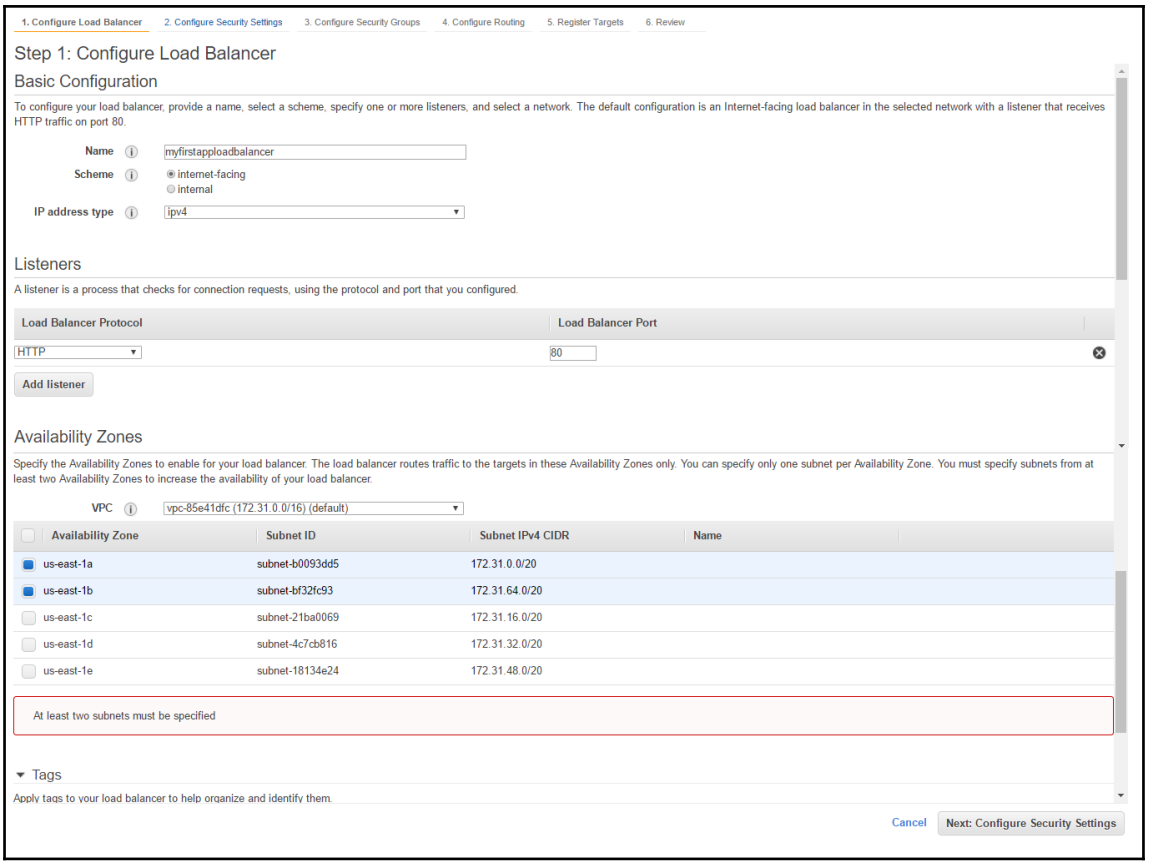

EC2 Dashboard
Events
Tags
Reports
Limits
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 4 of 4
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
IPv6 IPs
Key Name
i-08a43d009f051a36f
t2.micro
us-east-1c
running
2/2 checks ...
None
ec2-52-54-130-77.comp...
52.54.130.77
-
FirstEC2

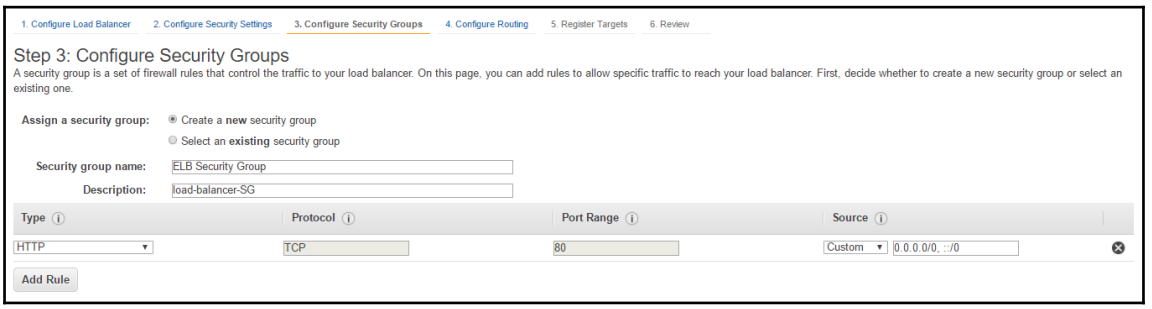

Connect To Your Instance
You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:
Download Remote Desktop File
When prompted, connect to your instance using the following details:
Public DNS
ec2-52-54-130-77.compute-1.amazonaws.com
User name
Administrator
Password
Get Password
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.
If you need any assistance connecting to your instance, please see our connection documentation.
Close

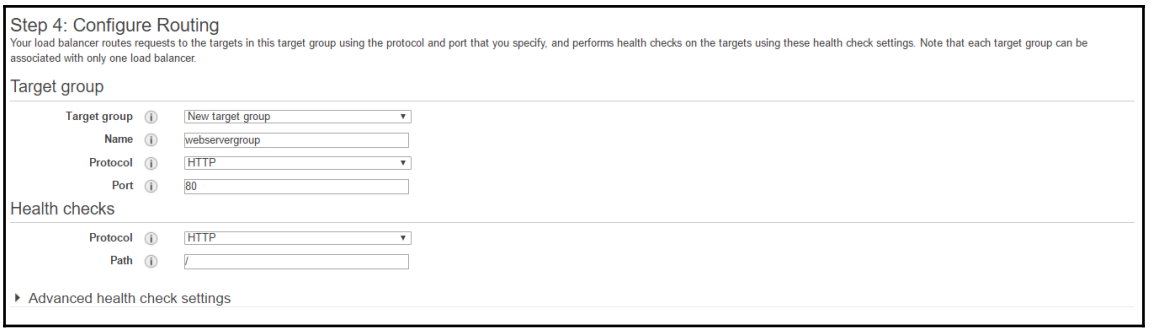

Connect To Your Instance > Get Password
The following Key Pair was associated with this instance when it was created.
Key Name
FirstEC2KeyPair.pem
In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:
Key Pair Path
Choose File
No file chosen
Or you can copy and paste the contents of the Key Pair below:
Decrypt Password
Back
Close

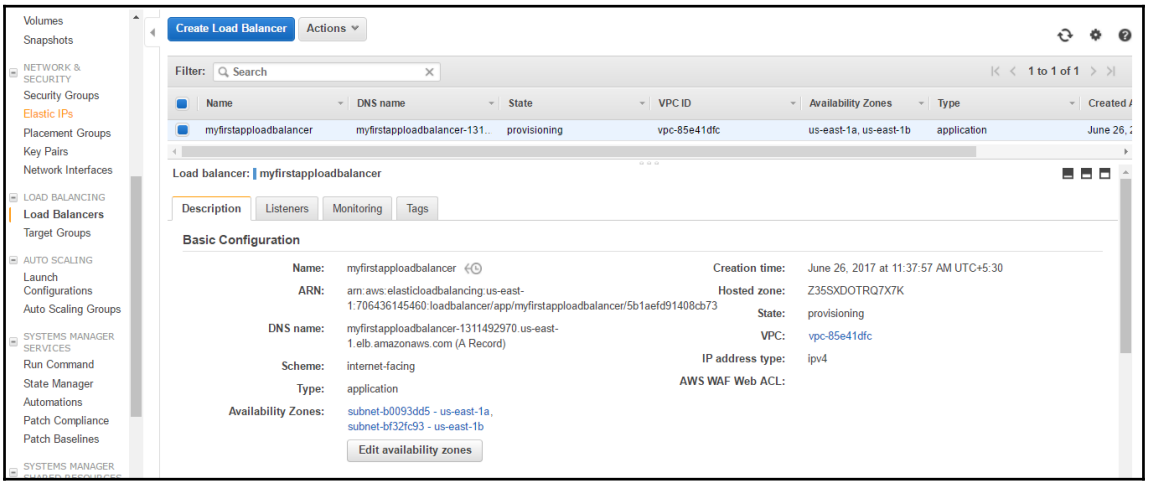

Windows Security
Enter your credentials
These credentials will be used to connect to
ec2-52-54-130-77.compute-1.amazonaws.com.
Administrator
Password
More choices
OK
Cancel

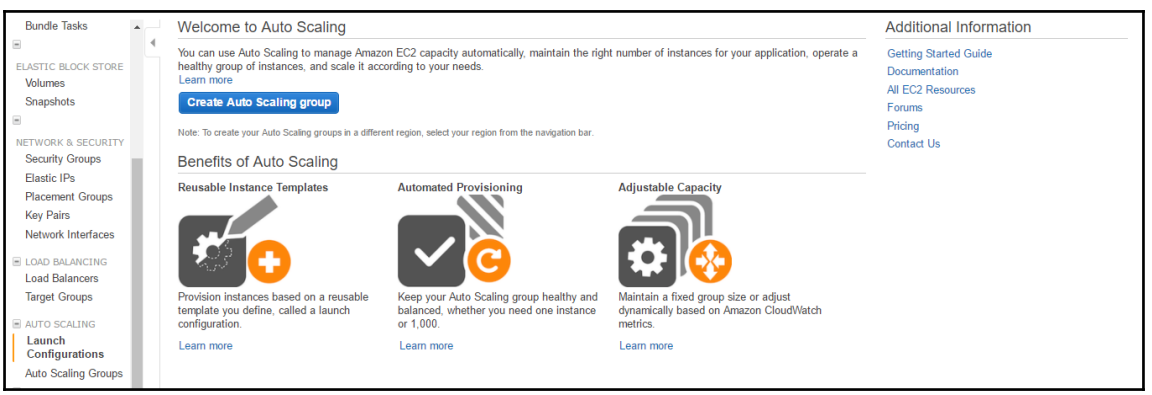

Welcome to Elastic Load Balancing
Select load balancer type
Elastic Load Balancing supports two types of load balancers: Application Load Balancers (new) and Classic Load Balancers. Choose the load balancer type that meets your needs. Learn more.
Application Load Balancer
Preferred for HTTP/HTTPS
An Application Load Balancer makes routing decisions at the application layer (HTTP/HTTPS), supports path-based routing, and can route requests to one or more ports on each EC2 instance or container instance in your VPC.
Classic Load Balancer
A Classic Load Balancer makes routing decisions at either the transport layer (TCP/SSL) or the application layer (HTTP/HTTPS), and supports either EC2-Classic or a VPC.
Cancel
Continue

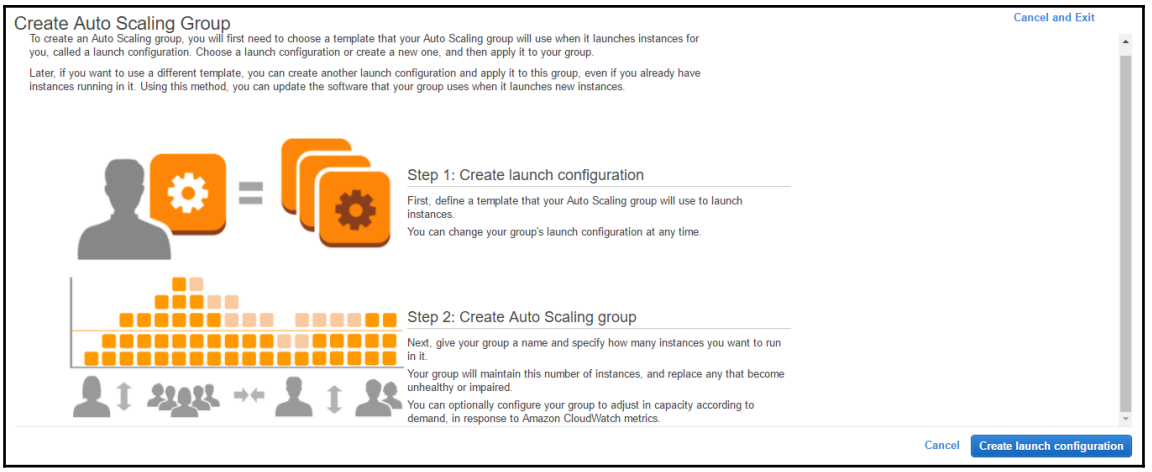

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 1: Configure Load Balancer
Basic Configuration
To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.
Name
myfirstapploadbalancer
Scheme
internet-facing
internal
IP address type
ipv4
Listeners
A listener is a process that checks for connection requests, using the protocol and port that you configured.
Load Balancer Protocol
Load Balancer Port
HTTP
80
Add listener
Availability Zones
Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.
VPC
vpc-85e41dfc (172.31.0.0/16) (default)
Availability Zone
Subnet ID
Subnet IPv4 CIDR
Name
us-east-1a
subnet-b0093dd5
172.31.0.0/20
us-east-1b
subnet-bf32fc93
172.31.64.0/20
us-east-1c
subnet-21ba0069
172.31.16.0/20
us-east-1d
subnet-4c7cb816
172.31.32.0/20
us-east-1e
subnet-18134e24
172.31.48.0/20
At least two subnets must be specified
Tags
Apply tags to your load balancer to help organize and identify them.
Cancel
Next: Configure Security Settings

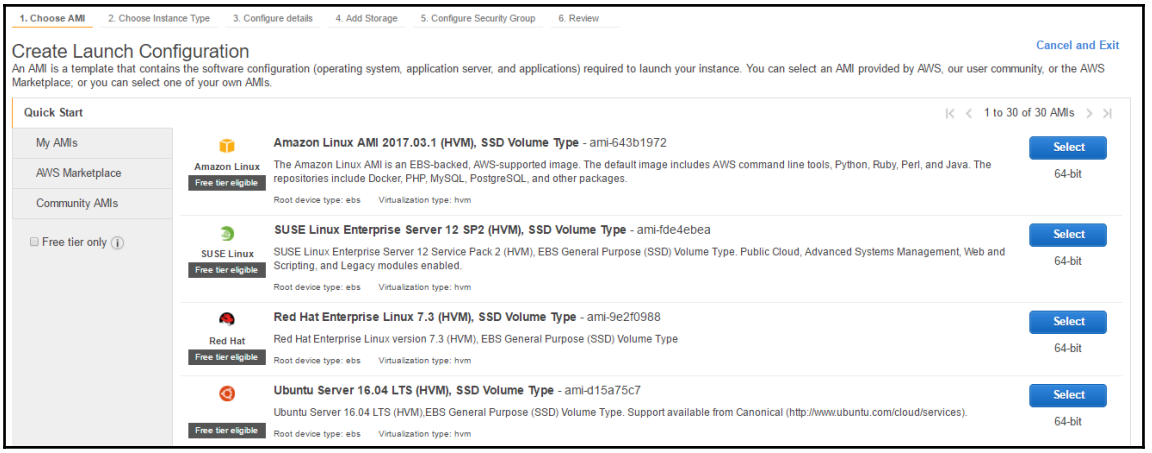

1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review
Step 3: Configure Security Groups
A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.
Assign a security group:
Create a new security group
Select an existing security group
Security group name:
ELB Security Group
Description:
load-balancer-SG
Type
Protocol
Port Range
Source
HTTP
TCP
80
Custom
0.0.0.0/0, ::/0
Add Rule

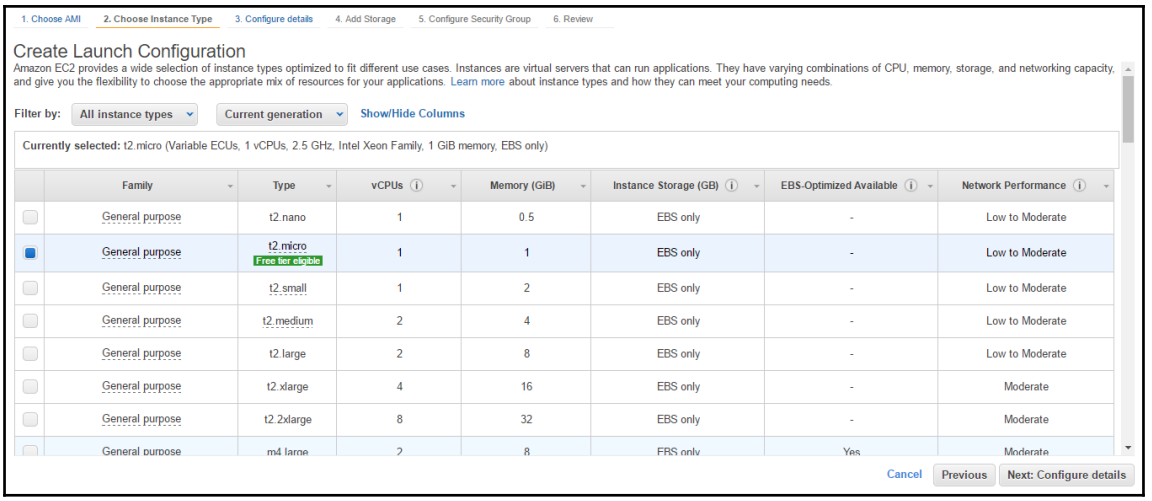

Step 4: Configure Routing
Your load balancer routes requests to the targets in this target group using the protocol and port that you specify, and performs health checks on the targets using these health check settings. Note that each target group can be associated with only one load balancer.
Target group
Target group
New target group
Name
webservergroup
Protocol
HTTP
Port
80
Health checks
Protocol
HTTP
Path
/
Advanced health check settings

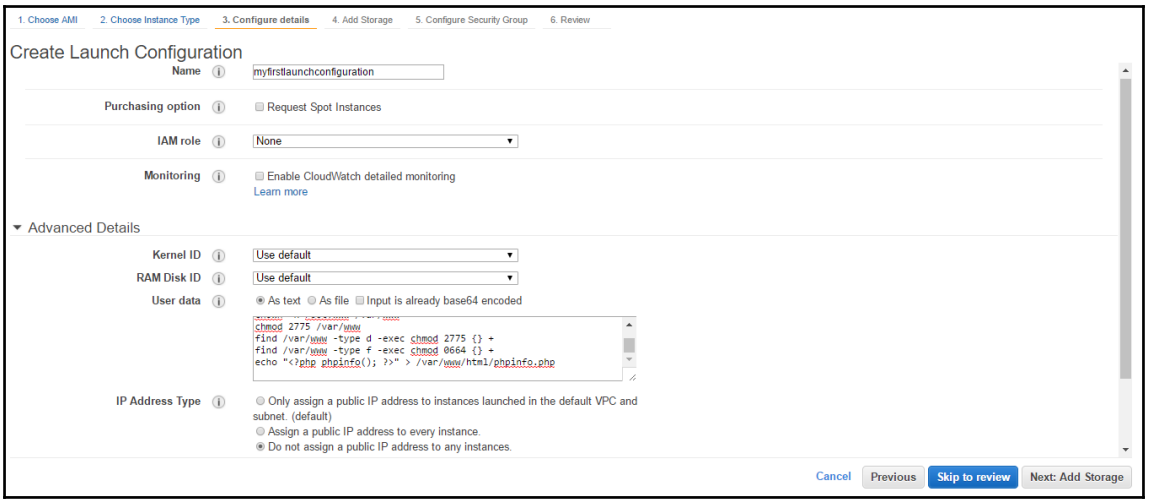

Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
SYSTEMS MANAGER SERVICES
Run Command
State Manager
Automations
Patch Compliance
Patch Baselines
Create Load Balancer
Actions
Filter:
Search
1 to 1 of 1
Name
DNS name
State
VPC ID
Availability Zones
Type
Created
myfirstapploadbalancer
myfirstapploadbalancer-131..
provisioning
vpc-85e41dfc
us-east-1a, us-east-1b
application
June 26,
Load balancer: myfirstapploadbalancer
Description
Listeners
Monitoring
Tags
Basic Configuration
Name: myfirstapploadbalancer
ARN: arn:aws:elasticloadbalancing:us-east-1:706436145460:loadbalancer/app/myfirstapploadbalancer/5b1aefd91408cb73
DNS name: myfirstapploadbalancer-1311492970.us-east-1.elb.amazonaws.com (A Record)
Scheme: internet-facing
Type: application
Availability Zones: subnet-b0093dd5 - us-east-1a, subnet-bf32fc93 - us-east-1b
Edit availability zones
Creation time: June 26, 2017 at 11:37:57 AM UTC+5:30
Hosted zone: Z35SXDOTRQ7X7K
State: provisioning
VPC: vpc-85e41dfc
IP address type: ipv4
AWS WAF Web ACL:

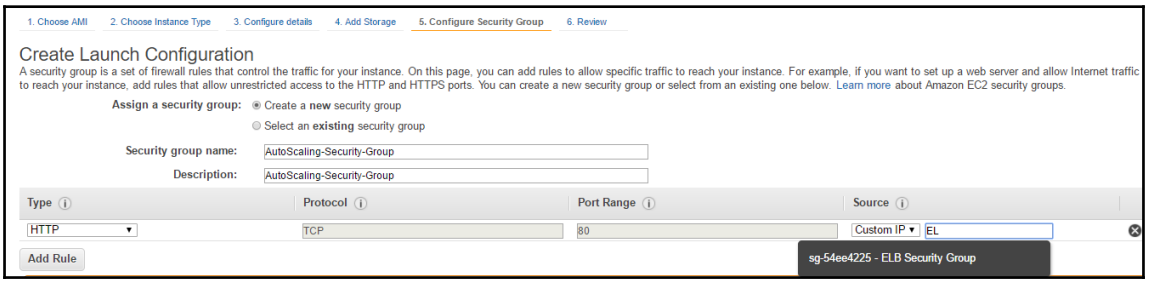

Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
Welcome to Auto Scaling
You can use Auto Scaling to manage Amazon EC2 capacity automatically, maintain the right number of instances for your application, operate a healthy group of instances, and scale it according to your needs.
Learn more
Create Auto Scaling group
Note: To create your Auto Scaling groups in a different region, select your region from the navigation bar.
Benefits of Auto Scaling
Reusable Instance Templates
Provision instances based on a reusable template you define, called a launch configuration.
Learn more
Automated Provisioning
Keep your Auto Scaling group healthy and balanced, whether you need one instance or 1,000.
Learn more
Adjustable Capacity
Maintain a fixed group size or adjust dynamically based on Amazon CloudWatch metrics.
Learn more
Additional Information
Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

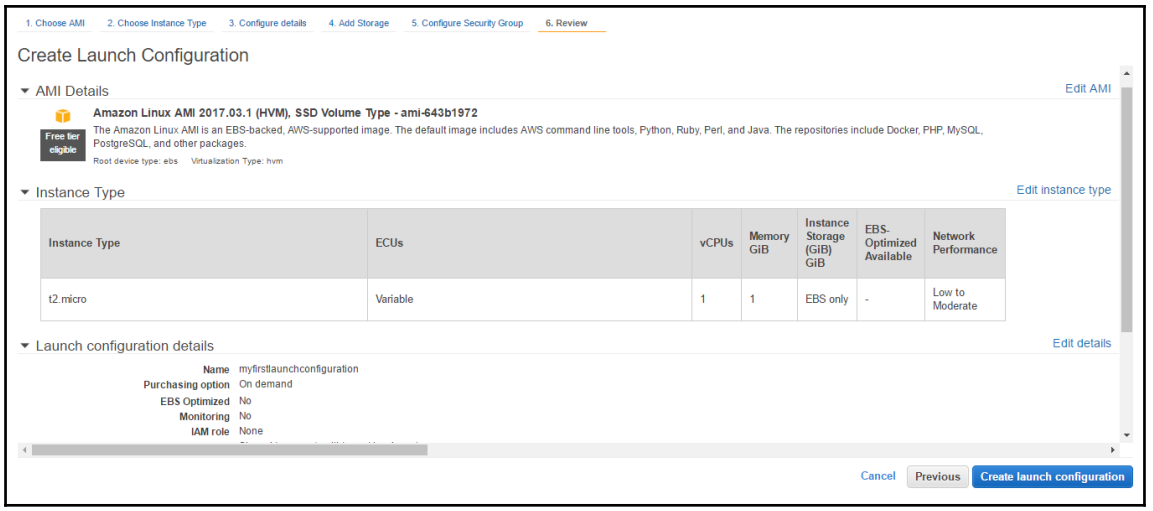

Create Auto Scaling Group
Cancel and Exit
To create an Auto Scaling group, you will first need to choose a template that your Auto Scaling group will use when it launches instances for you, called a launch configuration. Choose a launch configuration or create a new one, and then apply it to your group.
Later, if you want to use a different template, you can create another launch configuration and apply it to this group, even if you already have instances running in it. Using this method, you can update the software that your group uses when it launches new instances.
Step 1: Create launch configuration
First, define a template that your Auto Scaling group will use to launch instances.
You can change your group's launch configuration at any time.
Step 2: Create Auto Scaling group
Next, give your group a name and specify how many instances you want to run in it.
Your group will maintain this number of instances, and replace any that become unhealthy or impaired.
You can optionally configure your group to adjust in capacity according to demand, in response to Amazon CloudWatch metrics.
Cancel
Create launch configuration

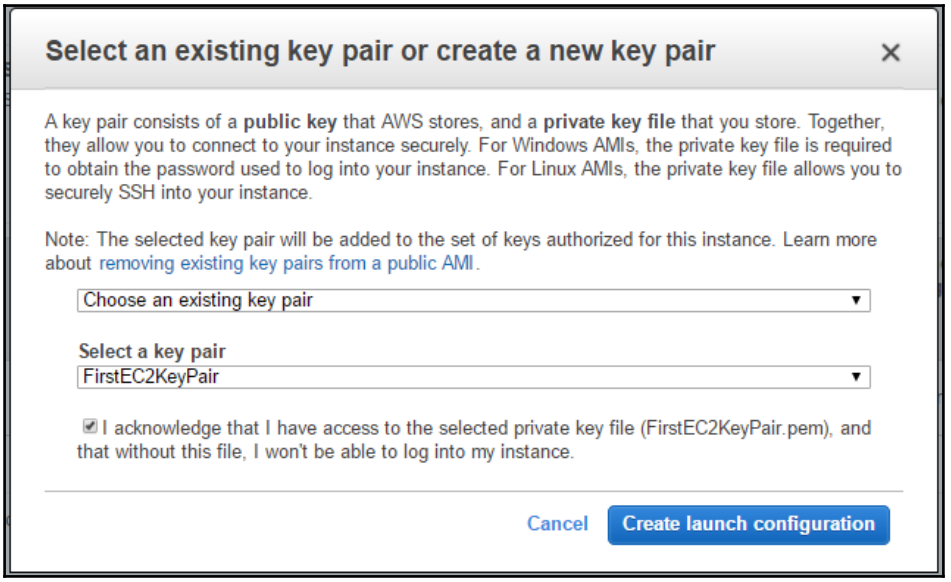

1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Cancel and Exit
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
Quick Start
1 to 30 of 30 AMIs
My AMIs
AWS Marketplace
Community AMIs
Free tier only
Amazon Linux
Free tier eligible
Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-643b1972
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm
Select
64-bit
SUSE Linux
Free tier eligible
SUSE Linux Enterprise Server 12 SP2 (HVM), SSD Volume Type - ami-fde4ebea
SUSE Linux Enterprise Server 12 Service Pack 2 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm
Select
64-bit
Red Hat
Free tier eligible
Red Hat Enterprise Linux 7.3 (HVM), SSD Volume Type - ami-9e2f0988
Red Hat Enterprise Linux version 7.3 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm
Select
64-bit
Free tier eligible
Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-d15a75c7
Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm
Select
64-bit

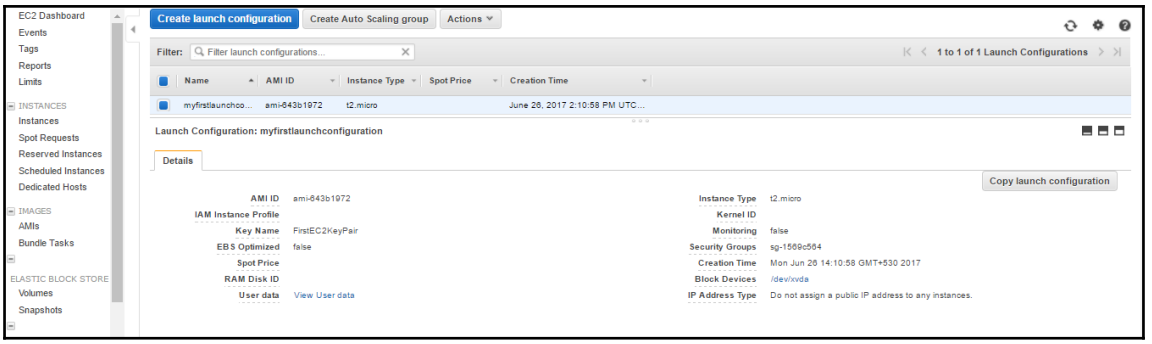

1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.
Filter by:
All instance types
Current generation
Show/Hide Columns
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)
Family
Type
vCPUs
Memory (GiB)
Instance Storage (GB)
EBS-Optimized Available
Network Performance
General purpose
t2.nano
1
0.5
EBS only
-
Low to Moderate
General purpose
t2.micro
Free tier eligible
1
1
EBS only
-
Low to Moderate
General purpose
t2.small
1
2
EBS only
-
Low to Moderate
General purpose
t2.medium
2
4
EBS only
-
Low to Moderate
General purpose
t2.large
2
8
EBS only
-
Low to Moderate
General purpose
t2.xlarge
4
16
EBS only
-
Moderate
General purpose
t2.2xlarge
8
32
EBS only
-
Moderate
General purpose
m4.large
2
8
EBS only
Yes
Moderate
Cancel
Previous
Next: Configure details

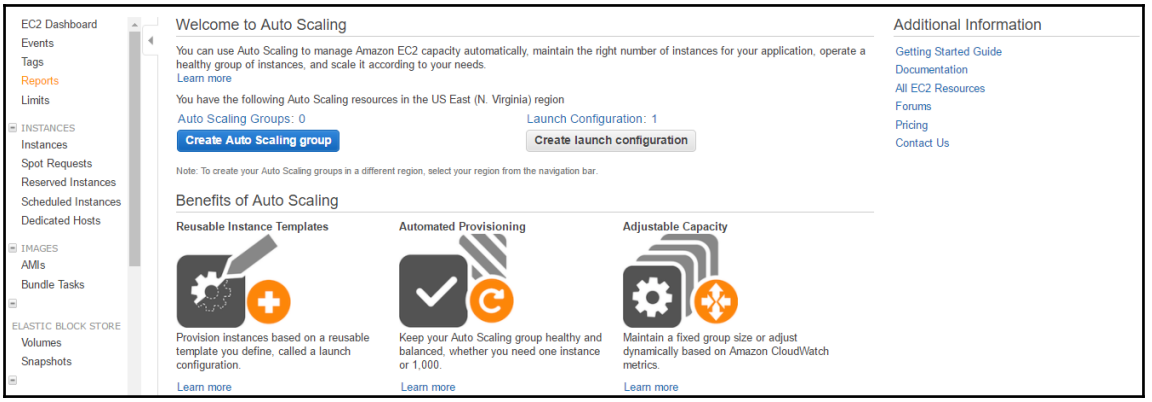

1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
Name
myfirstlaunchconfiguration
Purchasing option
Request Spot Instances
IAM role
None
Monitoring
Enable CloudWatch detailed monitoring
Learn more
Advanced Details
Kernel ID
Use default
RAM Disk ID
Use default
User data
As text
As file
Input is already base64 encoded
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} +
find /var/www -type f -exec chmod 0664 {} +
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
IP Address Type
Only assign a public IP address to instances launched in the default VPC and subnet. (default)
Assign a public IP address to every instance.
Do not assign a public IP address to any instances.
Cancel
Previous
Skip to review
Next: Add Storage


1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.
Assign a security group:
Create a new security group
Select an existing security group
Security group name:
AutoScaling-Security-Group
Description:
AutoScaling-Security-Group
Type
Protocol
Port Range
Source
HTTP
TCP
80
Custom IP
EL
sg-54ee4225 - ELB Security Group
Add Rule

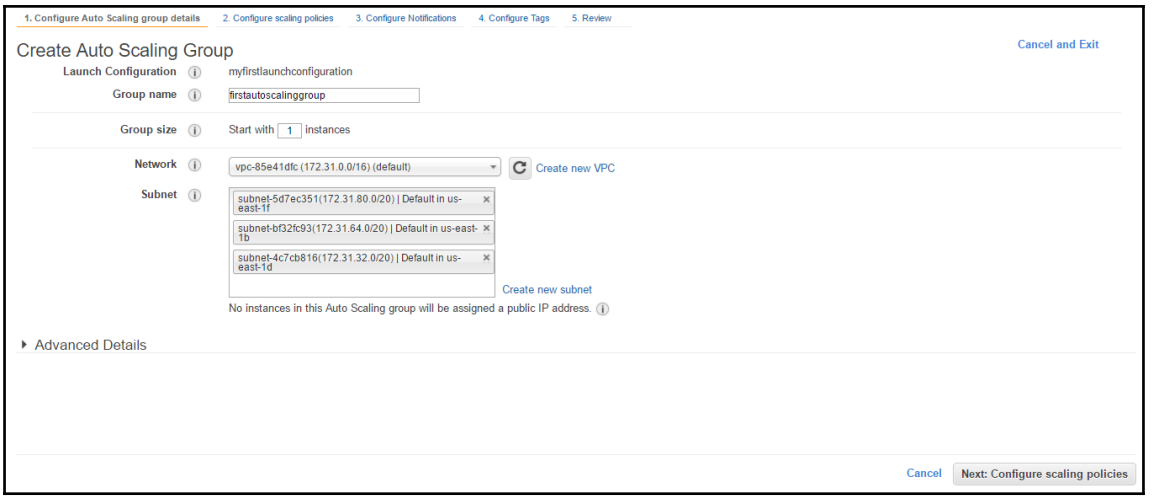

1. Choose AMI
2. Choose Instance Type
3. Configure details
4. Add Storage
5. Configure Security Group
6. Review
Create Launch Configuration
AMI Details
Edit AMI
Amazon Linux AMI 2017.03.1 (HVM), SSD Volume Type - ami-643b1972
Free tier eligible
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization Type: hvm
Instance Type
Edit instance type
Instance Type
ECUs
vCPUs
Memory GiB
Instance Storage (GiB) GiB
EBS-Optimized Available
Network Performance
t2.micro
Variable
1
1
EBS only
-
Low to Moderate
Launch configuration details
Edit details
Name myfirstlaunchconfiguration
Purchasing option On demand
EBS Optimized No
Monitoring No
IAM role None
Cancel
Previous
Create launch configuration

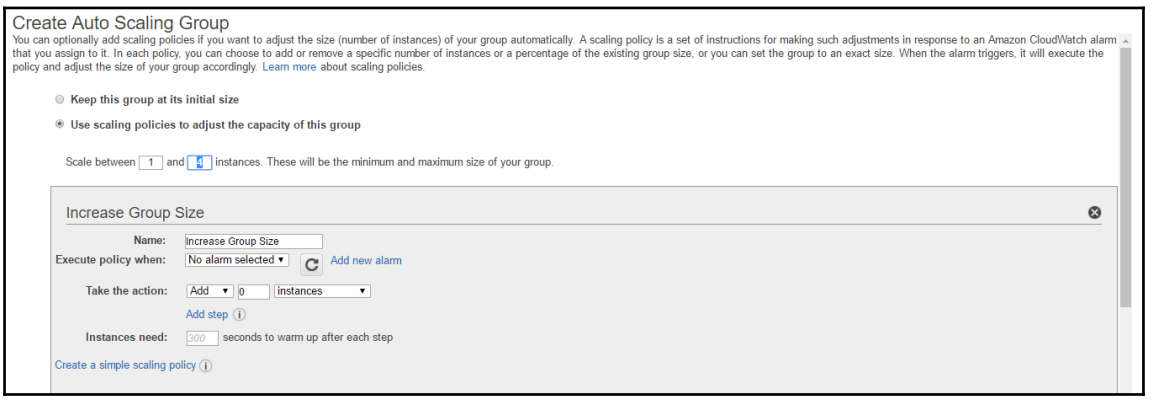

Select an existing key pair or create a new key pair
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
Choose an existing key pair
Select a key pair
FirstEC2KeyPair
I acknowledge that I have access to the selected private key file (FirstEC2KeyPair.pem), and that without this file, I won't be able to log into my instance.
Cancel
Create launch configuration

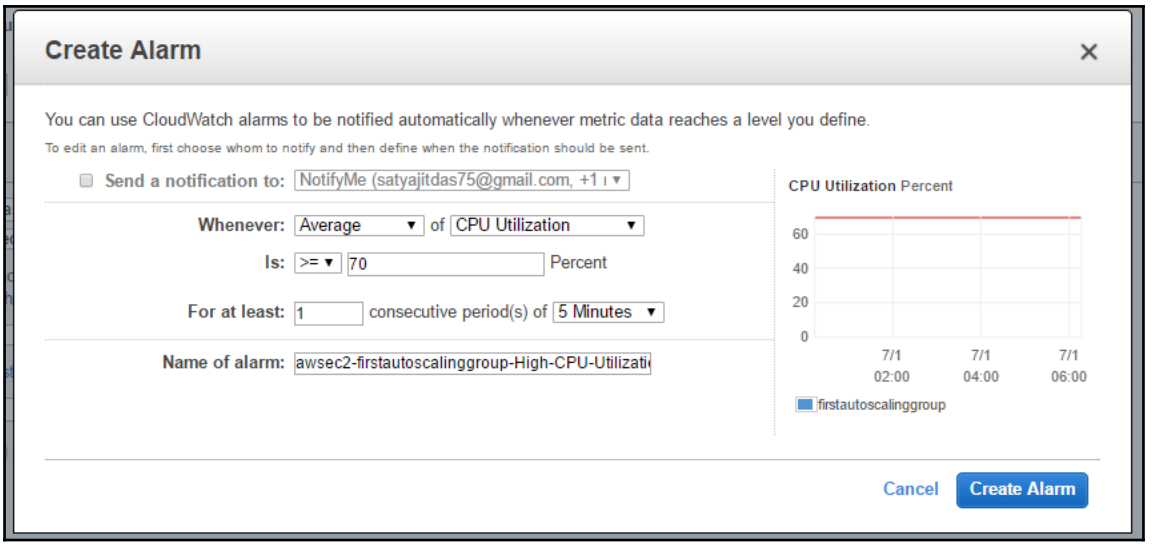

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Create launch configuration
Create Auto Scaling group
Actions
Filter:
Filter launch configurations...
1 to 1 of 1 Launch Configurations
Name
AMI ID
Instance Type
Spot Price
Creation Time
myfirstlaunchco...
ami-643b1972
t2.micro
June 26, 2017 2:10:58 PM UTC...
Launch Configuration: myfirstlaunchconfiguration
Details
Copy launch configuration
AMI ID
ami-643b1972
IAM Instance Profile
Key Name
FirstEC2KeyPair
EBS Optimized
false
Spot Price
RAM Disk ID
User data
View User data
Instance Type
t2.micro
Kernel ID
Monitoring
false
Security Groups
sg-1569c564
Creation Time
Mon Jun 26 14:10:58 GMT+530 2017
Block Devices
/dev/xvda
IP Address Type
Do not assign a public IP address to any instances.

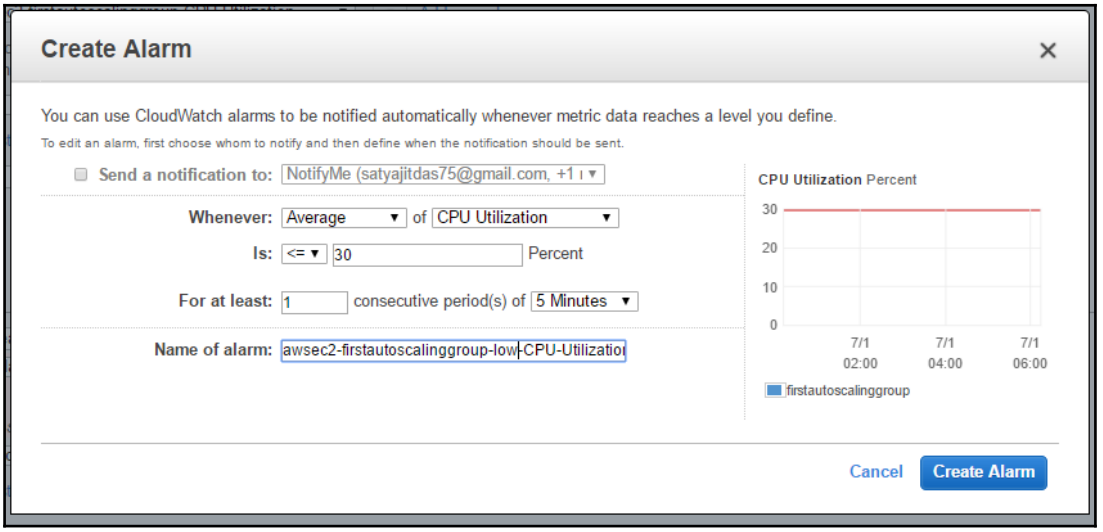

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Welcome to Auto Scaling
You can use Auto Scaling to manage Amazon EC2 capacity automatically, maintain the right number of instances for your application, operate a healthy group of instances, and scale it according to your needs.
Learn more
You have the following Auto Scaling resources in the US East (N. Virginia) region
Auto Scaling Groups: 0
Launch Configuration: 1
Create Auto Scaling group
Create launch configuration
Note: To create your Auto Scaling groups in a different region, select your region from the navigation bar.
Benefits of Auto Scaling
Reusable Instance Templates
Provision instances based on a reusable template you define, called a launch configuration.
Learn more
Automated Provisioning
Keep your Auto Scaling group healthy and balanced, whether you need one instance or 1,000.
Learn more
Adjustable Capacity
Maintain a fixed group size or adjust dynamically based on Amazon CloudWatch metrics.
Learn more
Additional Information
Getting Started Guide
Documentation
All EC2 Resources
Forums
Pricing
Contact Us

Create Auto Scaling Group
Cancel and Exit
To create an Auto Scaling group, you will first need to choose a template that your Auto Scaling group will use when it launches instances for you, called a launch configuration. Choose a launch configuration or create a new one, and then apply it to your group.
Later, if you want to use a different template, you can create another launch configuration and apply it to this group, even if you already have instances running in it. Using this method, you can update the software that your group uses when it launches new instances.
Create a new launch configuration
Create an Auto Scaling group from an existing launch configuration
Filter launch configurations...
1 to 1 of 1 Launch Configurations
Name
AMI ID
Instance Type
Spot Price
Security Groups
myfirstlaunchconfiguration
ami-643b1972
t2.micro
sg-1569c564
Cancel
Next Step

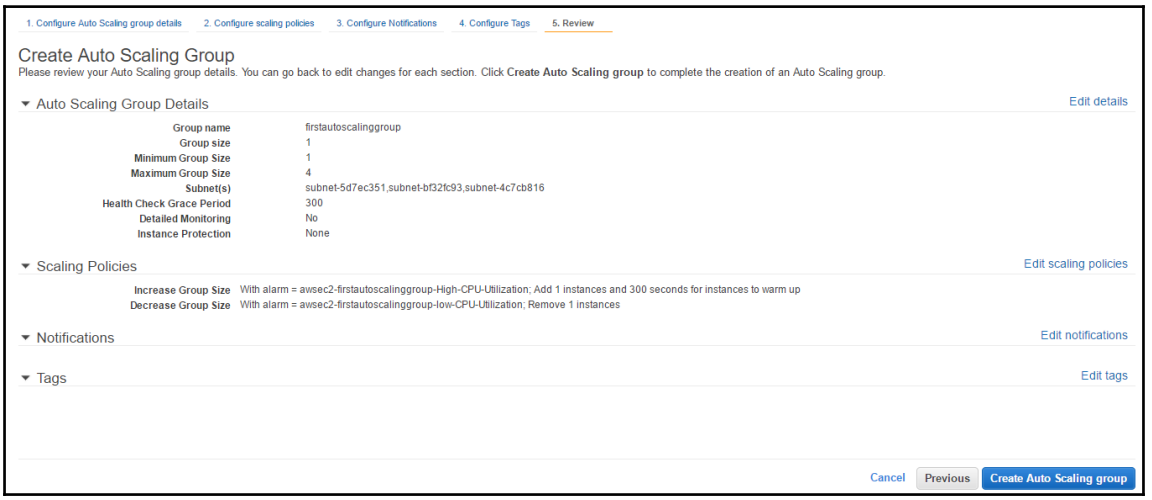

1. Configure Auto Scaling group details
2. Configure scaling policies
3. Configure Notifications
4. Configure Tags
5. Review
Create Auto Scaling Group
Cancel and Exit
Launch Configuration
myfirstlaunchconfiguration
Group name
firstautoscalinggroup
Group size
Start with 1 instances
Network
vpc-85e41dfc (172.31.0.0/16) (default)
Create new VPC
Subnet
subnet-5d7ec351(172.31.80.0/20) | Default in us-east-1f
subnet-bf32fc93(172.31.64.0/20) | Default in us-east-1b
subnet-4c7cb816(172.31.32.0/20) | Default in us-east-1d
Create new subnet
No instances in this Auto Scaling group will be assigned a public IP address.
Advanced Details
Cancel
Next: Configure scaling policies

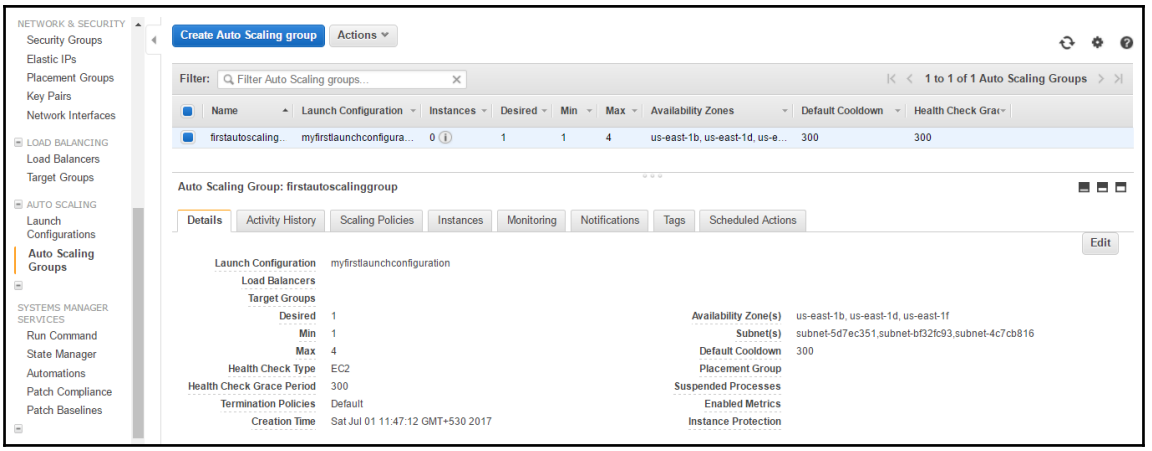

Create Auto Scaling Group
You can optionally add scaling policies if you want to adjust the size (number of instances) of your group automatically. A scaling policy is a set of instructions for making such adjustments in response to an Amazon CloudWatch alarm that you assign to it. In each policy, you can choose to add or remove a specific number of instances or a percentage of the existing group size, or you can set the group to an exact size. When the alarm triggers, it will execute the policy and adjust the size of your group accordingly. Learn more about scaling policies.
Keep this group at its initial size
Use scaling policies to adjust the capacity of this group
Scale between 1 and 4 instances. These will be the minimum and maximum size of your group.
Increase Group Size
Name:
Increase Group Size
Execute policy when:
No alarm selected
Add new alarm
Take the action:
Add
0
instances
Add step
Instances need:
300
seconds to warm up after each step
Create a simple scaling policy

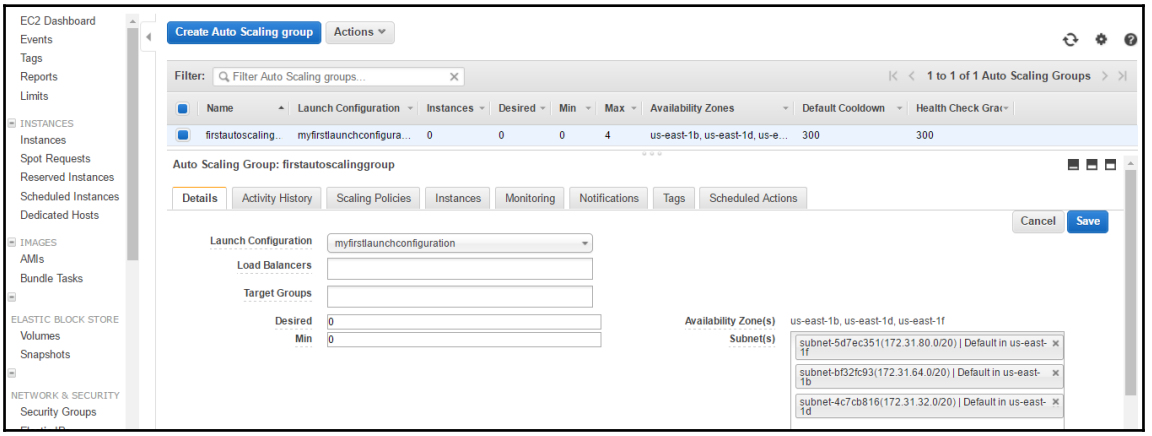

Create Alarm
You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.
Send a notification to:
NotifyMe (satyajitdas75@gmail.com, +1
Whenever:
Average
of
CPU Utilization
Is:
>=
70
Percent
For at least:
1
consecutive period(s) of
5 Minutes
Name of alarm:
awsec2-firstautoscalinggroup-High-CPU-Utilizati
CPU Utilization Percent
60
40
20
0
7/1
02:00
7/1
04:00
7/1
06:00
firstautoscalinggroup
Cancel
Create Alarm

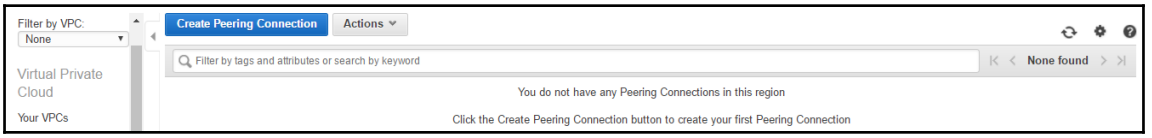

Create Alarm
You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.
Send a notification to:
NotifyMe (satyajitdas75@gmail.com, +1
Whenever:
Average
of
CPU Utilization
Is:
<=
30
Percent
For at least:
1
consecutive period(s) of
5 Minutes
Name of alarm:
awsec2-firstautoscalinggroup-low-CPU-Utilizatio
CPU Utilization Percent
30
20
10
0
7/1
02:00
7/1
04:00
7/1
06:00
firstautoscalinggroup
Cancel
Create Alarm

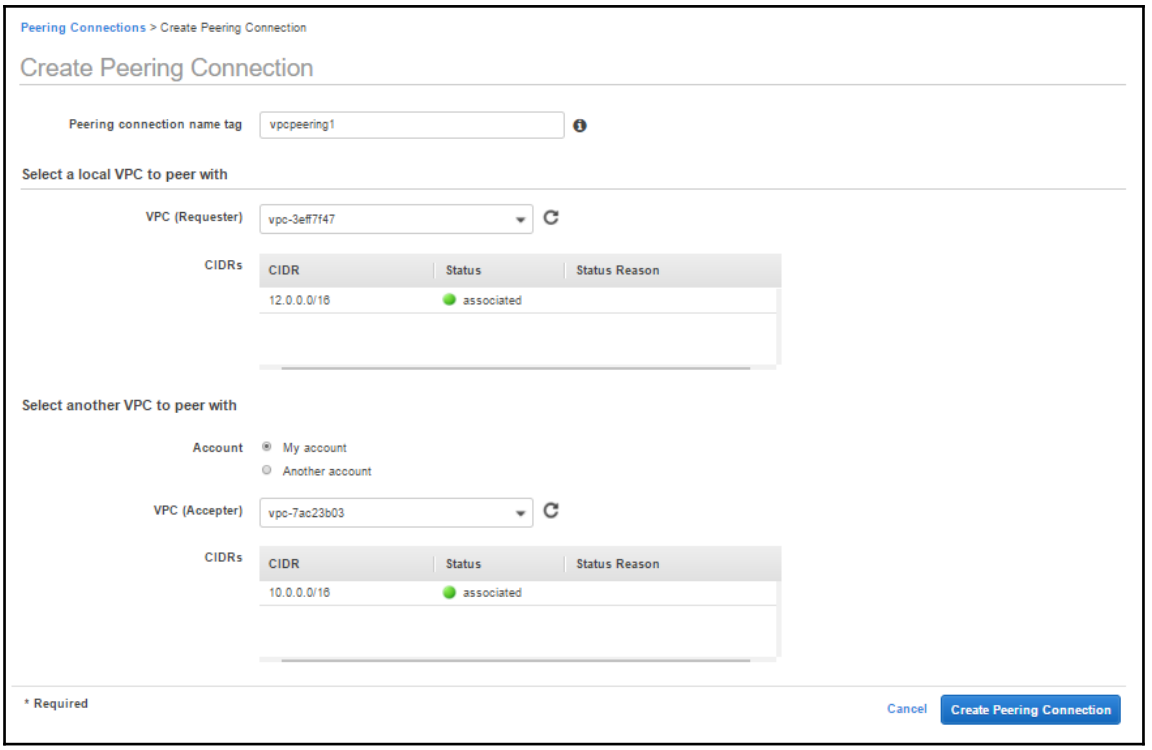
1. Configure Auto Scaling group details
2. Configure scaling policies
3. Configure Notifications
4. Configure Tags
5. Review
Create Auto Scaling Group
Increase Group Size
Name: Increase Group Size
Execute policy when: awsec2-firstautoscalinggroup-High-CPU-Utilization Edit Remove
breaches the alarm threshold: CPUUtilization >= 70 for 300 seconds
for the metric dimensions AutoScalingGroupName = firstautoscalinggroup
Take the action: Add 1 instances when 70 <= CPUUtilization < +infinity
Add step
Instances need: 300 seconds to warm up after each step
Create a simple scaling policy
Decrease Group Size
Name: Decrease Group Size
Execute policy when: awsec2-firstautoscalinggroup-low-CPU-Utilization Edit Remove
breaches the alarm threshold: CPUUtilization <= 30 for 300 seconds
for the metric dimensions AutoScalingGroupName = firstautoscalinggroup
Take the action: Remove 1 instances when 30 >= CPUUtilization > -infinity
Add step
Cancel
Previous
Review
Next: Configure Notifications

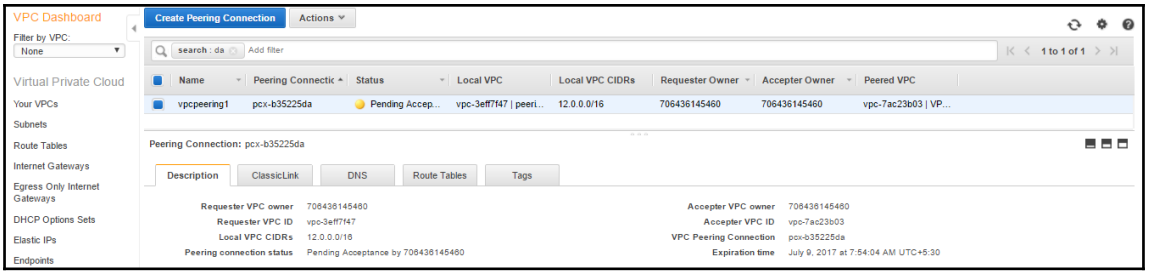

1. Configure Auto Scaling group details
2. Configure scaling policies
3. Configure Notifications
4. Configure Tags
5. Review
Create Auto Scaling Group
Please review your Auto Scaling group details. You can go back to edit changes for each section. Click Create Auto Scaling group to complete the creation of an Auto Scaling group.
Auto Scaling Group Details
Edit details
Group name firstautoscalinggroup
Group size 1
Minimum Group Size 1
Maximum Group Size 4
Subnet(s) subnet-5d7ec351,subnet-bf32fc93,subnet-4c7cb816
Health Check Grace Period 300
Detailed Monitoring No
Instance Protection None
Scaling Policies
Edit scaling policies
Increase Group Size With alarm = awsec2-firstautoscalinggroup-High-CPU-Utilization; Add 1 instances and 300 seconds for instances to warm up
Decrease Group Size With alarm = awsec2-firstautoscalinggroup-low-CPU-Utilization; Remove 1 instances
Notifications
Edit notifications
Tags
Edit tags
Cancel
Previous
Create Auto Scaling group

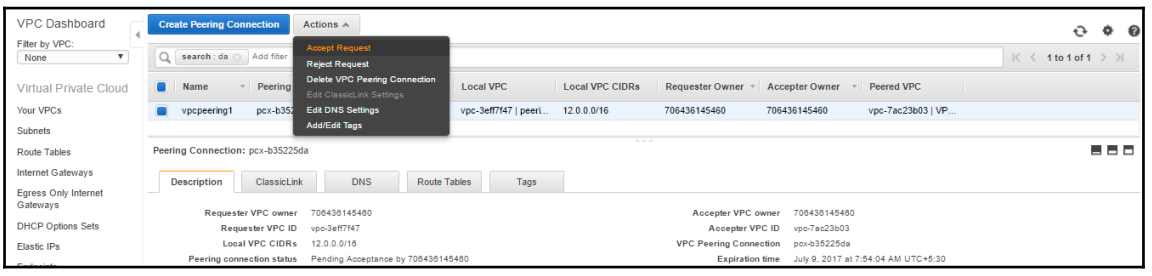

NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
AUTO SCALING
Launch Configurations
Auto Scaling Groups
SYSTEMS MANAGER SERVICES
Run Command
State Manager
Automations
Patch Compliance
Patch Baselines
Create Auto Scaling group
Actions
Filter: Filter Auto Scaling groups...
1 to 1 of 1 Auto Scaling Groups
Name
Launch Configuration
Instances
Desired
Min
Max
Availability Zones
Default Cooldown
Health Check Gra
firstautoscaling..
myfirstlaunchconfigura...
0
1
1
4
us-east-1b, us-east-1d, us-e...
300
300
Auto Scaling Group: firstautoscalinggroup
Details
Activity History
Scaling Policies
Instances
Monitoring
Notifications
Tags
Scheduled Actions
Edit
Launch Configuration
myfirstlaunchconfiguration
Load Balancers
Target Groups
Desired
1
Min
1
Max
4
Health Check Type
EC2
Health Check Grace Period
300
Termination Policies
Default
Creation Time
Sat Jul 01 11:47:12 GMT+530 2017
Availability Zone(s)
us-east-1b, us-east-1d, us-east-1f
Subnet(s)
subnet-5d7ec351,subnet-bf32fc93,subnet-4c7cb816
Default Cooldown
300
Placement Group
Suspended Processes
Enabled Metrics
Instance Protection

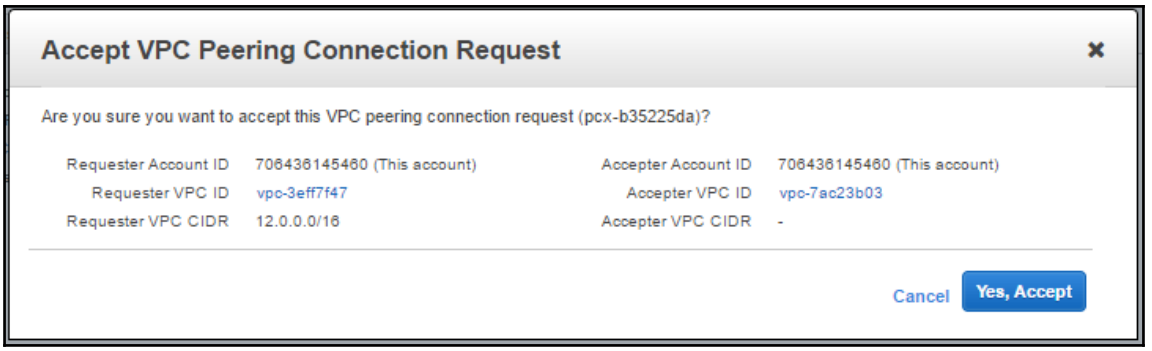

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Create Auto Scaling group
Actions
Filter: Filter Auto Scaling groups...
1 to 1 of 1 Auto Scaling Groups
Name
Launch Configuration
Instances
Desired
Min
Max
Availability Zones
Default Cooldown
Health Check Gra
firstautoscaling..
myfirstlaunchconfigura...
0
0
0
4
us-east-1b, us-east-1d, us-e...
300
300
Auto Scaling Group: firstautoscalinggroup
Details
Activity History
Scaling Policies
Instances
Monitoring
Notifications
Tags
Scheduled Actions
Cancel
Save
Launch Configuration
myfirstlaunchconfiguration
Load Balancers
Target Groups
Desired
0
Min
0
Availability Zone(s)
us-east-1b, us-east-1d, us-east-1f
Subnet(s)
subnet-5d7ec351(172.31.80.0/20) | Default in us-east-1f
subnet-bf32fc93(172.31.64.0/20) | Default in us-east-1b
subnet-4c7cb816(172.31.32.0/20) | Default in us-east-1d

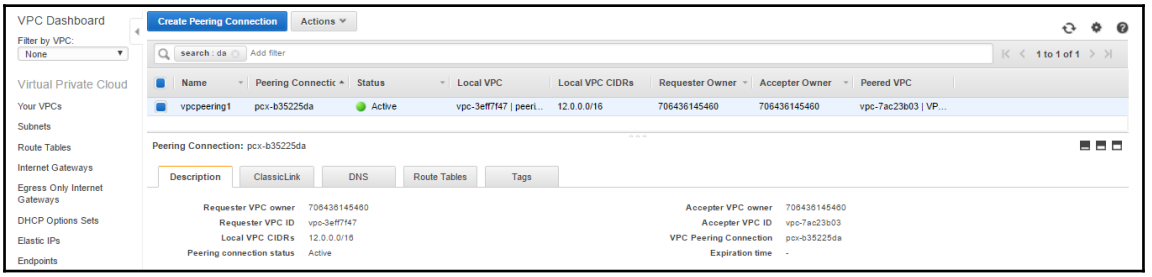

Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Create Peering Connection
Actions
Filter by tags and attributes or search by keyword
None found
You do not have any Peering Connections in this region
Click the Create Peering Connection button to create your first Peering Connection

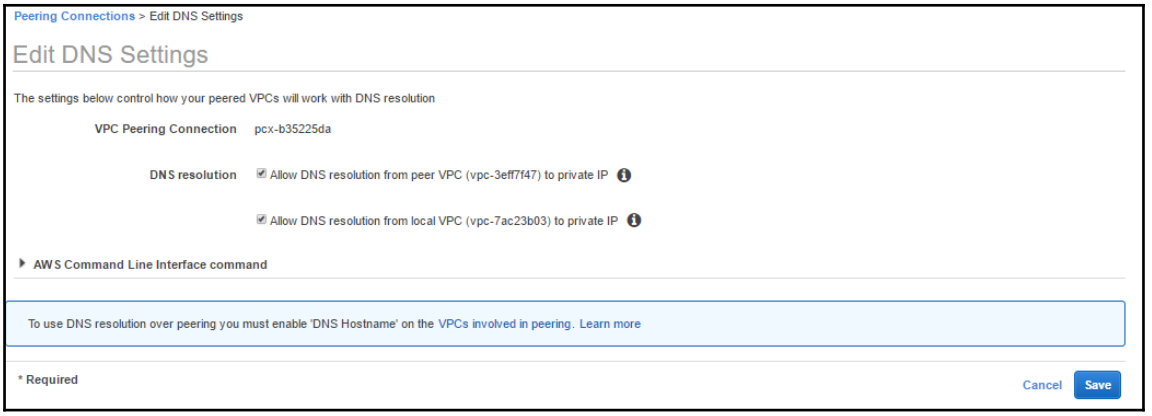

Peering Connections > Create Peering Connection
Create Peering Connection
Peering connection name tag
vpcpeering1
Select a local VPC to peer with
VPC (Requester)
vpc-3eff7f47
CIDRs
CIDR
Status
Status Reason
12.0.0.0/16
associated
Select another VPC to peer with
Account
My account
Another account
VPC (Accepter)
vpc-7ac23b03
CIDRs
CIDR
Status
Status Reason
10.0.0.0/16
associated
* Required
Cancel
Create Peering Connection

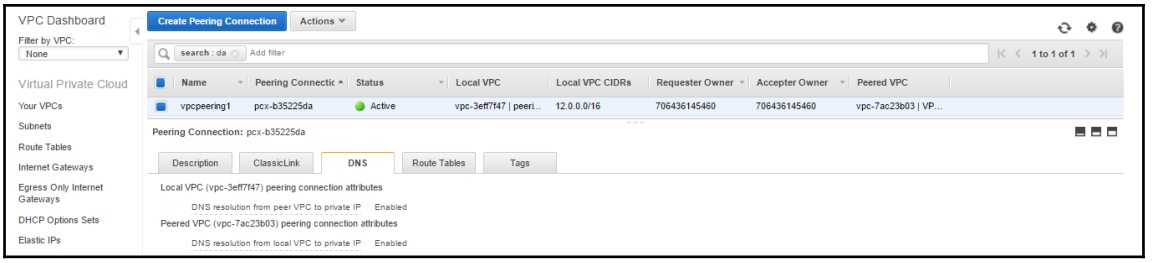

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create Peering Connection
Actions
1 to 1 of 1
Name
Peering Connectic
Status
Local VPC
Local VPC CIDRs
Requester Owner
Accepter Owner
Peered VPC
vpcpeering1
pcx-b35225da
Pending Accep...
vpc-3eff7f47 | peeri...
12.0.0.0/16
706436145460
706436145460
vpc-7ac23b03 | VP...
Peering Connection: pcx-b35225da
Description
ClassicLink
DNS
Route Tables
Tags
Requester VPC owner 706436145460
Requester VPC ID vpc-3eff7f47
Local VPC CIDRs 12.0.0.0/16
Peering connection status Pending Acceptance by 706436145460
Accepter VPC owner 706436145460
Accepter VPC ID vpc-7ac23b03
VPC Peering Connection pcx-b35225da
Expiration time July 9, 2017 at 7:54:04 AM UTC+5:30

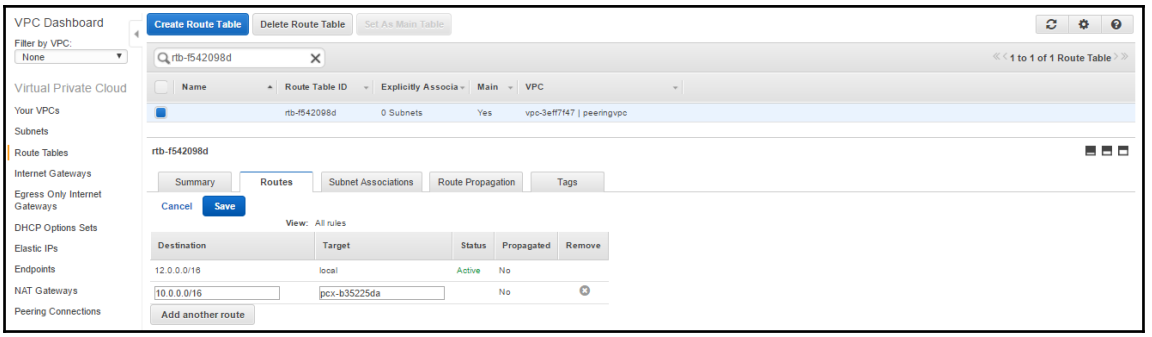

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create Peering Connection
Actions
Accept Request
Reject Request
Delete VPC Peering Connection
Edit ClassicLink Settings
Edit DNS Settings
Add/Edit Tags
1 to 1 of 1
Name
Local VPC
Local VPC CIDRs
Requester Owner
Accepter Owner
Peered VPC
vpcpeering1
vpc-3eff7f47 | peeri...
12.0.0.0/16
706436145460
706436145460
vpc-7ac23b03 | VP...
Peering Connection: pcx-b35225da
Description
ClassicLink
DNS
Route Tables
Tags
Requester VPC owner 706436145460
Requester VPC ID vpc-3eff7f47
Local VPC CIDRs 12.0.0.0/16
Peering connection status Pending Acceptance by 706436145460
Accepter VPC owner 706436145460
Accepter VPC ID vpc-7ac23b03
VPC Peering Connection pcx-b35225da
Expiration time July 9, 2017 at 7:54:04 AM UTC+5:30

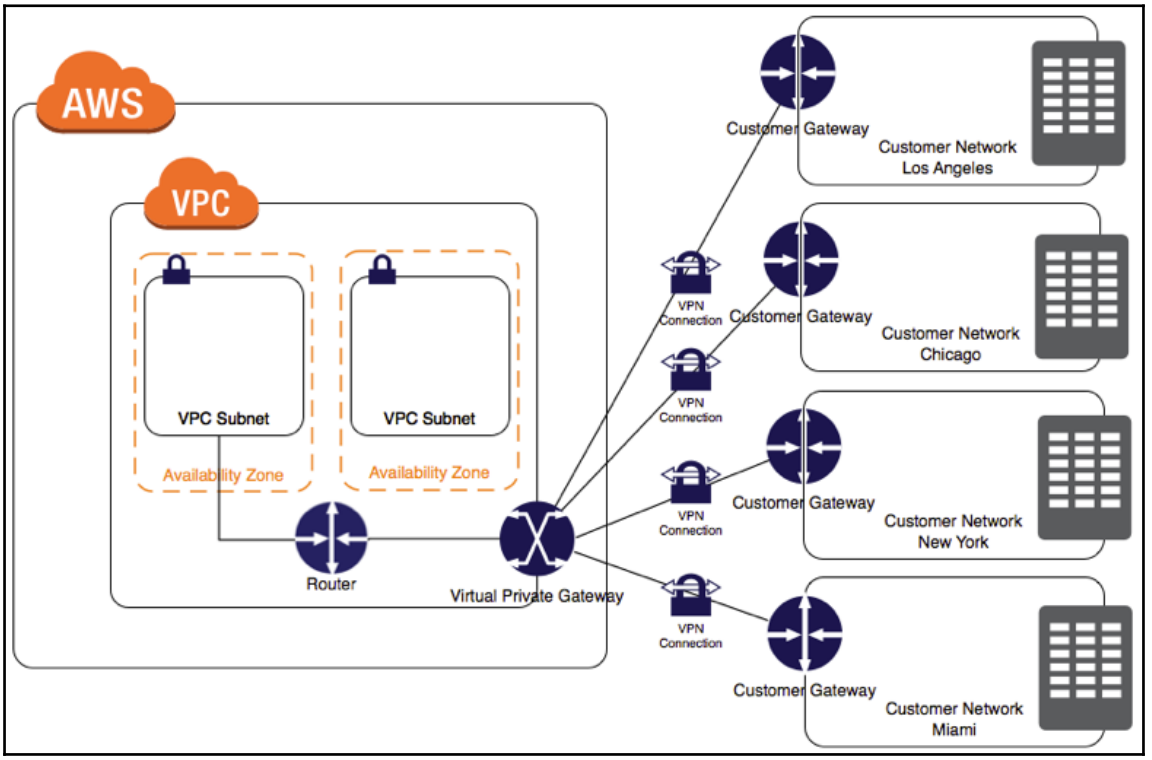

Accept VPC Peering Connection Request
Are you sure you want to accept this VPC peering connection request (pcx-b35225da)?
Requester Account ID 706436145460 (This account)
Requester VPC ID vpc-3eff7f47
Requester VPC CIDR 12.0.0.0/16
Accepter Account ID 706436145460 (This account)
Accepter VPC ID vpc-7ac23b03
Accepter VPC CIDR -
Cancel
Yes, Accept

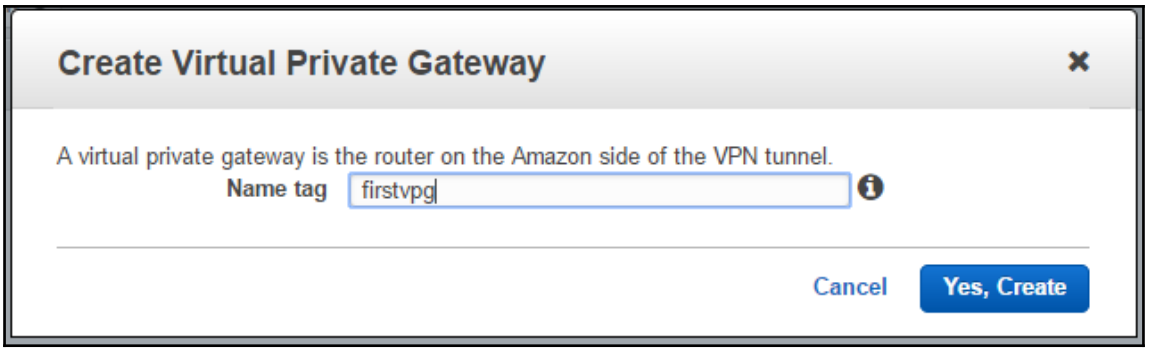

VPC Dashboard
Create Peering Connection
Actions
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Name
Peering Connectic
Status
Local VPC
Local VPC CIDRs
Requester Owner
Accepter Owner
Peered VPC
vpcpeering1
pcx-b35225da
Active
vpc-3eff7f47 | peeri..
12.0.0.0/16
706436145460
706436145460
vpc-7ac23b03 | VP...
Peering Connection: pcx-b35225da
Description
ClassicLink
DNS
Route Tables
Tags
Requester VPC owner 706436145460
Requester VPC ID vpc-3eff7f47
Local VPC CIDRs 12.0.0.0/16
Peering connection status Active
Accepter VPC owner 706436145460
Accepter VPC ID vpc-7ac23b03
VPC Peering Connection pcx-b35225da
Expiration time -

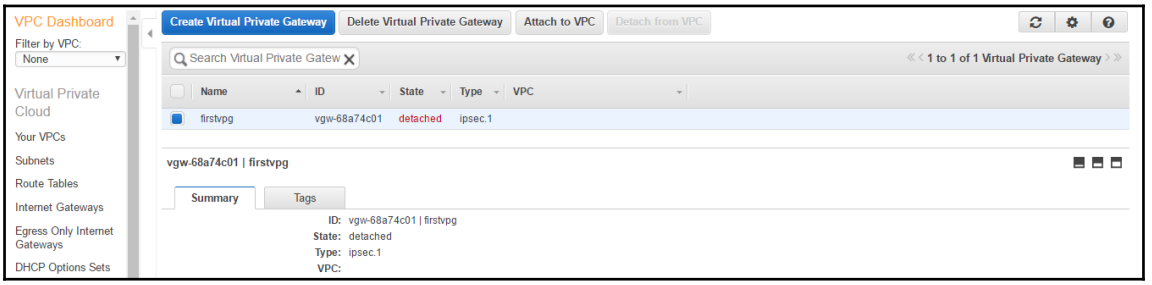

Peering Connections > Edit DNS Settings
Edit DNS Settings
The settings below control how your peered VPCs will work with DNS resolution
VPC Peering Connection pcx-b35225da
DNS resolution
Allow DNS resolution from peer VPC (vpc-3eff7f47) to private IP
Allow DNS resolution from local VPC (vpc-7ac23b03) to private IP
AWS Command Line Interface command
To use DNS resolution over peering you must enable 'DNS Hostname' on the VPCs involved in peering. Learn more
* Required
Cancel
Save


VPC Dashboard
Create Peering Connection
Actions
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Name
Peering Connectic
Status
Local VPC
Local VPC CIDRs
Requester Owner
Accepter Owner
Peered VPC
vpcpeering1
pcx-b35225da
Active
vpc-3eff7f47 | peeri..
12.0.0.0/16
706436145460
706436145460
vpc-7ac23b03 | VP...
Peering Connection: pcx-b35225da
Description
ClassicLink
DNS
Route Tables
Tags
Local VPC (vpc-3eff7f47) peering connection attributes
DNS resolution from peer VPC to private IP Enabled
Peered VPC (vpc-7ac23b03) peering connection attributes
DNS resolution from local VPC to private IP Enabled

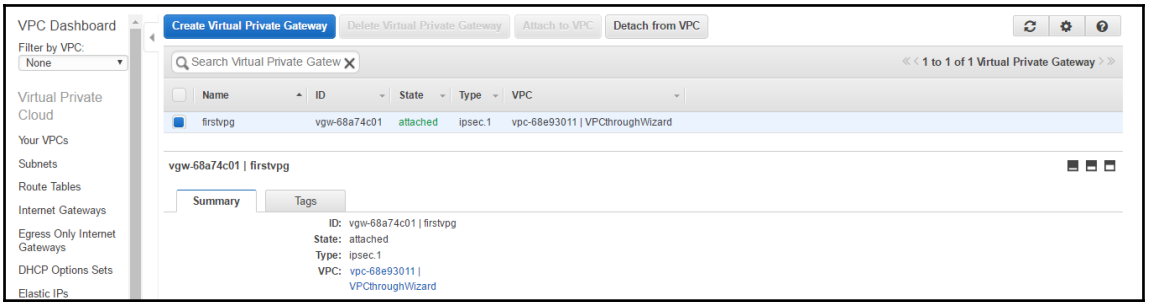

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
rtb-f542098d
1 to 1 of 1 Route Table
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-f542098d
0 Subnets
Yes
vpc-3eff7f47 | peeringvpc
rtb-f542098d
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
12.0.0.0/16
local
Active
No
10.0.0.0/16
pcx-b35225da
No
Add another route

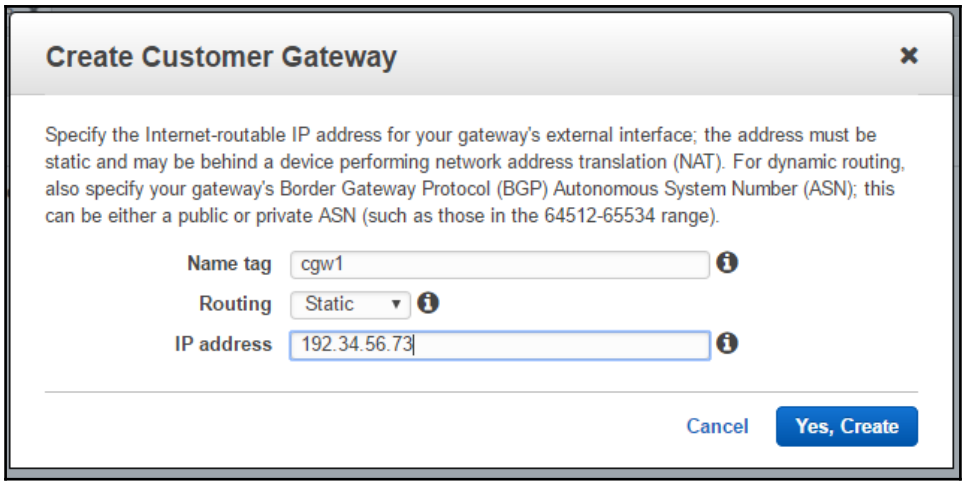

AWS
VPC
VPC Subnet
VPC Subnet
Availability Zone
Availability Zone
Router
Virtual Private Gateway
VPN Connection
VPN Connection
VPN Connection
VPN Connection
Customer Gateway
Customer Gateway
Customer Gateway
Customer Gateway
Customer Network Los Angeles
Customer Network Chicago
Customer Network New York
Customer Network Miami


Create Virtual Private Gateway
A virtual private gateway is the router on the Amazon side of the VPN tunnel.
Name tag
firstvpg
Cancel
Yes, Create

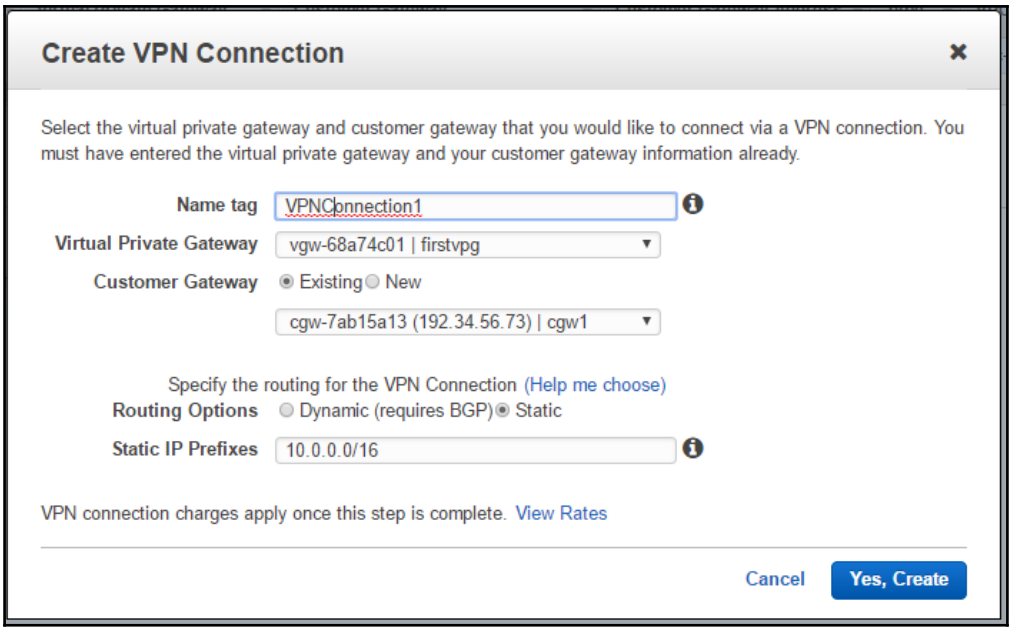

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Create Virtual Private Gateway
Delete Virtual Private Gateway
Attach to VPC
Detach from VPC
Search Virtual Private Gatew
1 to 1 of 1 Virtual Private Gateway
Name
ID
State
Type
VPC
firstvpg
vgw-68a74c01
detached
ipsec.1
vgw-68a74c01 | firstvpg
Summary
Tags
ID: vgw-68a74c01 | firstvpg
State: detached
Type: ipsec.1
VPC:

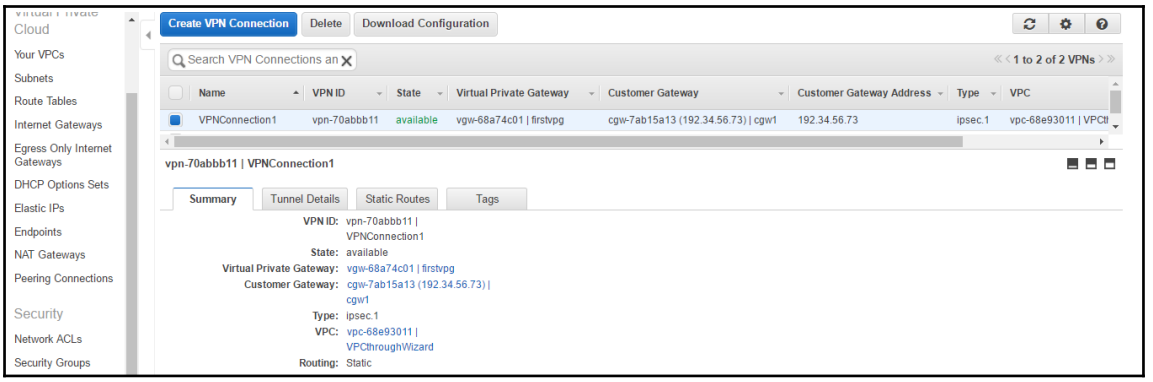
Attach to VPC
Select the VPC to attach to the virtual private gateway
VPC
vpc-68e93011 | VPCthroughWizard
Cancel
Yes, Attach


VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create Virtual Private Gateway
Delete Virtual Private Gateway
Attach to VPC
Detach from VPC
Search Virtual Private Gatew
1 to 1 of 1 Virtual Private Gateway
Name
ID
State
Type
VPC
firstvpg
vgw-68a74c01
attached
ipsec.1
vpc-68e93011 | VPCthroughWizard
vgw-68a74c01 | firstvpg
Summary
Tags
ID: vgw-68a74c01 | firstvpg
State: attached
Type: ipsec.1
VPC: vpc-68e93011 | VPCthroughWizard


Create Customer Gateway
Specify the Internet-routable IP address for your gateway's external interface; the address must be static and may be behind a device performing network address translation (NAT). For dynamic routing, also specify your gateway's Border Gateway Protocol (BGP) Autonomous System Number (ASN); this can be either a public or private ASN (such as those in the 64512-65534 range).
Name tag
cgw1
Routing
Static
IP address
192.34.56.73
Cancel
Yes, Create

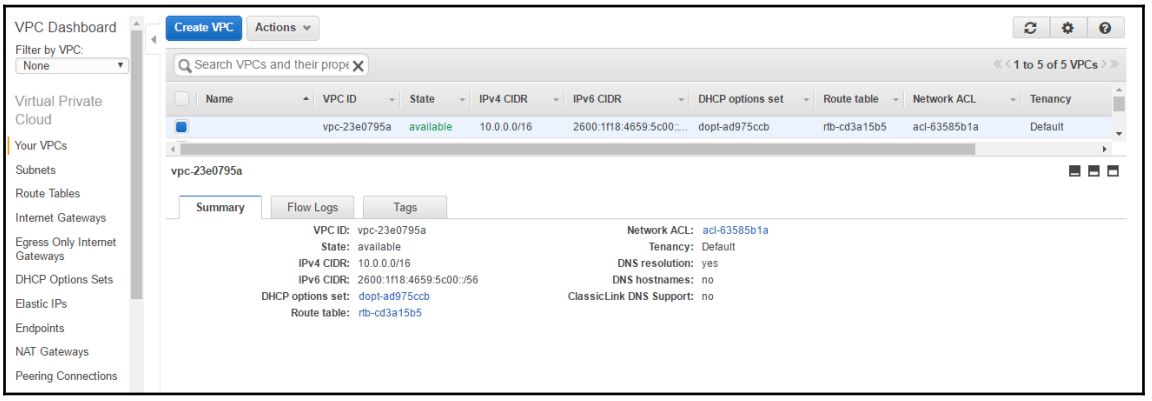
Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Create Customer Gateway
Delete Customer Gateway
Search Customer Gateways
1 to 1 of 1 Customer Gateway
Name
ID
State
Type
IP Address
BGP ASN
VPC
cgw1
cgw-7ab15a13
available
ipsec.1
192.34.56.73
65000
cgw-7ab15a13 (192.34.56.73) | cgw1
Summary
Tags
ID: cgw-7ab15a13 (192.34.56.73) | cgw1
State: available
Type: ipsec.1
IP address: 192.34.56.73
BGP ASN: 65000
VPC:


Create VPN Connection
Select the virtual private gateway and customer gateway that you would like to connect via a VPN connection. You must have entered the virtual private gateway and your customer gateway information already.
Name tag
VPNConnection1
Virtual Private Gateway
vgw-68a74c01 | firstvpg
Customer Gateway
Existing
New
cgw-7ab15a13 (192.34.56.73) | cgw1
Specify the routing for the VPN Connection (Help me choose)
Routing Options
Dynamic (requires BGP)
Static
Static IP Prefixes
10.0.0.0/16
VPN connection charges apply once this step is complete. View Rates
Cancel
Yes, Create

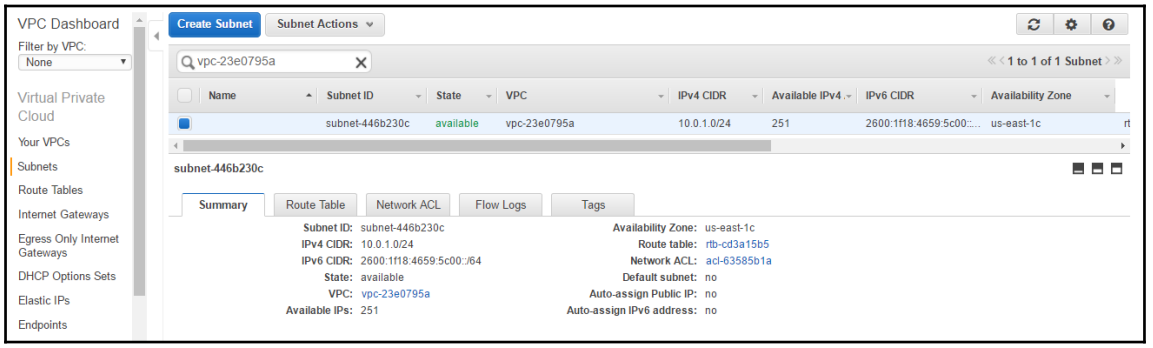

Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create VPN Connection
Delete
Download Configuration
Search VPN Connections an
1 to 2 of 2 VPNs
Name
VPN ID
State
Virtual Private Gateway
Customer Gateway
Customer Gateway Address
Type
VPC
VPNConnection1
vpn-70abbb11
available
vgw-68a74c01 | firstvpg
cgw-7ab15a13 (192.34.56.73) | cgw1
192.34.56.73
ipsec.1
vpc-68e93011 | VPCtl
vpn-70abbb11 | VPNConnection1
Summary
Tunnel Details
Static Routes
Tags
VPN ID: vpn-70abbb11 | VPNConnection1
State: available
Virtual Private Gateway: vgw-68a74c01 | firstvpg
Customer Gateway: cgw-7ab15a13 (192.34.56.73) | cgw1
Type: ipsec.1
VPC: vpc-68e93011 | VPCthroughWizard
Routing: Static

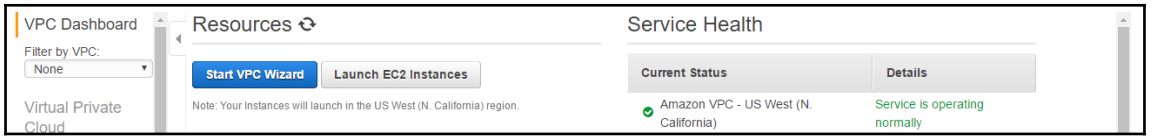
Chapter 4: Configuring Global Scale Infrastructure

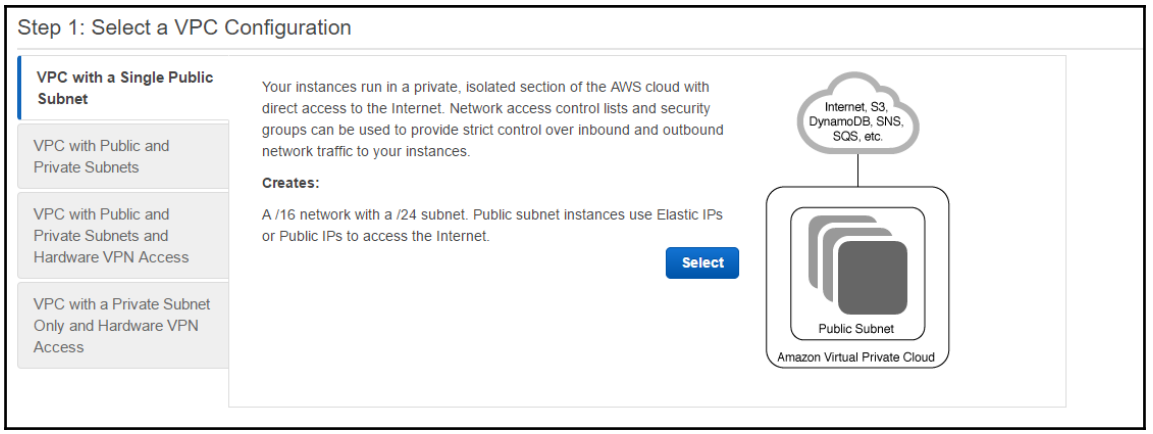
```
D:\>aws ec2 create-vpc --profile user2 --region us-east-1 --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
{
    "Vpc": {
        "VpcId": "vpc-23e0795a",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [
            {
                "Ipv6CidrBlock": "",
                "AssociationId": "vpc-cidr-assoc-039f0b68",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                }
            }
        ],
        "State": "pending",
        "DhcpOptionsId": "dopt-ad975ccb",
        "CidrBlock": "10.0.0.0/16",
        "IsDefault": false
    }
}
```

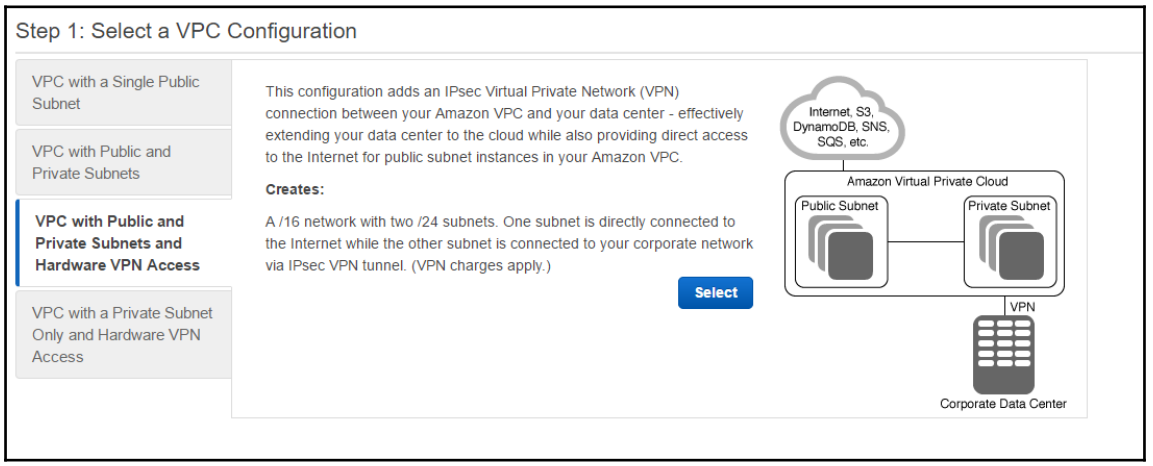


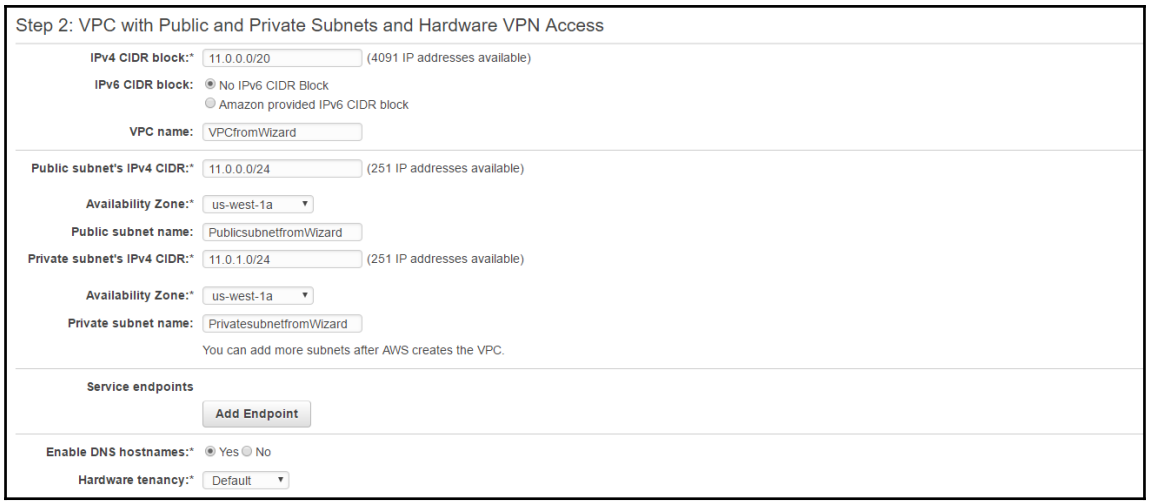
```
D:\>aws ec2 create-subnet --profile user2 --region us-east-1 --vpc-id vpc-23e0795a --cidr-block 10.0.1.0/24 --ipv6-cid
r-block 2600:1f18:4659:5c00::/64
{
    "Subnet": {
        "VpcId": "vpc-23e0795a",
        "AvailableIpAddressCount": 251,
        "MapPublicIpOnLaunch": false,
        "DefaultForAz": false,
        "Ipv6CidrBlockAssociationSet": [
            {
                "Ipv6CidrBlock": "2600:1f18:4659:5c00::/64",
                "AssociationId": "subnet-cidr-assoc-96133cdc",
                "Ipv6CidrBlockState": {
                    "State": "associating"
                }
            }
        ],
        "State": "pending",
        "AvailabilityZone": "us-east-1c",
        "SubnetId": "subnet-446b230c",
        "CidrBlock": "10.0.1.0/24",
        "AssignIpv6AddressOnCreation": false
    }
}

D:\>
```



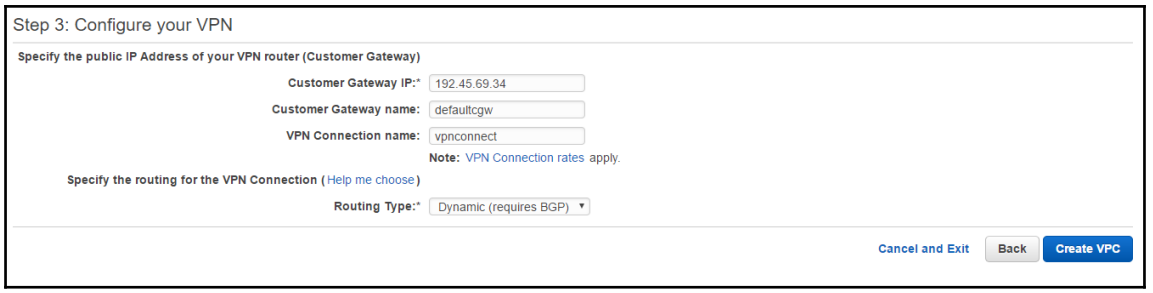


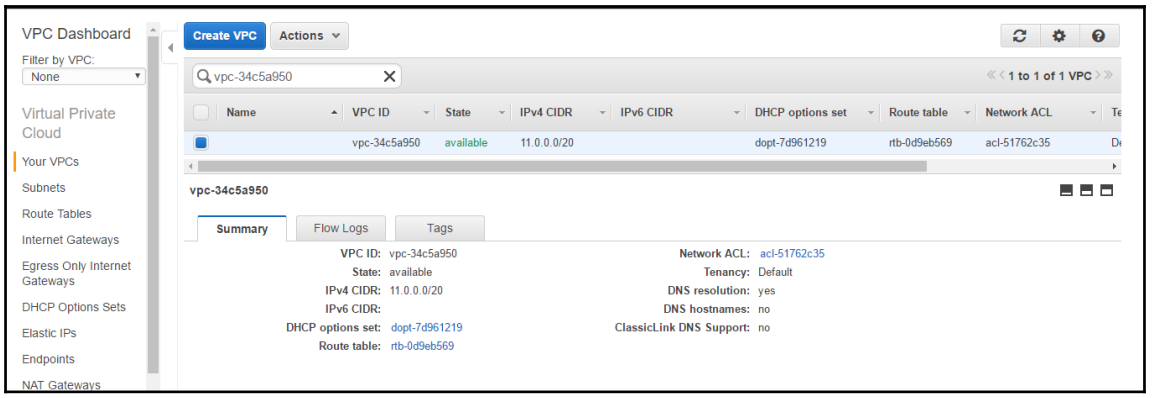

Step 1: Select a VPC Configuration
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Your instances run in a private, isolated section of the AWS cloud with direct access 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.
Creates:
A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.
Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Public Subnet
Amazon Virtual Private Cloud

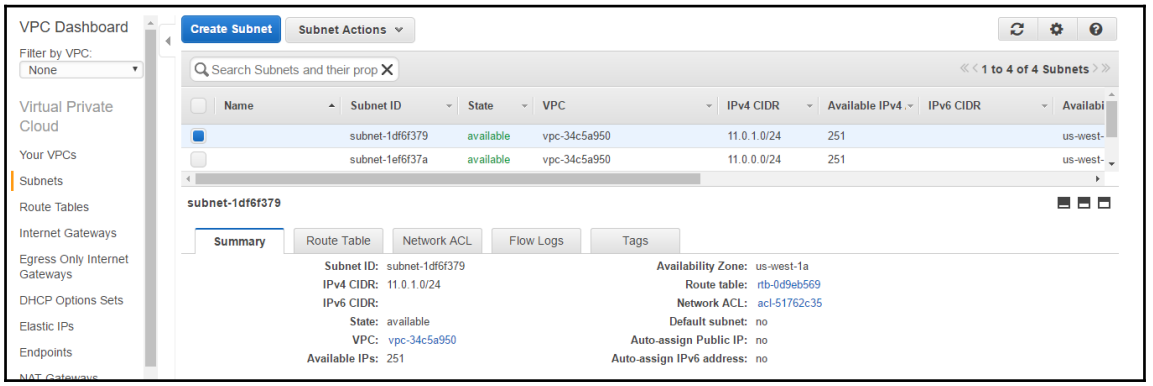

Step 1: Select a VPC Configuration
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
This configuration adds an IPsec Virtual Private Network (VPN) connection between your Amazon VPC and your data center - effectively extending your data center to the cloud while also providing direct access to the Internet for public subnet instances in your Amazon VPC.
Creates:
A /16 network with two /24 subnets. One subnet is directly connected to the Internet while the other subnet is connected to your corporate network via IPsec VPN tunnel. (VPN charges apply.)
Select
Internet, S3, DynamoDB, SNS, SQS, etc.
Amazon Virtual Private Cloud
Public Subnet
Private Subnet
VPN
Corporate Data Center

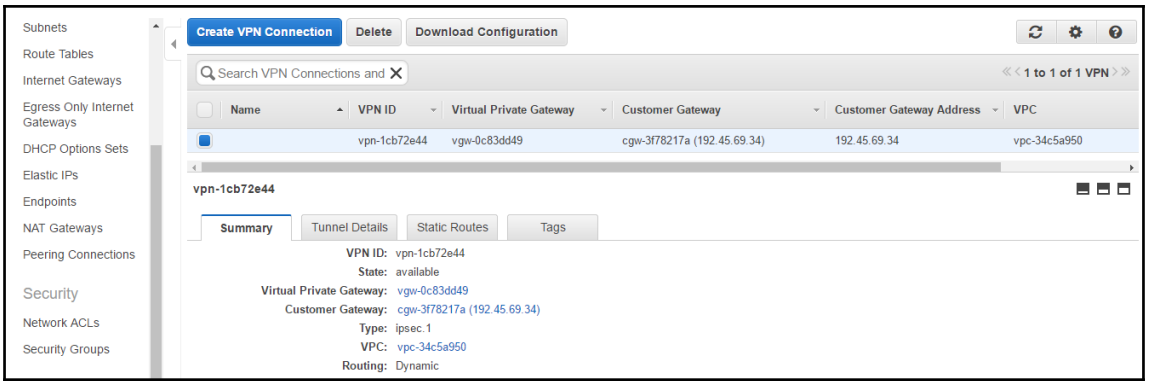

Step 2: VPC with Public and Private Subnets and Hardware VPN Access
IPv4 CIDR block:*
11.0.0.0/20
(4091 IP addresses available)
IPv6 CIDR block:
No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
VPC name:
VPCfromWizard
Public subnet's IPv4 CIDR:*
11.0.0.0/24
(251 IP addresses available)
Availability Zone:*
us-west-1a
Public subnet name:
PublicsubnetfromWizard
Private subnet's IPv4 CIDR:*
11.0.1.0/24
(251 IP addresses available)
Availability Zone:*
us-west-1a
Private subnet name:
PrivatesubnetfromWizard
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:*
Yes
No
Hardware tenancy:*
Default

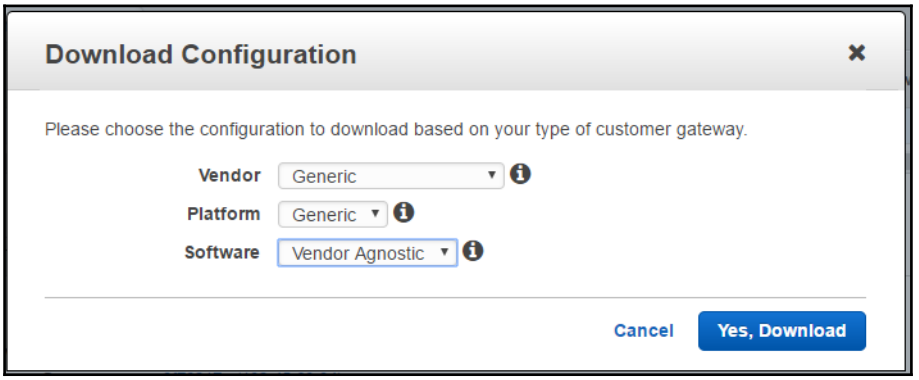
Service endpoints
Service
com.amazonaws.us-west-1.s3
Subnet
Public and Private subnets
Policy*
Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies — IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) — must grant the necessary permissions for access to succeed.
Custom
Use the policy creation tool to generate a policy, then paste the generated policy below.
{
"Statement": [
{
"Action": "*",
"Effect": "Allow",
"Resource": "*",
"Principal": "*"
}
]
}
Add Endpoint
Enable DNS hostnames:*
Yes
No
Hardware tenancy:*
Default

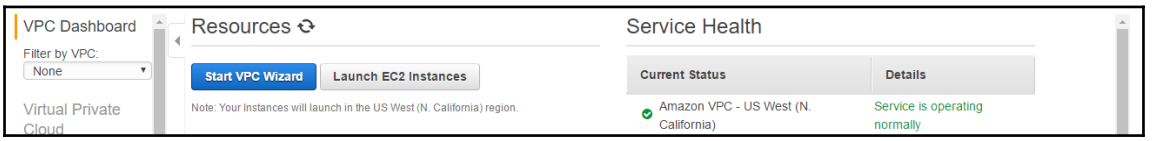

Step 3: Configure your VPN
Specify the public IP Address of your VPN router (Customer Gateway)
Customer Gateway IP:* 192.45.69.34
Customer Gateway name: defaultcgw
VPN Connection name: vpnconnect
Note: VPN Connection rates apply.
Specify the routing for the VPN Connection (Help me choose)
Routing Type:* Dynamic (requires BGP)
Cancel and Exit
Back
Create VPC

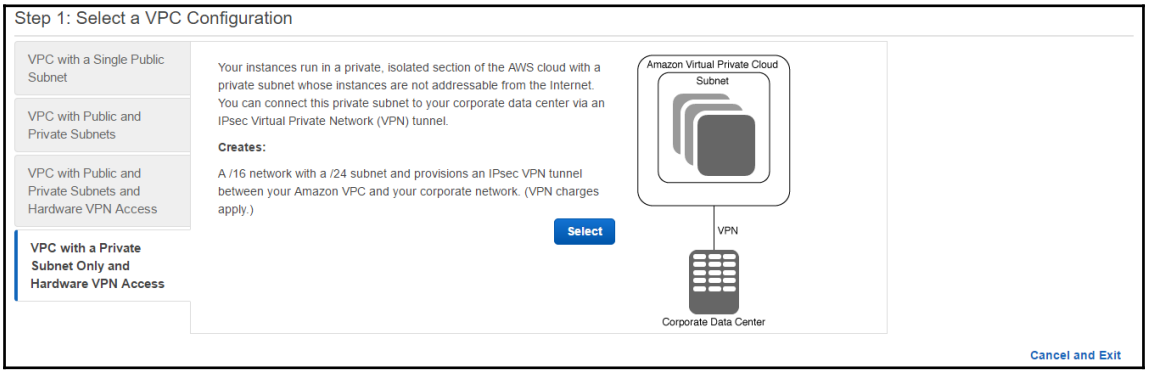

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create VPC
Actions
vpc-34c5a950
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
vpc-34c5a950
available
11.0.0.0/20
dopt-7d961219
rtb-0d9eb569
acl-51762c35
vpc-34c5a950
Summary
Flow Logs
Tags
VPC ID: vpc-34c5a950
State: available
IPv4 CIDR: 11.0.0.0/20
IPv6 CIDR:
DHCP options set: dopt-7d961219
Route table: rtb-0d9eb569
Network ACL: acl-51762c35
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
ClassicLink DNS Support: no


VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 4 of 4 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
subnet-1df6f379
available
vpc-34c5a950
11.0.1.0/24
251
subnet-1ef6f37a
available
vpc-34c5a950
11.0.0.0/24
251
subnet-1df6f379
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-1df6f379
IPv4 CIDR: 11.0.1.0/24
IPv6 CIDR:
State: available
VPC: vpc-34c5a950
Available IPs: 251
Availability Zone: us-west-1a
Route table: rtb-0d9eb569
Network ACL: acl-51762c35
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no


Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create VPN Connection
Delete
Download Configuration
Search VPN Connections and
1 to 1 of 1 VPN
Name
VPN ID
Virtual Private Gateway
Customer Gateway
Customer Gateway Address
VPC
vpn-1cb72e44
vgw-0c83dd49
cgw-3f78217a (192.45.69.34)
192.45.69.34
vpc-34c5a950
vpn-1cb72e44
Summary
Tunnel Details
Static Routes
Tags
VPN ID: vpn-1cb72e44
State: available
Virtual Private Gateway: vgw-0c83dd49
Customer Gateway: cgw-3f78217a (192.45.69.34)
Type: ipsec.1
VPC: vpc-34c5a950
Routing: Dynamic

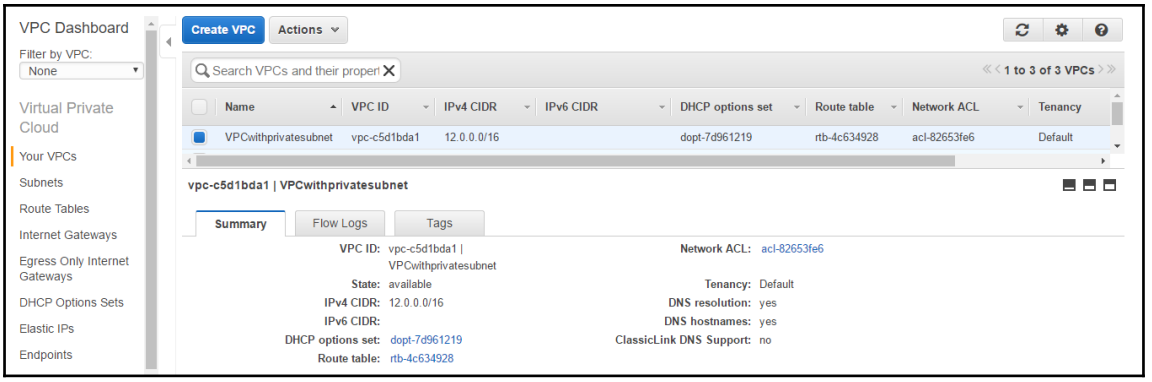

Download Configuration
Please choose the configuration to download based on your type of customer gateway.
Vendor
Generic
Platform
Generic
Software
Vendor Agnostic
Cancel
Yes, Download

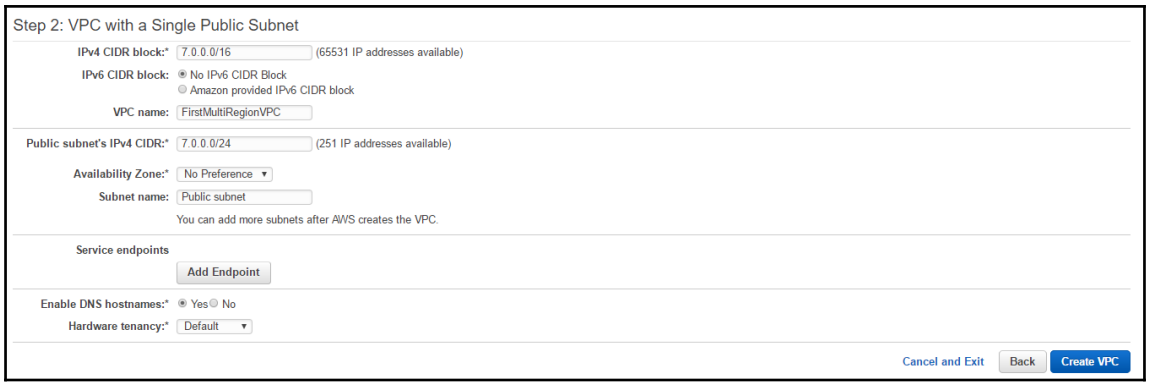

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Resources
Start VPC Wizard
Launch EC2 Instances
Note: Your instances will launch in the US West (N. California) region.
Service Health
Current Status
Details
Amazon VPC - US West (N. California)
Service is operating normally


Step 1: Select a VPC Configuration
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
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 data center via an IPsec Virtual Private Network (VPN) tunnel.
Creates:
A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)
Select
Amazon Virtual Private Cloud
Subnet
VPN
Corporate Data Center
Cancel and Exit

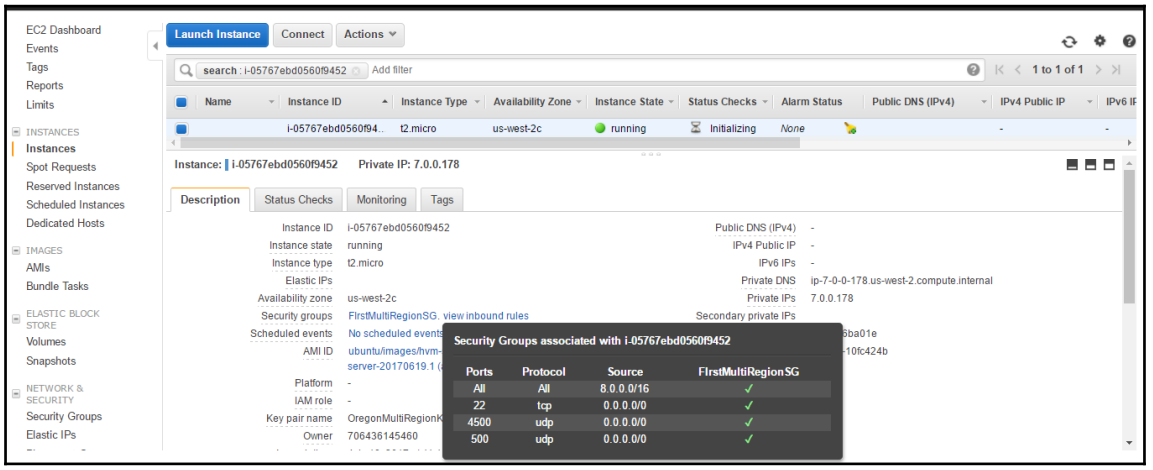
Step 2: VPC with a Private Subnet Only and Hardware VPN Access
IPv4 CIDR block:* 12.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
VPC name: VPCwithprivatesubnet
Private subnet's IPv4 CIDR:* 12.0.1.0/24 (251 IP addresses available)
Availability Zone:* us-west-1a
Private subnet name: Privatesubnet2
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Next

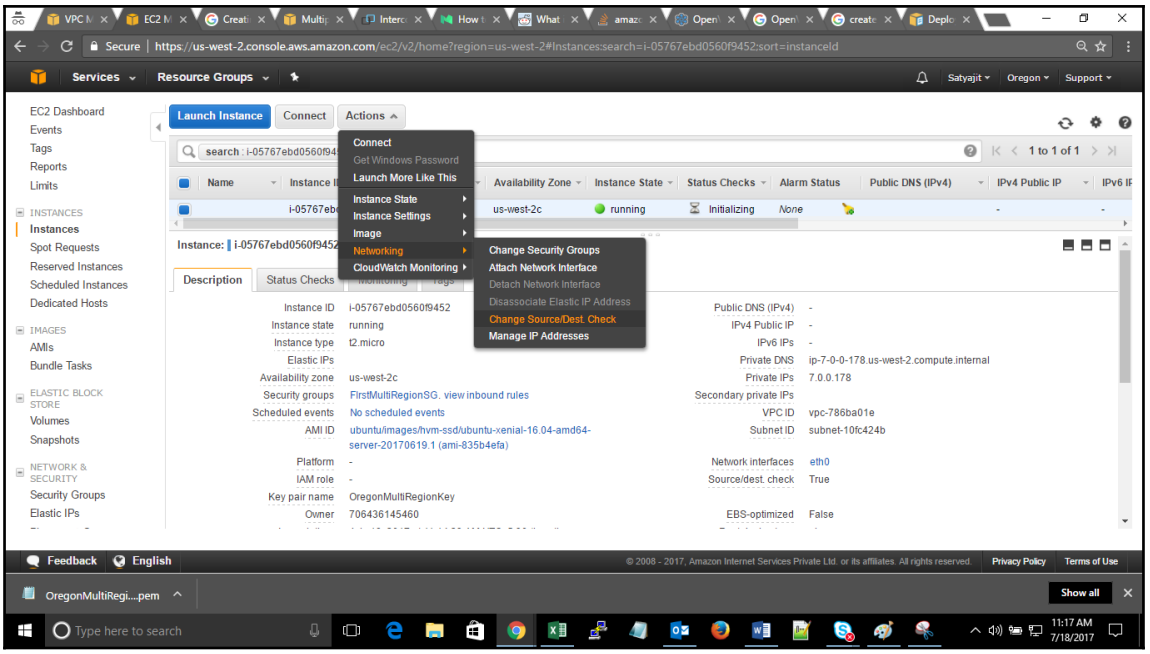
Step 3: Configure your VPN
Specify the public IP Address of your VPN router (Customer Gateway)
Customer Gateway IP:* 196.34.23.12
Customer Gateway name: cgw2
VPN Connection name: vpn2
Note: VPN Connection rates apply.
Specify the routing for the VPN Connection (Help me choose)
Routing Type:* Dynamic (requires BGP)
Cancel and Exit
Back
Create VPC

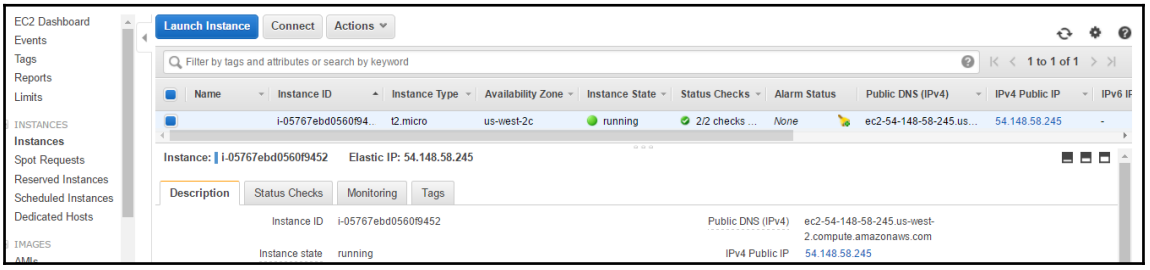

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create VPC
Actions
Search VPCs and their proper
1 to 3 of 3 VPCs
Name
VPC ID
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCwithprivatesubnet
vpc-c5d1bda1
12.0.0.0/16
dopt-7d961219
rtb-4c634928
acl-82653fe6
Default
vpc-c5d1bda1 | VPCwithprivatesubnet
Summary
Flow Logs
Tags
VPC ID: vpc-c5d1bda1 | VPCwithprivatesubnet
State: available
IPv4 CIDR: 12.0.0.0/16
IPv6 CIDR:
DHCP options set: dopt-7d961219
Route table: rtb-4c634928
Network ACL: acl-82653fe6
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

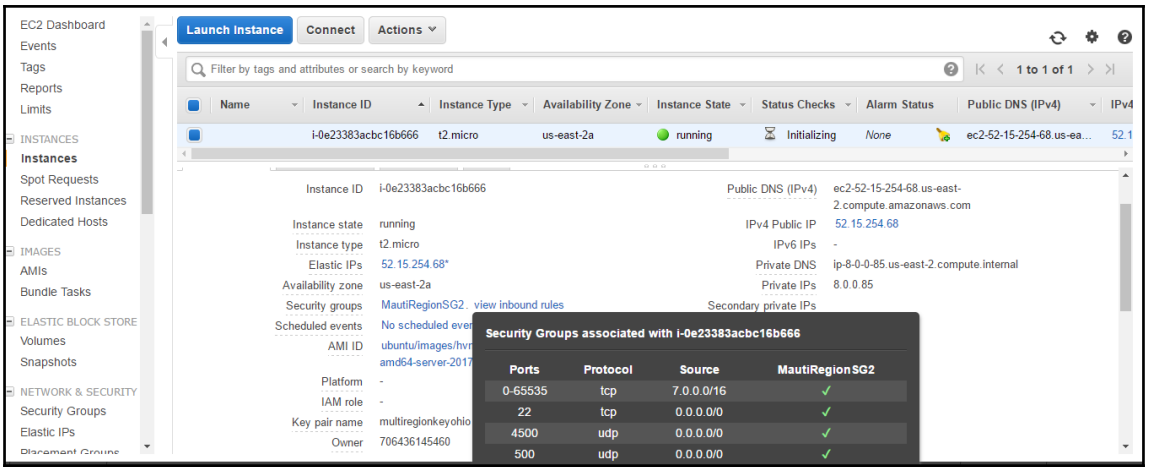

Step 2: VPC with a Single Public Subnet
IPv4 CIDR block:* 7.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
VPC name: FirstMultiRegionVPC
Public subnet's IPv4 CIDR:* 7.0.0.0/24 (251 IP addresses available)
Availability Zone:* No Preference
Subnet name: Public subnet
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Create VPC

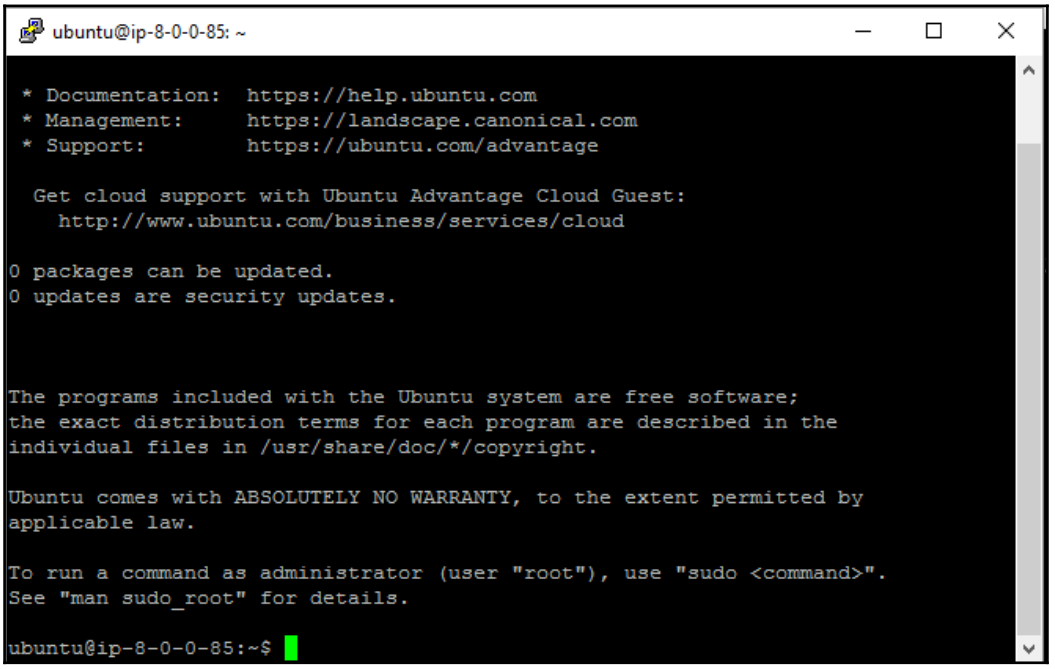
Step 2: VPC with a Single Public Subnet
IPv4 CIDR block:* 8.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: No IPv6 CIDR Block
Amazon provided IPv6 CIDR block
VPC name: SecondMultiRegionVPC
Public subnet's IPv4 CIDR:* 8.0.0.0/24 (251 IP addresses available)
Availability Zone:* No Preference
Subnet name: Public subnet
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames:* Yes No
Hardware tenancy:* Default
Cancel and Exit
Back
Create VPC


EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Launch Instance
Connect
Actions
search : i-05767ebd0560f9452
Add filter
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
i-05767ebd0560f94..
t2.micro
us-west-2c
running
Initializing
None
Instance: i-05767ebd0560f9452 Private IP: 7.0.0.178
Description
Status Checks
Monitoring
Tags
Instance ID i-05767ebd0560f9452
Instance state running
Instance type t2.micro
Elastic IPs
Availability zone us-west-2c
Security groups FirstMultiRegionSG. view inbound rules
Scheduled events No scheduled events
AMI ID ubuntu/images/hvm-ssd/ubuntu-xenial-16.04-amd64-server-20170619.1
Platform -
IAM role -
Key pair name OregonMultiRegionK
Owner 706436145460
Public DNS (IPv4) -
IPv4 Public IP -
IPv6 IPs -
Private DNS ip-7-0-0-178.us-west-2.compute.internal
Private IPs 7.0.0.178
Secondary private IPs
Security Groups associated with i-05767ebd0560f9452
Ports Protocol Source FirstMultiRegionSG
All All 8.0.0.0/16
22 tcp 0.0.0.0/0
4500 udp 0.0.0.0/0
500 udp 0.0.0.0/0

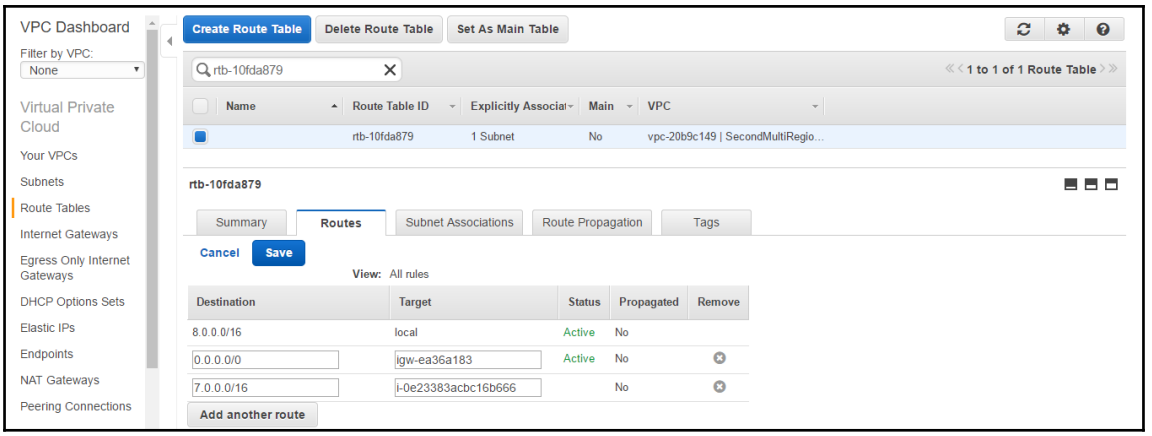

Launch Instance
Connect
Actions
Connect
Get Windows Password
Launch More Like This
Instance State
Instance Settings
Image
Networking
CloudWatch Monitoring
Change Security Groups
Attach Network Interface
Detach Network Interface
Disassociate Elastic IP Address
Change Source/Dest. Check
Manage IP Addresses
Description
Status Checks
Monitoring
Tags

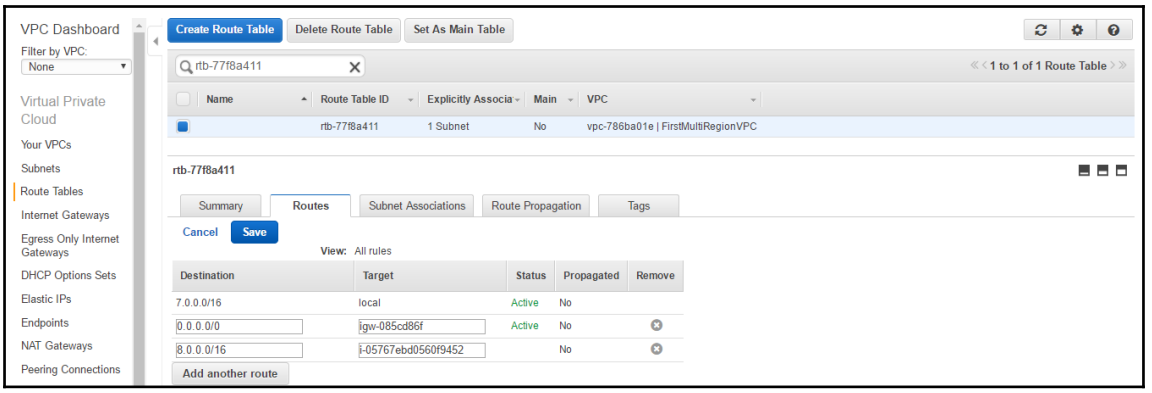

Launch Instance
Connect
Actions
Description
Status Checks
Monitoring
Tags

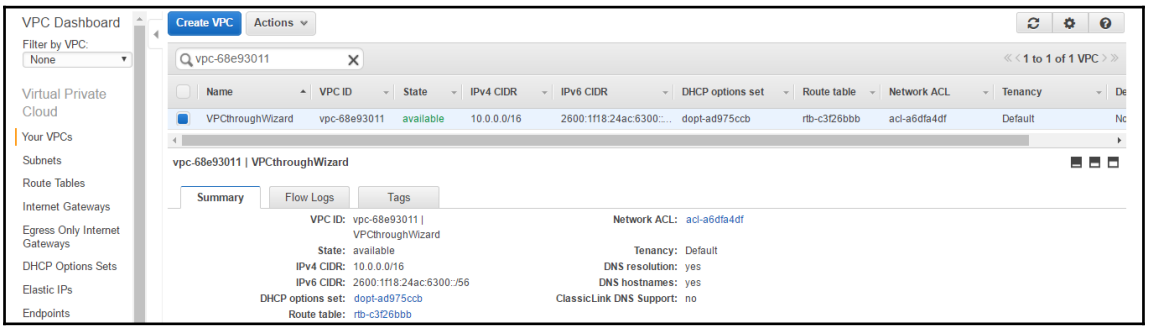


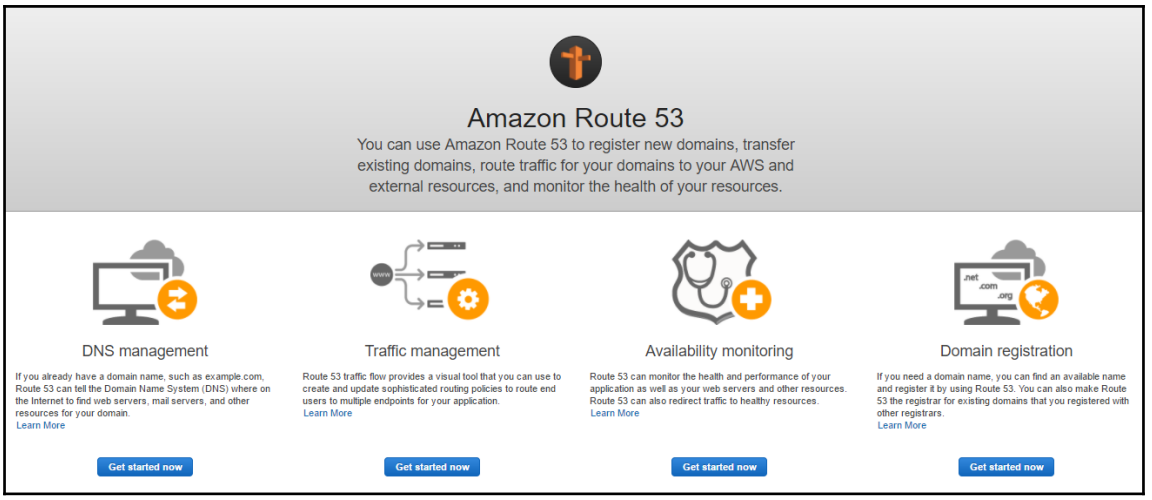


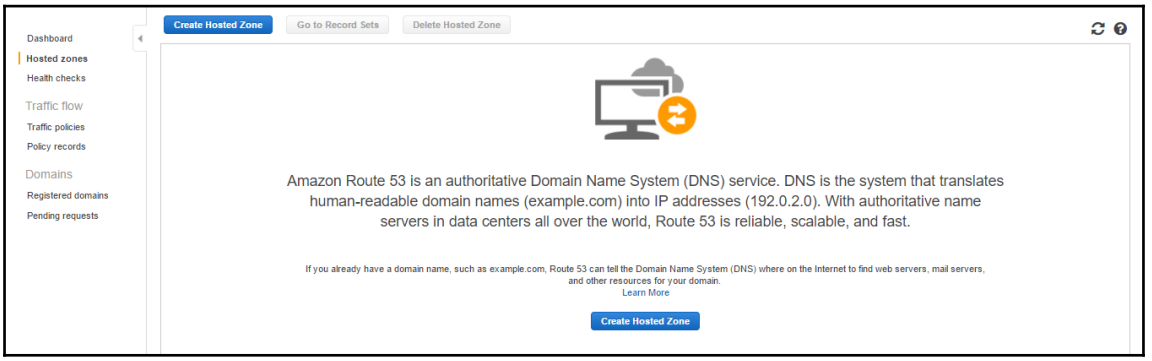

```
ubuntu@ip-8-0-0-85:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

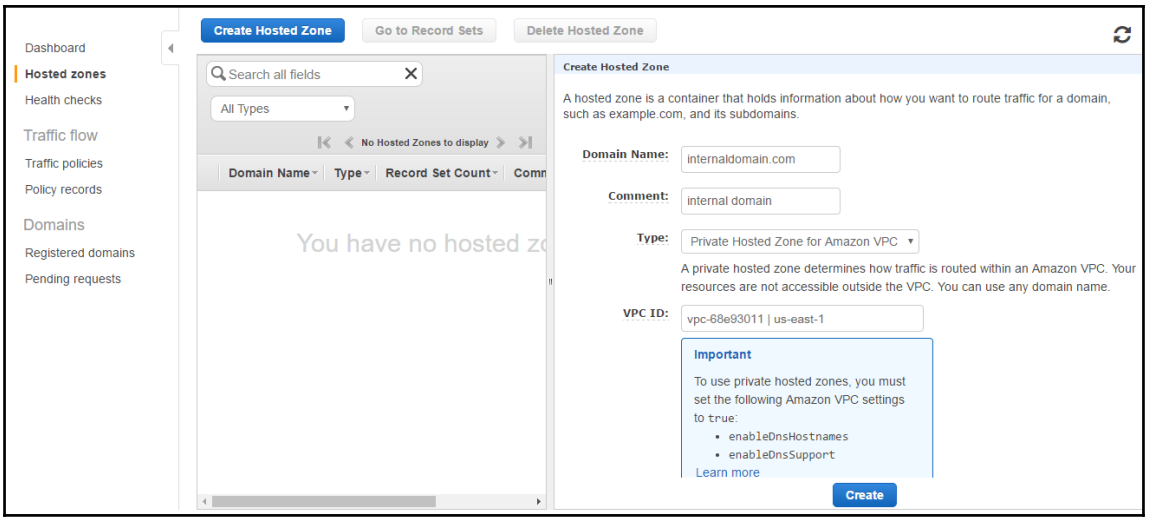

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
rtb-10fda879
1 to 1 of 1 Route Table
Name
Route Table ID
Explicitly Associat
Main
VPC
rtb-10fda879
1 Subnet
No
vpc-20b9c149 | SecondMultiRegio...
rtb-10fda879
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
8.0.0.0/16
local
Active
No
0.0.0.0/0
igw-ea36a183
Active
No
7.0.0.0/16
i-0e23383acbc16b666
No
Add another route

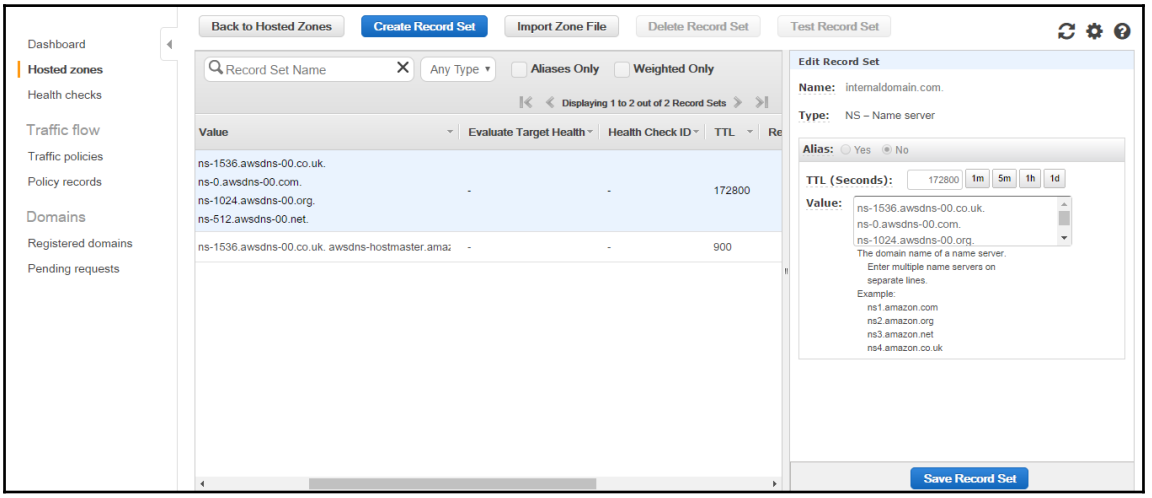

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create Route Table
Delete Route Table
Set As Main Table
rtb-77f8a411
1 to 1 of 1 Route Table
Name
Route Table ID
Explicitly Associa
Main
VPC
rtb-77f8a411
1 Subnet
No
vpc-786ba01e | FirstMultiRegionVPC
rtb-77f8a411
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
7.0.0.0/16
local
Active
No
0.0.0.0/0
igw-085cd86f
Active
No
8.0.0.0/16
i-05767ebd0560f9452
No
Add another route

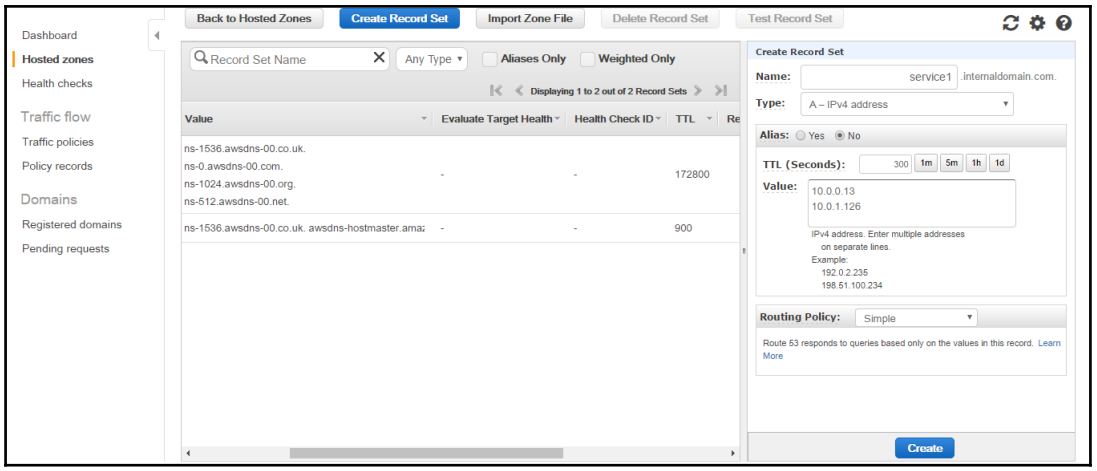

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create VPC
Actions
vpc-68e93011
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCthroughWizard
vpc-68e93011
available
10.0.0.0/16
2600:1f18:24ac:6300:...
dopt-ad975ccb
rtb-c3f26bbb
acl-a6dfa4df
Default
vpc-68e93011 | VPCthroughWizard
Summary
Flow Logs
Tags
VPC ID: vpc-68e93011 | VPCthroughWizard
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR: 2600:1f18:24ac:6300::/56
DHCP options set: dopt-ad975ccb
Route table: rtb-c3f26bbb
Network ACL: acl-a6dfa4df
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

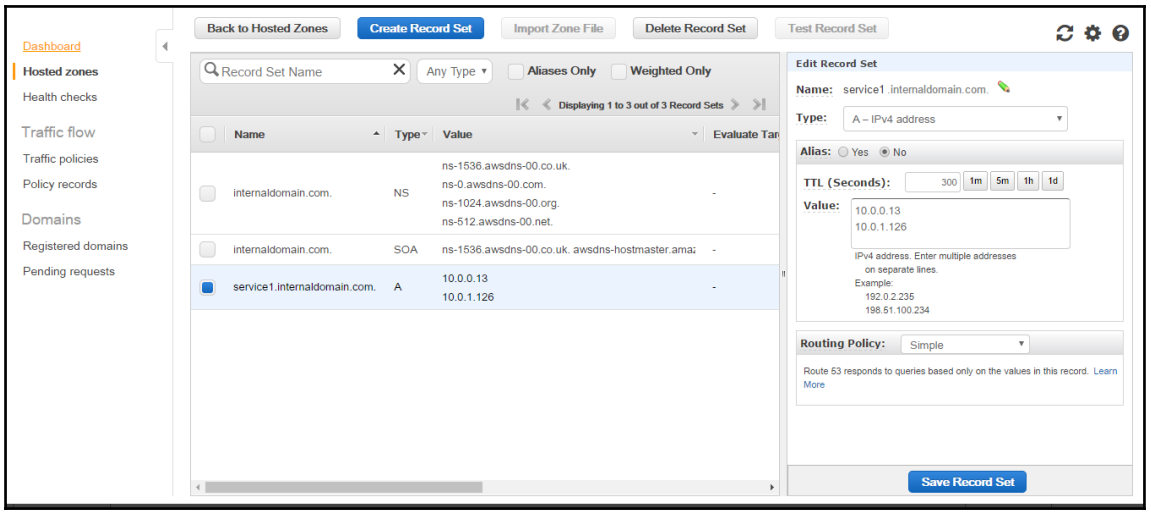

Amazon Route 53
You can use Amazon Route 53 to register new domains, transfer existing domains, route traffic for your domains to your AWS and external resources, and monitor the health of your resources.
DNS management
If you already have a domain name, such as example.com, Route 53 can tell the Domain Name System (DNS) where on the Internet to find web servers, mail servers, and other resources for your domain.
Learn More
Get started now
Traffic management
Route 53 traffic flow provides a visual tool that you can use to create and update sophisticated routing policies to route end users to multiple endpoints for your application.
Learn More
Get started now
Availability monitoring
Route 53 can monitor the health and performance of your application as well as your web servers and other resources. Route 53 can also redirect traffic to healthy resources.
Learn More
Get started now
Domain registration
If you need a domain name, you can find an available name and register it by using Route 53. You can also make Route 53 the registrar for existing domains that you registered with other registrars.
Learn More
Get started now

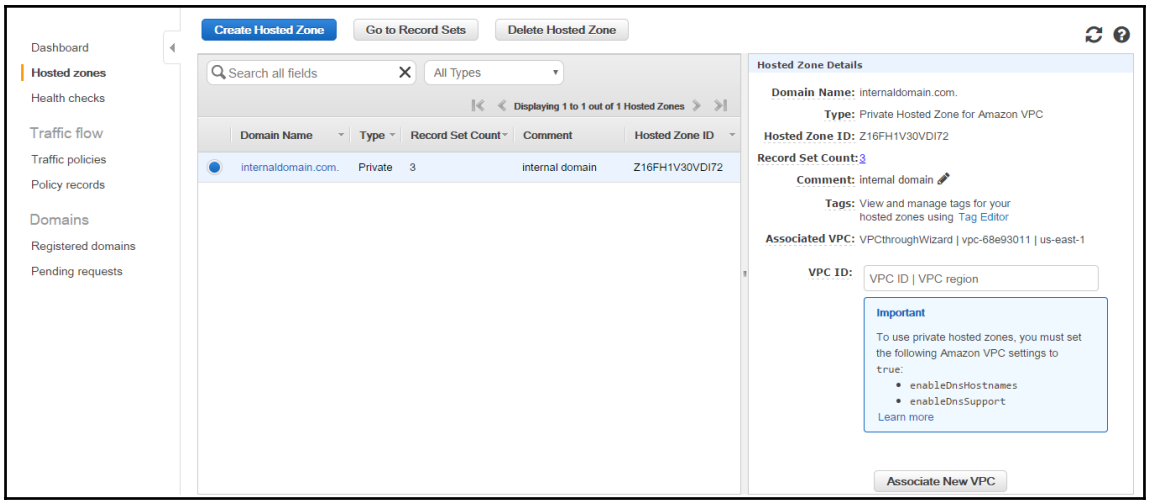

Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Amazon Route 53 is an authoritative Domain Name System (DNS) service. DNS is the system that translates human-readable domain names (example.com) into IP addresses (192.0.2.0). With authoritative name servers in data centers all over the world, Route 53 is reliable, scalable, and fast.
If you already have a domain name, such as example.com, Route 53 can tell the Domain Name System (DNS) where on the Internet to find web servers, mail servers, and other resources for your domain.
Learn More
Create Hosted Zone

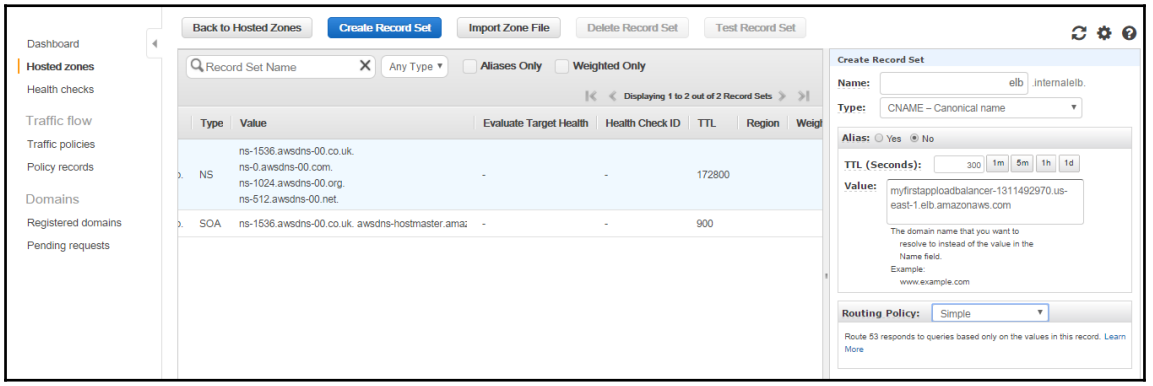

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Search all fields
All Types
No Hosted Zones to display
Domain Name
Type
Record Set Count
You have no hosted zo
Create Hosted Zone
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.
Domain Name:
internaldomain.com
Comment:
internal domain
Type:
Private Hosted Zone for Amazon VPC
A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.
VPC ID:
vpc-68e93011 | us-east-1
Important
To use private hosted zones, you must set the following Amazon VPC settings to true:
enableDnsHostnames
enableDnsSupport
Learn more
Create

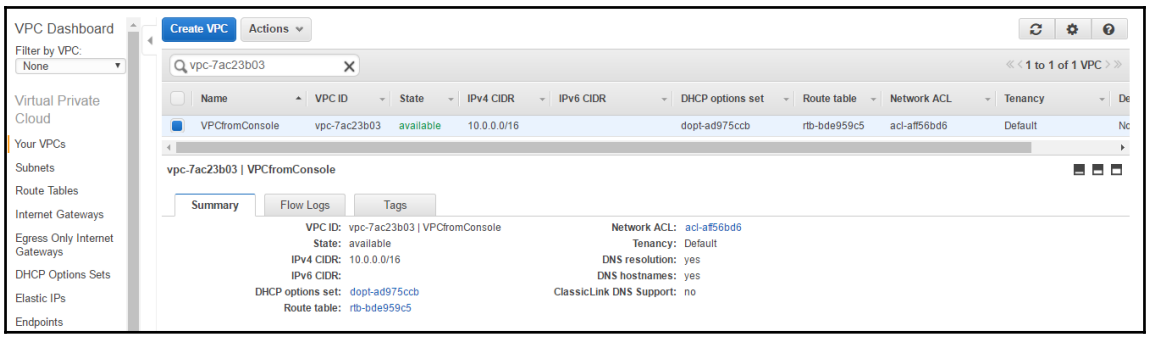

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Test Record Set
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 2 out of 2 Record Sets
Value
Evaluate Target Health
Health Check ID
TTL
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
ns-512.awsdns-00.net.
172800
ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz
900
Edit Record Set
Name: internaldomain.com.
Type: NS – Name server
Alias: Yes No
TTL (Seconds): 172800 1m 5m 1h 1d
Value:
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
The domain name of a name server.
Enter multiple name servers on separate lines.
Example:
ns1.amazon.com
ns2.amazon.org
ns3.amazon.net
ns4.amazon.co.uk
Save Record Set

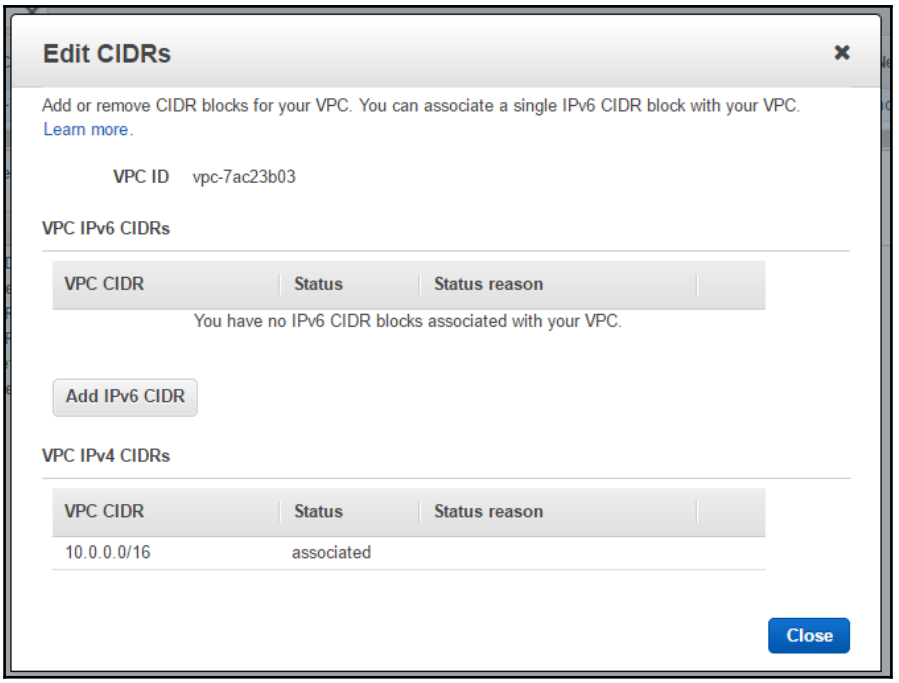

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Test Record Set
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 2 out of 2 Record Sets
Value
Evaluate Target Health
Health Check ID
TTL
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
ns-512.awsdns-00.net.
172800
ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz
900
Create Record Set
Name:
service1
.internaldomain.com.
Type:
A – IPv4 address
Alias:
Yes
No
TTL (Seconds):
300
1m
5m
1h
1d
Value:
10.0.0.13
10.0.1.126
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234
Routing Policy:
Simple
Route 53 responds to queries based only on the values in this record. Learn More
Create

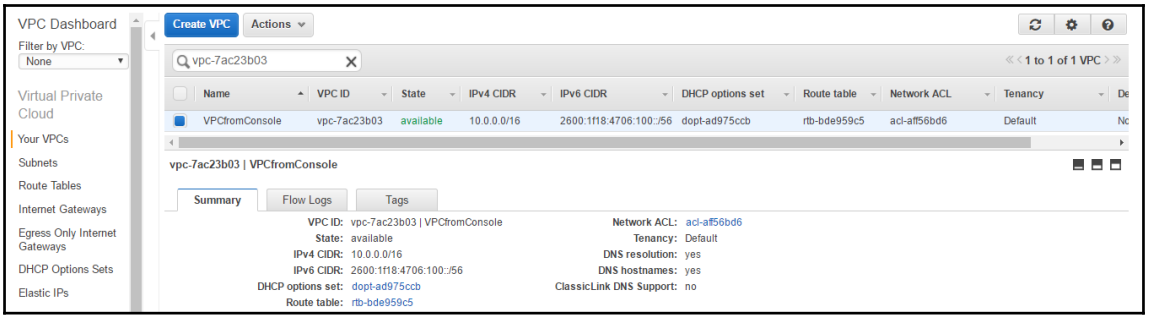

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Test Record Set
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 3 out of 3 Record Sets
Name
Type
Value
internaldomain.com.
NS
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
ns-512.awsdns-00.net.
internaldomain.com.
SOA
ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amaz
service1.internaldomain.com.
A
10.0.0.13
10.0.1.126
Edit Record Set
Name:
service1.internaldomain.com.
Type:
A – IPv4 address
Alias:
Yes
No
TTL (Seconds):
300
1m
5m
1h
1d
Value:
10.0.0.13
10.0.1.126
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234
Routing Policy:
Simple
Route 53 responds to queries based only on the values in this record. Learn More
Save Record Set

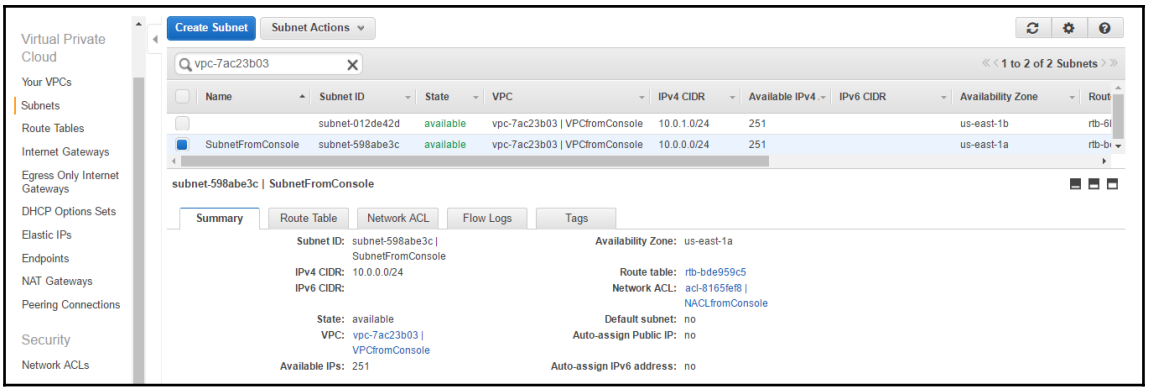

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Search all fields
All Types
Displaying 1 to 1 out of 1 Hosted Zones
Domain Name
Type
Record Set Count
Comment
Hosted Zone ID
internaldomain.com.
Private
3
internal domain
Z16FH1V30VDI72
Hosted Zone Details
Domain Name: internaldomain.com.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z16FH1V30VDI72
Record Set Count: 3
Comment: internal domain
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPC: VPCthroughWizard | vpc-68e93011 | us-east-1
VPC ID:
VPC ID | VPC region
Important
To use private hosted zones, you must set the following Amazon VPC settings to true:
enableDnsHostnames
enableDnsSupport
Learn more
Associate New VPC

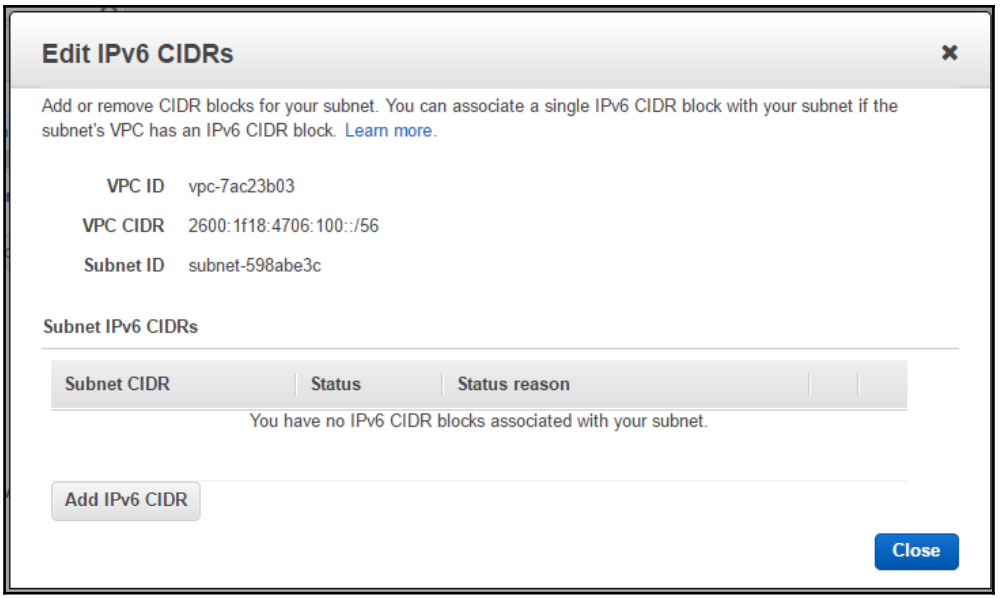

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Test Record Set
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 2 out of 2 Record Sets
Type
Value
Evaluate Target Health
Health Check ID
TTL
Region
NS
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.
ns-512.awsdns-00.net.
172800
SOA
ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama
900
Create Record Set
Name:
elb
.internalelb.
Type:
CNAME – Canonical name
Alias: Yes No
TTL (Seconds):
300
1m
5m
1h
1d
Value:
myfirstapploadbalancer-1311492970.us-east-1.elb.amazonaws.com
The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com
Routing Policy:
Simple
Route 53 responds to queries based only on the values in this record. Learn More

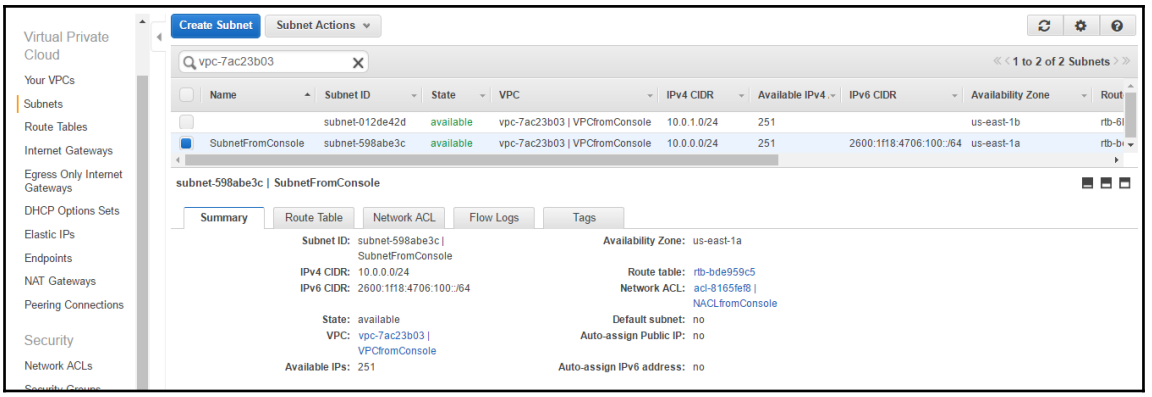

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Create VPC
Actions
vpc-7ac23b03
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCfromConsole
vpc-7ac23b03
available
10.0.0.0/16
dopt-ad975ccb
rtb-bde959c5
acl-af56bd6
Default
vpc-7ac23b03 | VPCfromConsole
Summary
Flow Logs
Tags
VPC ID: vpc-7ac23b03 | VPCfromConsole
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR:
DHCP options set: dopt-ad975ccb
Route table: rtb-bde959c5
Network ACL: acl-af56bd6
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

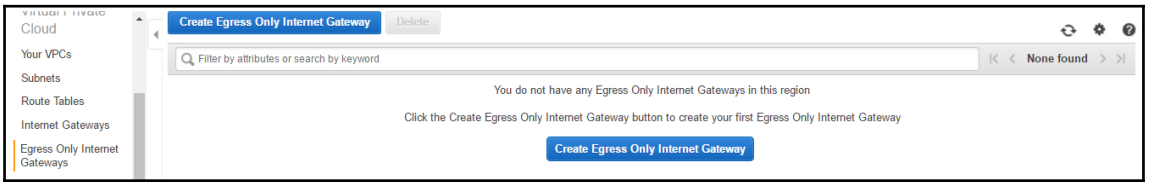

Edit CIDRs
Add or remove CIDR blocks for your VPC. You can associate a single IPv6 CIDR block with your VPC.
Learn more.
VPC ID vpc-7ac23b03
VPC IPv6 CIDRs
VPC CIDR
Status
Status reason
You have no IPv6 CIDR blocks associated with your VPC.
Add IPv6 CIDR
VPC IPv4 CIDRs
VPC CIDR
Status
Status reason
10.0.0.0/16
associated
Close


VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Create VPC
Actions
vpc-7ac23b03
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
Tenancy
VPCfromConsole
vpc-7ac23b03
available
10.0.0.0/16
2600:1f18:4706:100::/56
dopt-ad975ccb
rtb-bde959c5
acl-aff56bd6
Default
vpc-7ac23b03 | VPCfromConsole
Summary
Flow Logs
Tags
VPC ID: vpc-7ac23b03 | VPCfromConsole
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR: 2600:1f18:4706:100::/56
DHCP options set: dopt-ad975ccb
Route table: rtb-bde959c5
Network ACL: acl-aff56bd6
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

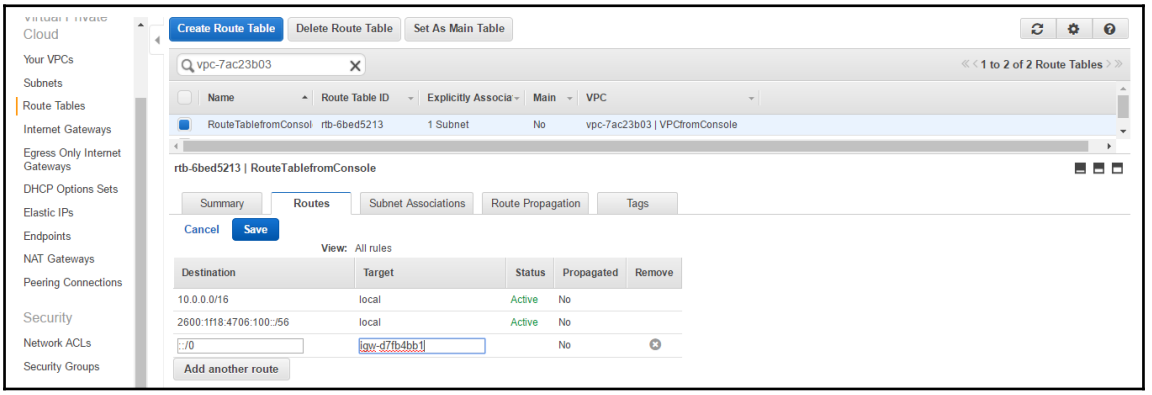

Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Create Subnet
Subnet Actions
vpc-7ac23b03
1 to 2 of 2 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
subnet-012de42d available vpc-7ac23b03 | VPCfromConsole 10.0.1.0/24 251 us-east-1b
SubnetFromConsole subnet-598abe3c available vpc-7ac23b03 | VPCfromConsole 10.0.0.0/24 251 us-east-1a
subnet-598abe3c | SubnetFromConsole
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-598abe3c | SubnetFromConsole
IPv4 CIDR: 10.0.0.0/24
IPv6 CIDR:
State: available
VPC: vpc-7ac23b03 | VPCfromConsole
Available IPs: 251
Availability Zone: us-east-1a
Route table: rtb-bde959c5
Network ACL: acl-8165fef8 | NACLfromConsole
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no

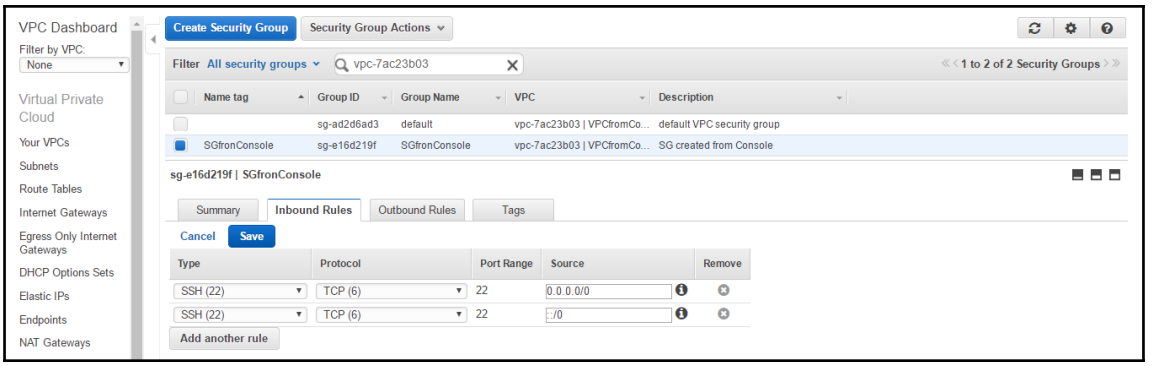

Edit IPv6 CIDRs
Add or remove CIDR blocks for your subnet. You can associate a single IPv6 CIDR block with your subnet if the subnet's VPC has an IPv6 CIDR block. Learn more.
VPC ID vpc-7ac23b03
VPC CIDR 2600:1f18:4706:100::/56
Subnet ID subnet-598abe3c
Subnet IPv6 CIDRs
Subnet CIDR
Status
Status reason
You have no IPv6 CIDR blocks associated with your subnet.
Add IPv6 CIDR
Close

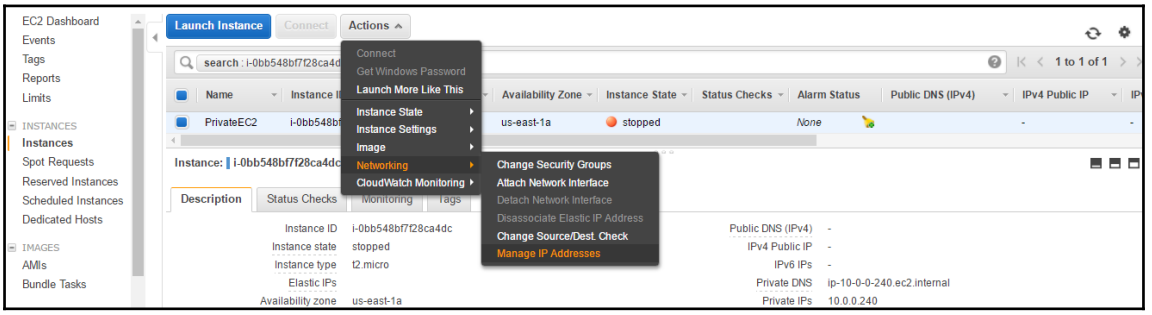

Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Create Subnet
Subnet Actions
vpc-7ac23b03
1 to 2 of 2 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Availability Zone
subnet-012de42d
available
vpc-7ac23b03 | VPCfromConsole
10.0.1.0/24
251
us-east-1b
SubnetFromConsole
subnet-598abe3c
available
vpc-7ac23b03 | VPCfromConsole
10.0.0.0/24
251
2600:1f18:4706:100::/64
us-east-1a
subnet-598abe3c | SubnetFromConsole
Summary
Route Table
Network ACL
Flow Logs
Tags
Subnet ID: subnet-598abe3c | SubnetFromConsole
IPv4 CIDR: 10.0.0.0/24
IPv6 CIDR: 2600:1f18:4706:100::/64
State: available
VPC: vpc-7ac23b03 | VPCfromConsole
Available IPs: 251
Availability Zone: us-east-1a
Route table: rtb-bde959c5
Network ACL: acl-8165fef8 | NACLfromConsole
Default subnet: no
Auto-assign Public IP: no
Auto-assign IPv6 address: no


Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
Create Egress Only Internet Gateway
Delete
Filter by attributes or search by keyword
None found
You do not have any Egress Only Internet Gateways in this region
Click the Create Egress Only Internet Gateway button to create your first Egress Only Internet Gateway
Create Egress Only Internet Gateway

Egress Only Internet Gateways > Create Egress Only Internet Gateway
Create Egress Only Internet Gateway
An Internet Gateway is a virtual router that connects a VPC to the internet
VPC*
vpc-7ac23b03
* Required
Cancel
Create


Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Security
Network ACLs
Security Groups
Create Route Table
Delete Route Table
Set As Main Table
vpc-7ac23b03
1 to 2 of 2 Route Tables
Name
Route Table ID
Explicitly Associa
Main
VPC
RouteTablefromConsol
rtb-6bed5213
1 Subnet
No
vpc-7ac23b03 | VPCfromConsole
rtb-6bed5213 | RouteTablefromConsole
Summary
Routes
Subnet Associations
Route Propagation
Tags
Cancel
Save
View: All rules
Destination
Target
Status
Propagated
Remove
10.0.0.0/16
local
Active
No
2600:1f18:4706:100::/56
local
Active
No
::/0
igw-d7fb4bb1
No
Add another route

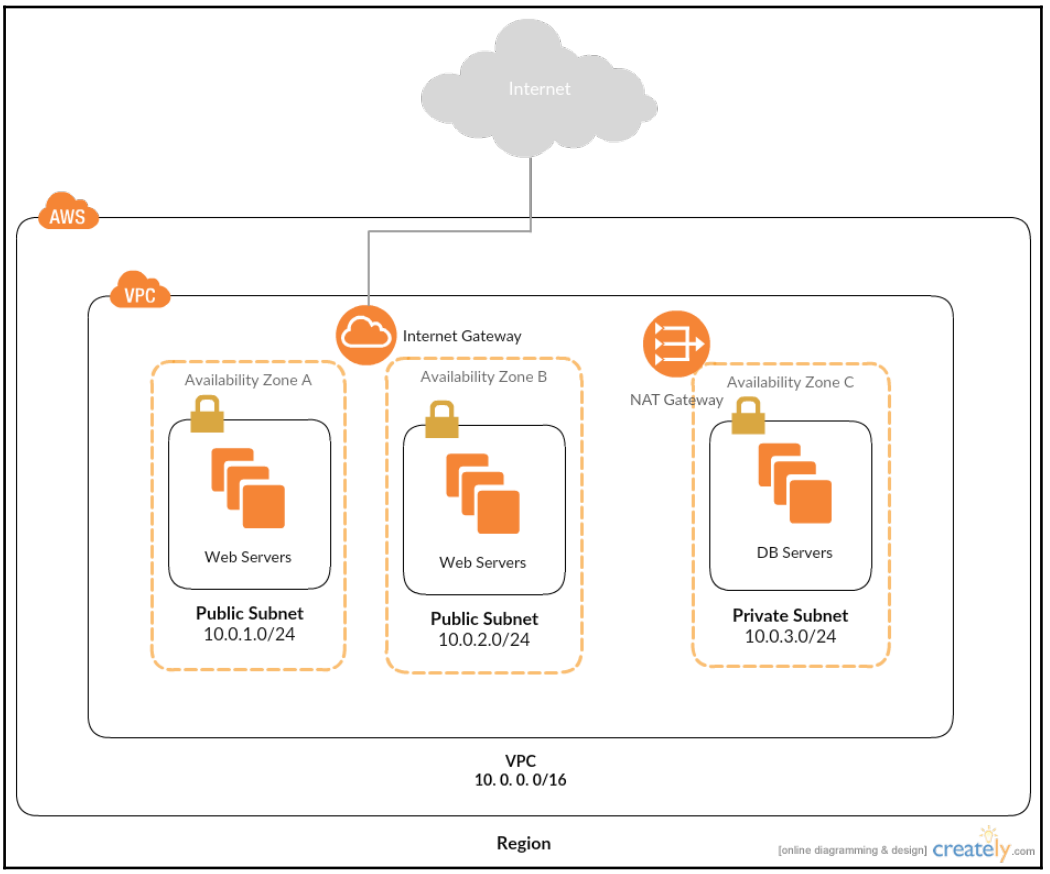

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Create Security Group
Security Group Actions
Filter All security groups
vpc-7ac23b03
1 to 2 of 2 Security Groups
Name tag
Group ID
Group Name
VPC
Description
sg-ad2d6ad3 default vpc-7ac23b03 | VPCfromCo... default VPC security group
SGfronConsole sg-e16d219f SGfronConsole vpc-7ac23b03 | VPCfromCo... SG created from Console
sg-e16d219f | SGfronConsole
Summary
Inbound Rules
Outbound Rules
Tags
Cancel
Save
Type
Protocol
Port Range
Source
Remove
SSH (22) TCP (6) 22 0.0.0.0/0
SSH (22) TCP (6) 22 ::/0
Add another rule

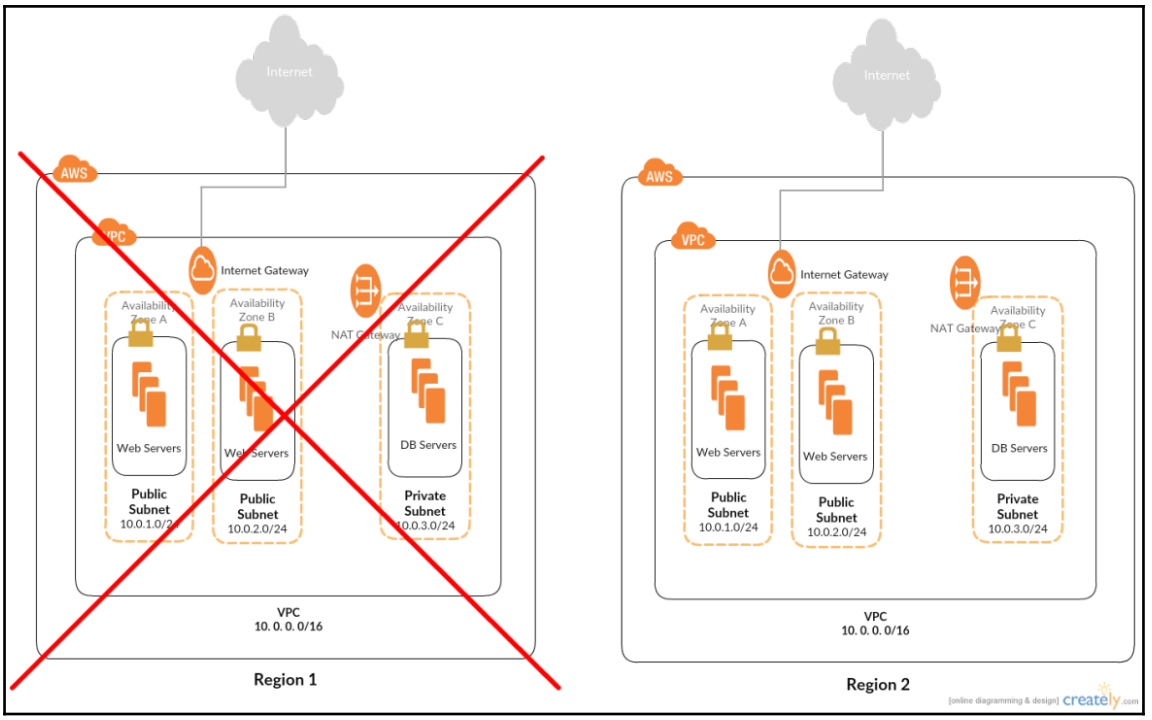

EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Bundle Tasks
Launch Instance
Connect
Actions
Connect
Get Windows Password
Launch More Like This
Instance State
Instance Settings
Image
Networking
CloudWatch Monitoring
Change Security Groups
Attach Network Interface
Detach Network Interface
Disassociate Elastic IP Address
Change Source/Dest. Check
Manage IP Addresses
search : i-0bb548bf7f28ca4dc
1 to 1 of 1
Name
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
PrivateEC2 i-0bb548bf us-east-1a stopped None
Instance: i-0bb548bf7f28ca4dc
Description
Status Checks
Monitoring
Tags
Instance ID i-0bb548bf7f28ca4dc
Instance state stopped
Instance type t2.micro
Elastic IPs
Availability zone us-east-1a
Public DNS (IPv4)
IPv4 Public IP
IPv6 IPs
Private DNS ip-10-0-0-240.ec2.internal
Private IPs 10.0.0.240

Manage IP Addresses
You can assign and unassign IPv4 and IPv6 IP addresses on each network interface. Leave the IP address field blank and an available address will be assigned or enter an IP address that you want to assign.
To add or edit an IPv4 public IP Allocate an Elastic IP to this instance or network interface.
eth0: eni-b126d4a6 - Primary network interface - 10.0.0.0/24
IPv4 Addresses
Private IP
Public IP
10.0.0.240
Assign new IP
IPv6 Addresses
IP Addresses
Auto-assign
Undo
Cancel
Yes, Update

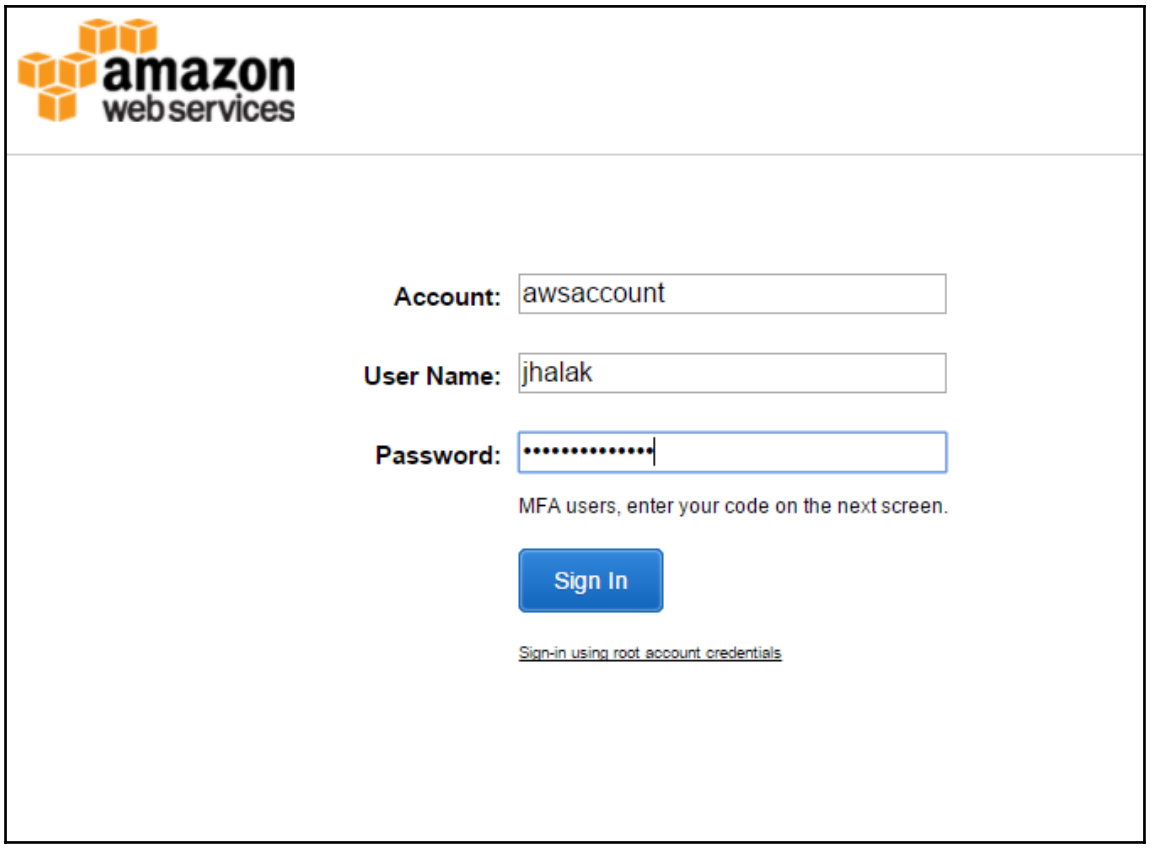
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Spot Requests
Reserved Instances
Scheduled Instances
Dedicated Hosts
IMAGES
AMIs
Launch Instance
Connect
Actions
search : i-0bb548bf7f28ca4dc
Add filter
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
IPv4 Public IP
IPv6 IP
PrivateEC2
i-0bb548bf7f28ca4dc
t2.micro
us-east-1a
stopped
None
-
2600:1
Instance: i-0bb548bf7f28ca4dc (PrivateEC2)
Private IP: 10.0.0.240
Description
Status Checks
Monitoring
Tags
Instance ID
i-0bb548bf7f28ca4dc
Instance state
stopped
Instance type
t2.micro
Public DNS (IPv4)
-
IPv4 Public IP
-
IPv6 IPs
2600:1f18:24ac:6300:5856:1a65:bcc5:7e56

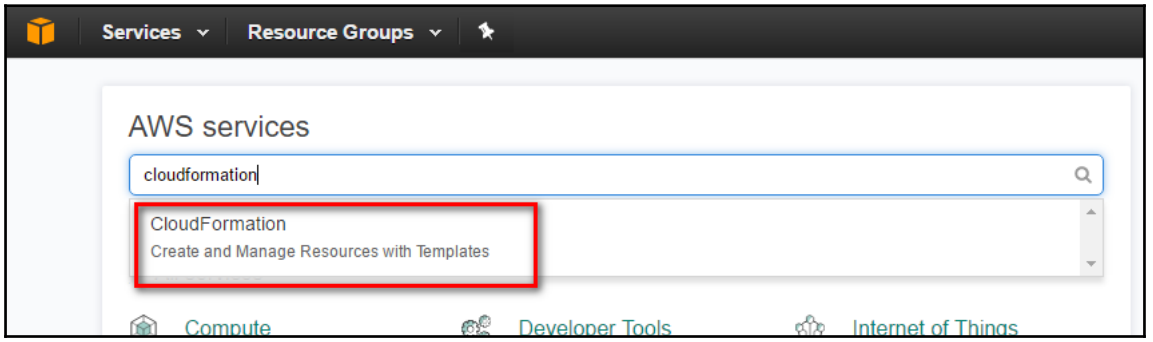
Chapter 5: Working with Infrastructure Automation

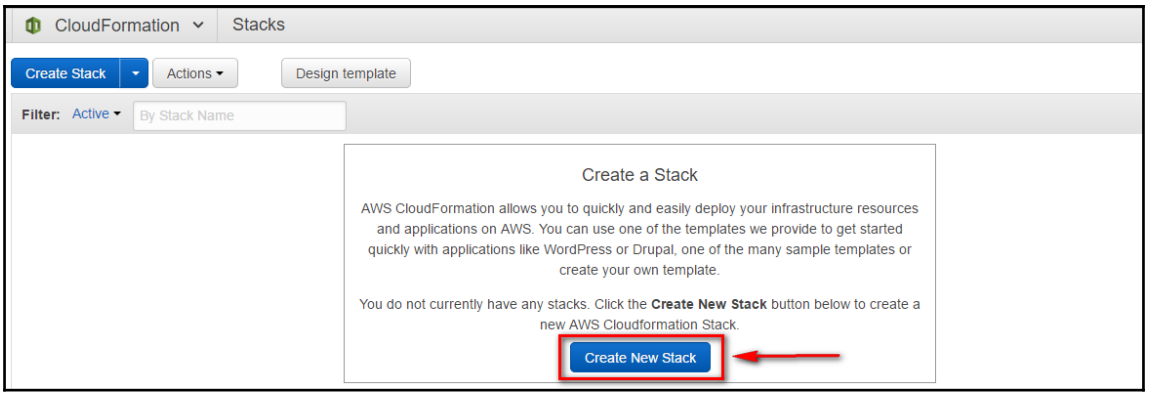


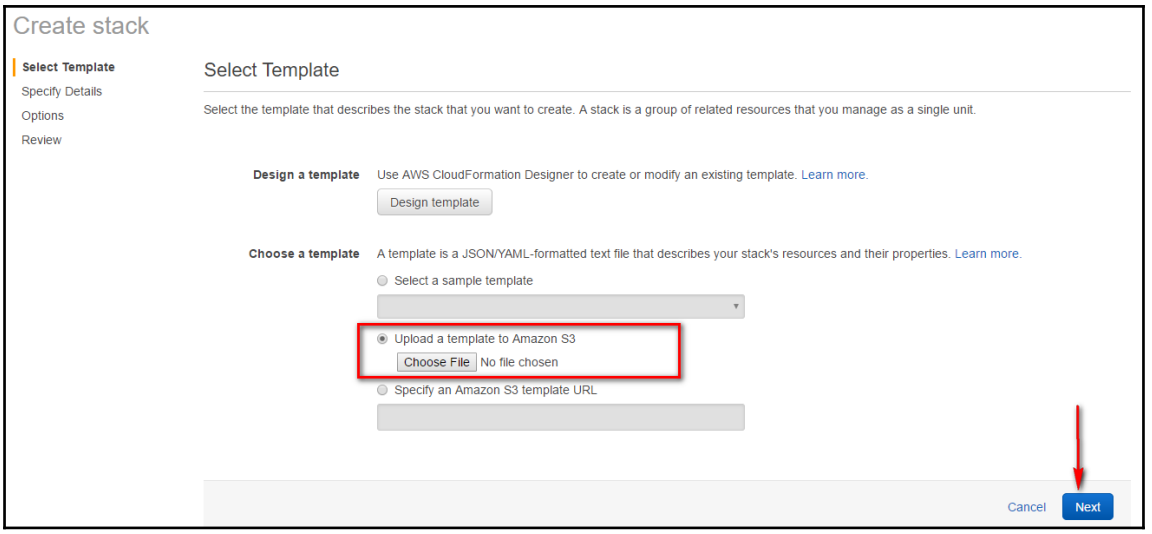

Internet
AWS
VPC
Internet Gateway
Availability Zone A
Availability Zone B
Availability Zone C
NAT Gateway
Web Servers
Web Servers
DB Servers
Public Subnet 10.0.1.0/24
Public Subnet 10.0.2.0/24
Private Subnet 10.0.3.0/24
VPC 10. 0. 0. 0/16
Region 1
Internet
AWS
VPC
Internet Gateway
Availability Zone A
Availability Zone B
Availability Zone C
NAT Gateway
Web Servers
Web Servers
DB Servers
Public Subnet 10.0.1.0/24
Public Subnet 10.0.2.0/24
Private Subnet 10.0.3.0/24
VPC 10. 0. 0. 0/16
Region 2
[online diagramming & design] creately.com

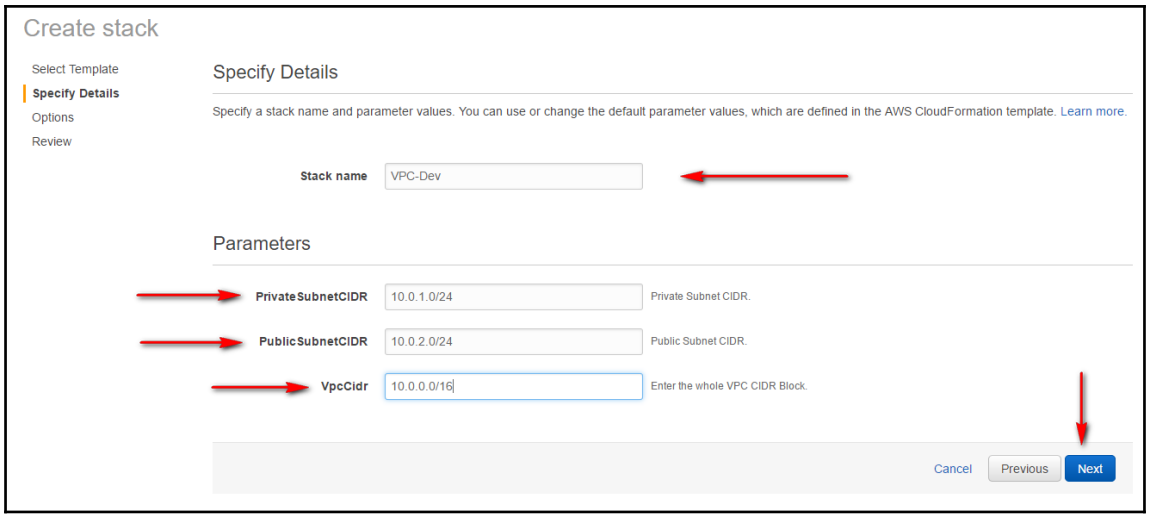
{
"AWSTemplateFormatVersion": "2010-09-09",
"Description": "Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.",
"Parameters": {
"VpcCidr": {
"Description": "Enter the whole VPC CIDR Block.",
"Type": "String",
"ConstraintDescription": "Supports subnet sizes of /16 to /22 only. Input must be a correct CIDR, such as: 10.0.0.0/16'
"AllowedPattern": "^((\\d)+.){3}(0)\\/(16|17|18|19|20|21|22)"
},
"PublicSubnetCIDR": {
Validate JSON
Clear
Support JSONLint for $2/Month
Results
Valid JSON

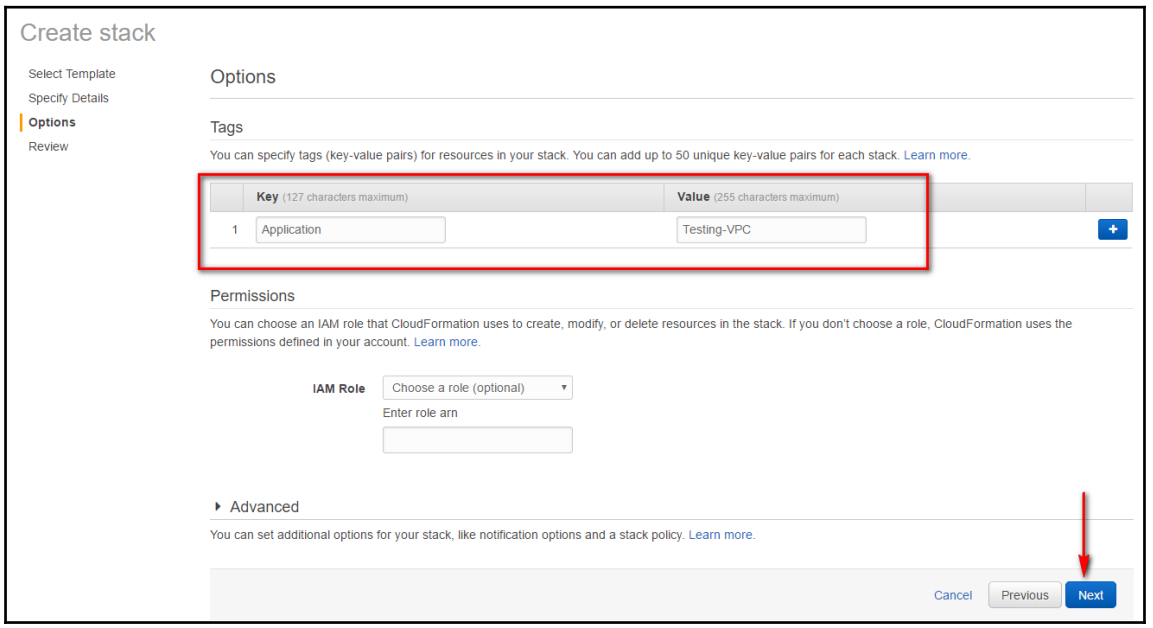

amazon
web services
Account:
awsaccount
User Name:
jhalak
Password:
MFA users, enter your code on the next screen.
Sign In
Sign-in using root account credentials

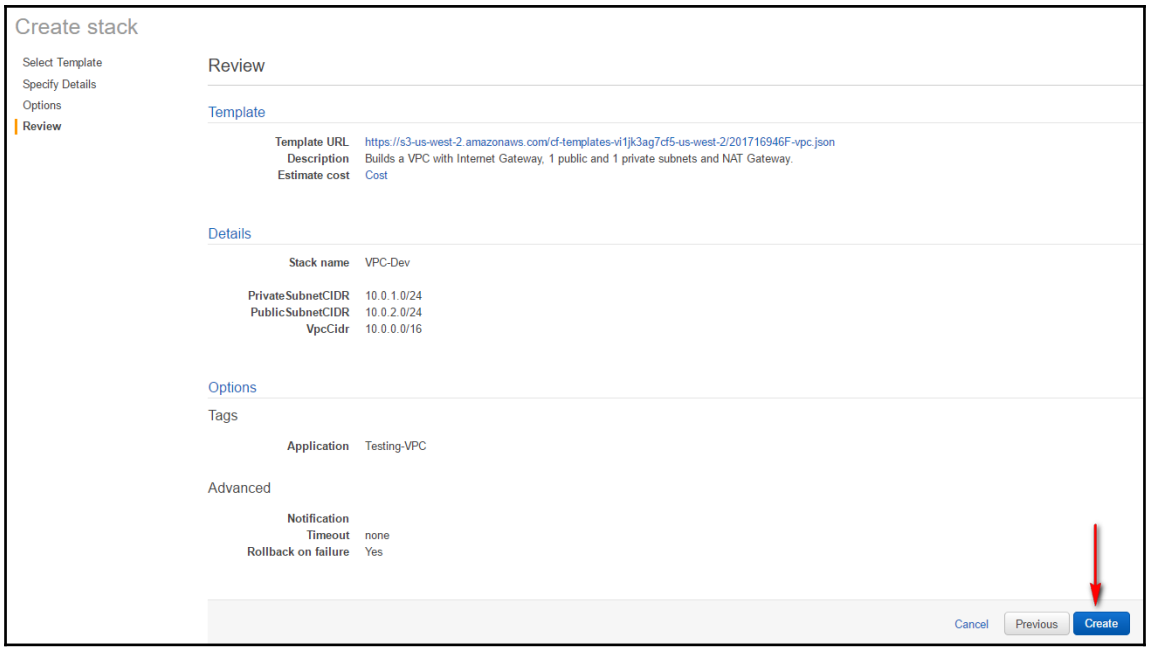

Services
Resource Groups
AWS services
cloudformation
CloudFormation
Create and Manage Resources with Templates
Compute
Developer Tools
Internet of Things

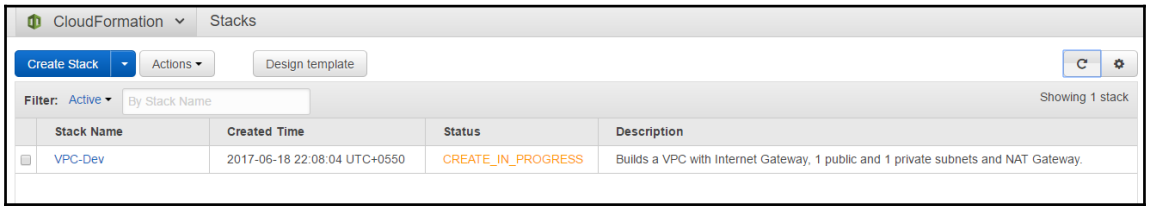

CloudFormation
Stacks
Create Stack
Actions
Design template
Filter:
Active
By Stack Name
Create a Stack
AWS CloudFormation allows you to quickly and easily deploy your infrastructure resources and applications on AWS. You can use one of the templates we provide to get started quickly with applications like WordPress or Drupal, one of the many sample templates or create your own template.
You do not currently have any stacks. Click the Create New Stack button below to create a new AWS Cloudformation Stack.
Create New Stack

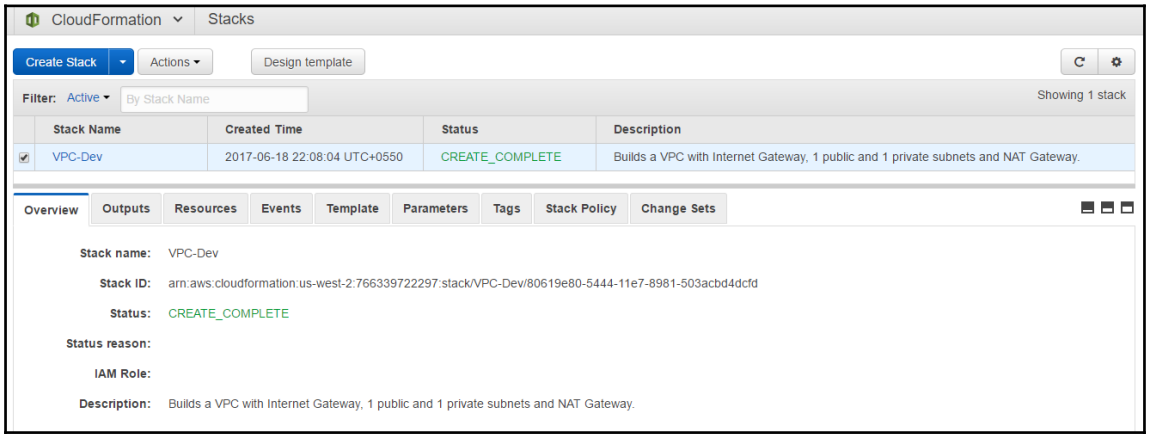

Create stack
Select Template
Specify Details
Options
Review
Select Template
Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.
Design a template
Use AWS CloudFormation Designer to create or modify an existing template. Learn more.
Design template
Choose a template
A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.
Select a sample template
Upload a template to Amazon S3
Choose File
No file chosen
Specify an Amazon S3 template URL
Cancel
Next

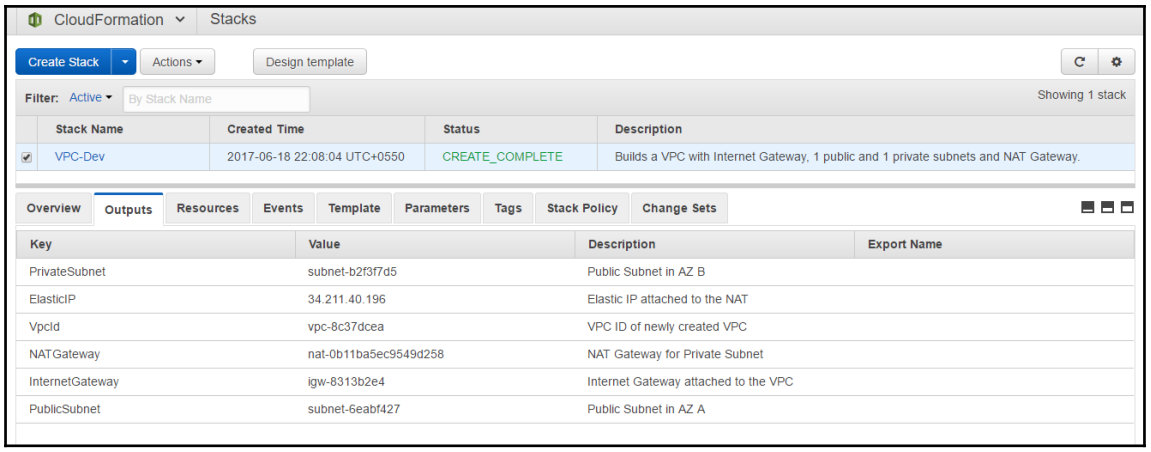

Create stack
Select Template
Specify Details
Options
Review
Specify Details
Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.
Stack name
VPC-Dev
Parameters
PrivateSubnetCIDR
10.0.1.0/24
Private Subnet CIDR.
PublicSubnetCIDR
10.0.2.0/24
Public Subnet CIDR.
VpcCidr
10.0.0.0/16
Enter the whole VPC CIDR Block.
Cancel
Previous
Next

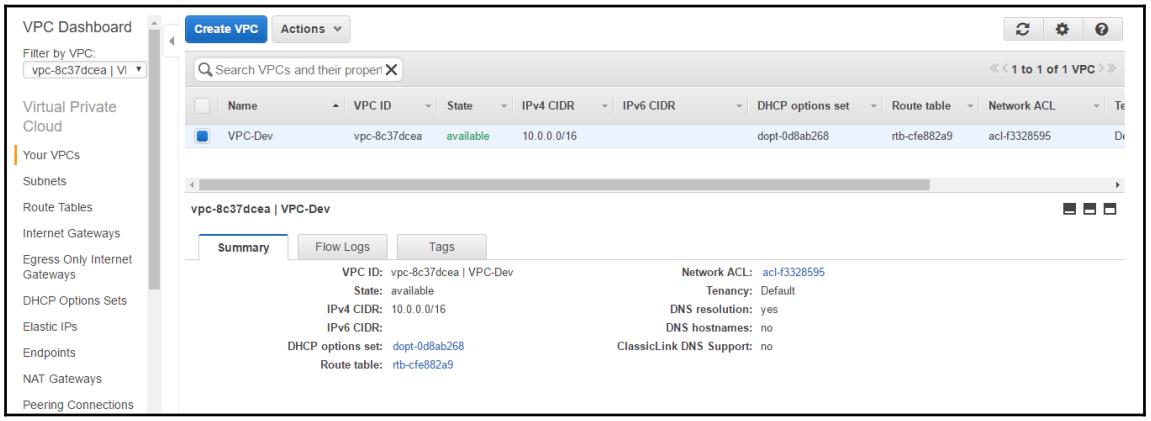

Create stack
Select Template
Specify Details
Options
Review
Options
Tags
You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.
Key (127 characters maximum)
Value (255 characters maximum)
1
Application
Testing-VPC
Permissions
You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.
IAM Role
Choose a role (optional)
Enter role arn
Advanced
You can set additional options for your stack, like notification options and a stack policy. Learn more.
Cancel
Previous
Next

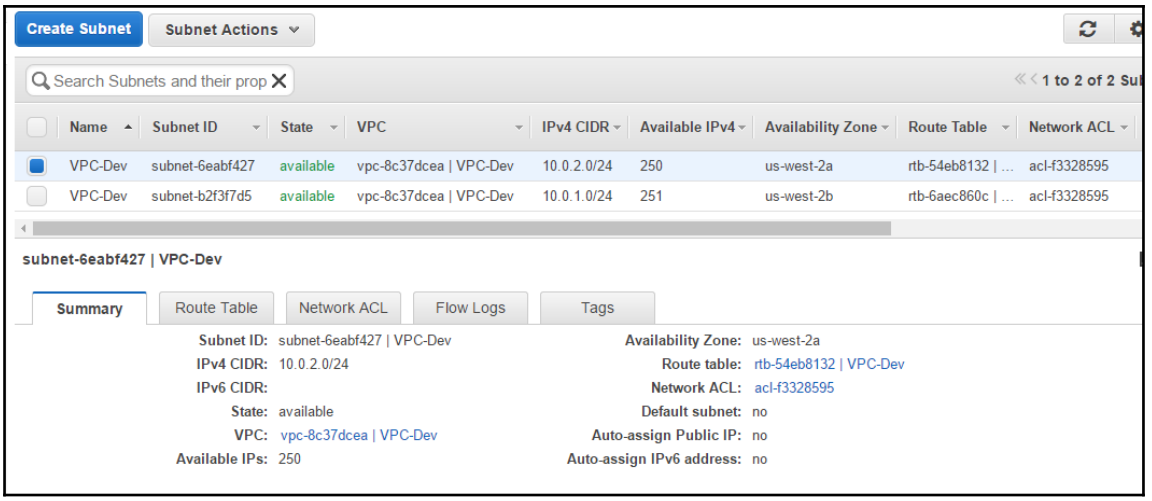

Create stack
Select Template
Specify Details
Options
Review
Review
Template
Template URL https://s3-us-west-2.amazonaws.com/cf-templates-vi1jk3ag7cf5-us-west-2/201716946F-vpc.json
Description Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Estimate cost Cost
Details
Stack name VPC-Dev
PrivateSubnetCIDR 10.0.1.0/24
PublicSubnetCIDR 10.0.2.0/24
VpcCidr 10.0.0.0/16
Options
Tags
Application Testing-VPC
Advanced
Notification
Timeout none
Rollback on failure Yes
Cancel
Previous
Create


CloudFormation
Stacks
Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 1 stack
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
CREATE_IN_PROGRESS
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.

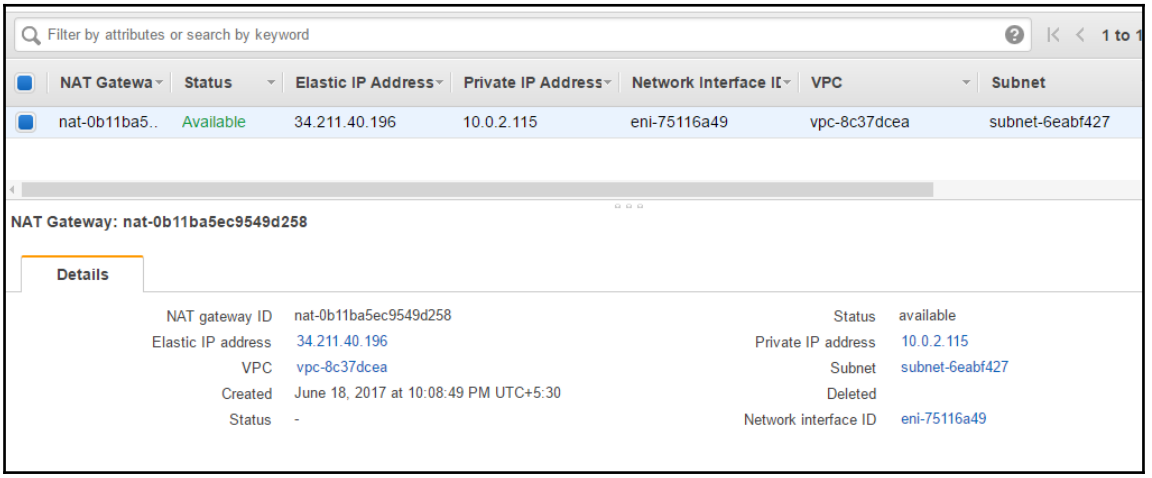

CloudFormation
Stacks
Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 1 stack
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
CREATE_COMPLETE
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Stack name: VPC-Dev
Stack ID: arn:aws:cloudformation:us-west-2:766339722297:stack/VPC-Dev/80619e80-5444-11e7-8981-503acbd4dcfd
Status: CREATE_COMPLETE
Status reason:
IAM Role:
Description: Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.

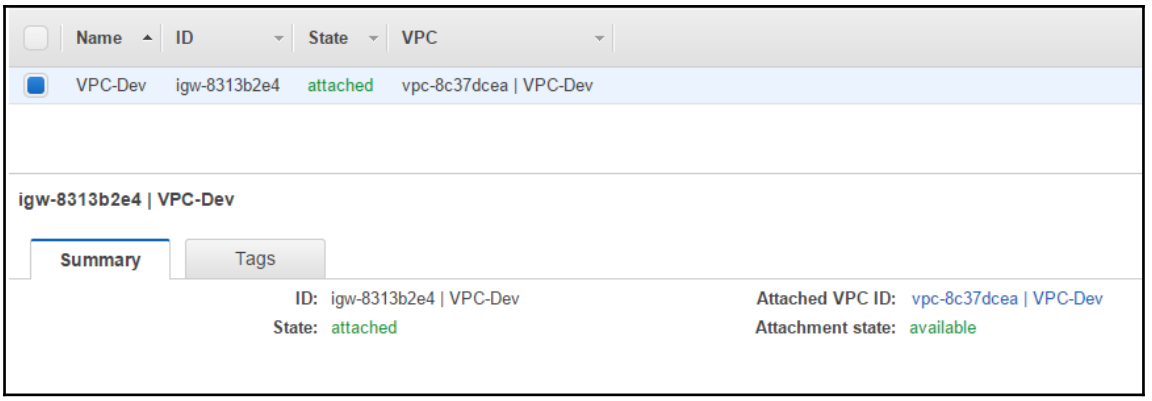

CloudFormation
Stacks
Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 1 stack
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
CREATE_COMPLETE
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Key
Value
Description
Export Name
PrivateSubnet
subnet-b2f3f7d5
Public Subnet in AZ B
ElasticIP
34.211.40.196
Elastic IP attached to the NAT
VpcId
vpc-8c37dcea
VPC ID of newly created VPC
NATGateway
nat-0b11ba5ec9549d258
NAT Gateway for Private Subnet
InternetGateway
igw-8313b2e4
Internet Gateway attached to the VPC
PublicSubnet
subnet-6eabf427
Public Subnet in AZ A

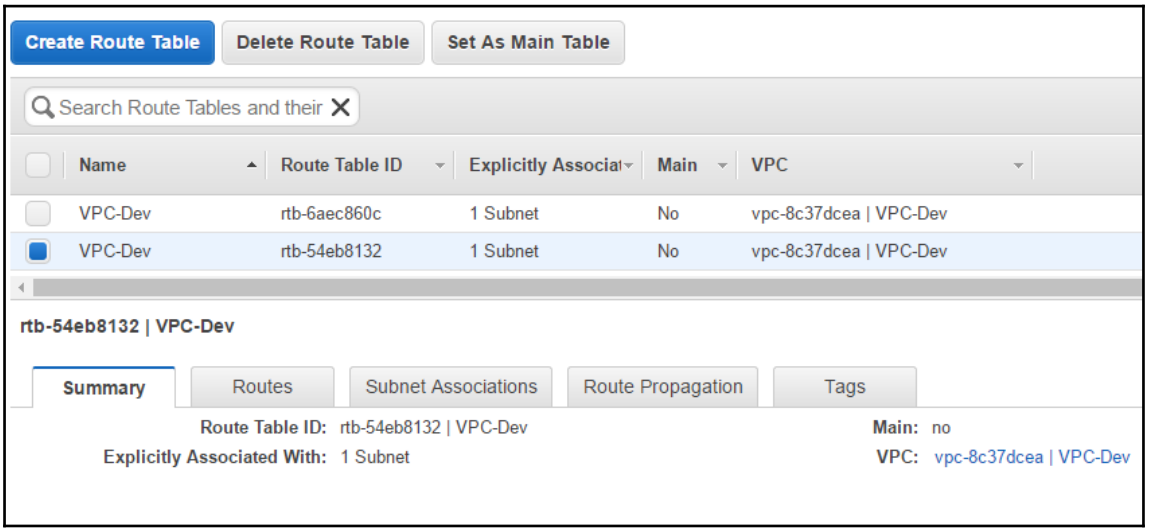

VPC Dashboard
Filter by VPC:
vpc-8c37dcea | Vl
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
NAT Gateways
Peering Connections
Create VPC
Actions
Search VPCs and their proper
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
Network ACL
VPC-Dev
vpc-8c37dcea
available
10.0.0.0/16
dopt-0d8ab268
rtb-cfe882a9
acl-f3328595
vpc-8c37dcea | VPC-Dev
Summary
Flow Logs
Tags
VPC ID: vpc-8c37dcea | VPC-Dev
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR:
DHCP options set: dopt-0d8ab268
Route table: rtb-cfe882a9
Network ACL: acl-f3328595
Tenancy: Default
DNS resolution: yes
DNS hostnames: no
ClassicLink DNS Support: no

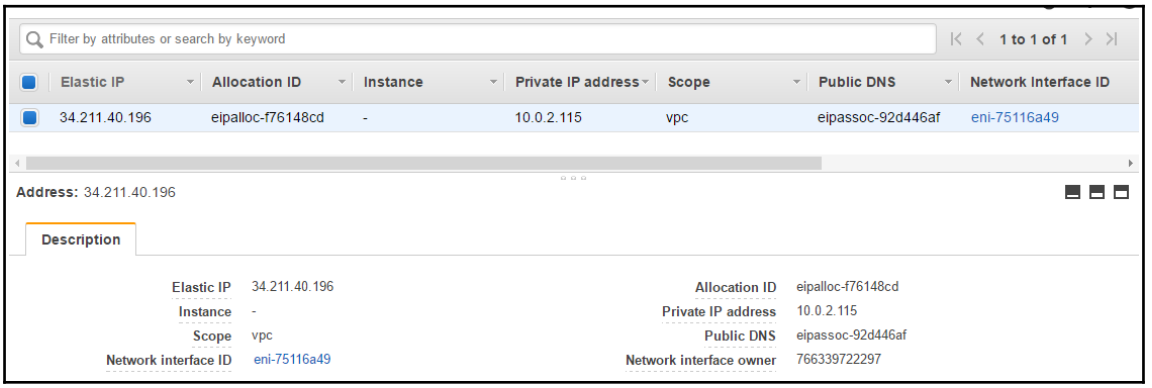


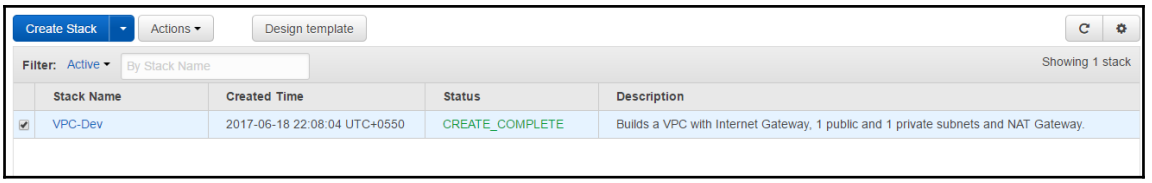
Key	Value
Name	VPC-Dev
Application	Testing-VPC
Environment	Dev
Network	Public
aws:cloudformation:logical-id	PublicSubnet

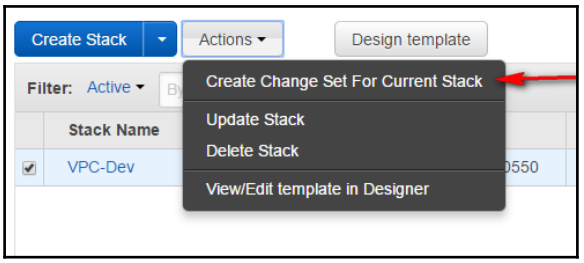


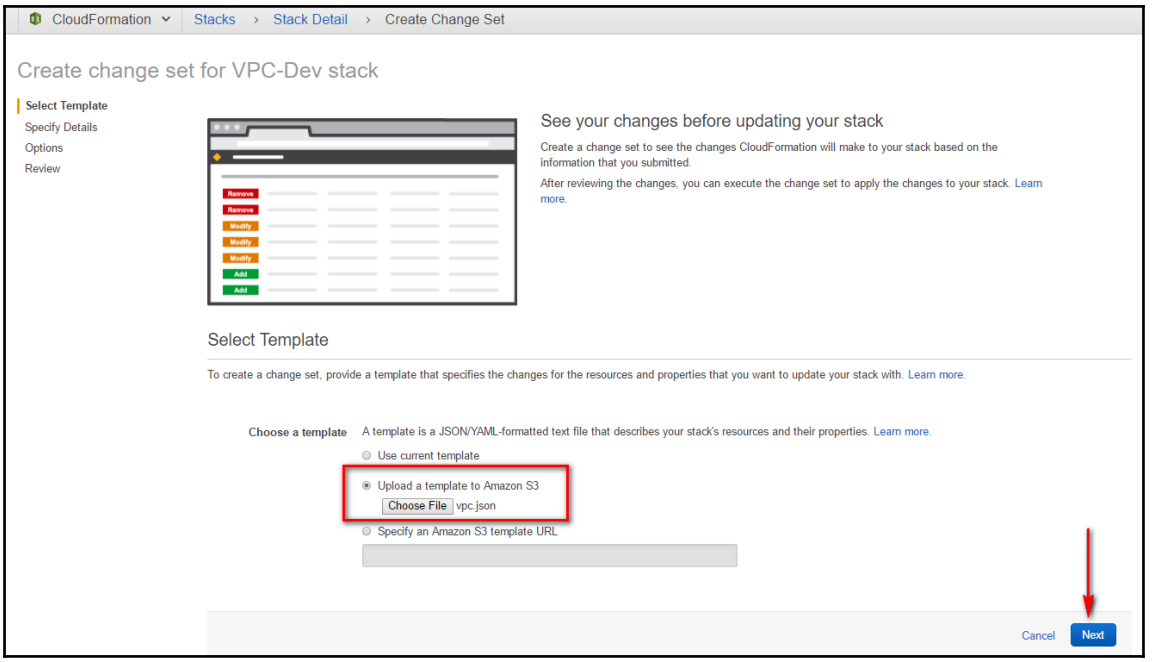

Name
ID
State
VPC
VPC-Dev
igw-8313b2e4
attached
vpc-8c37dcea | VPC-Dev
igw-8313b2e4 | VPC-Dev
Summary
Tags
ID: igw-8313b2e4 | VPC-Dev
State: attached
Attached VPC ID: vpc-8c37dcea | VPC-Dev
Attachment state: available

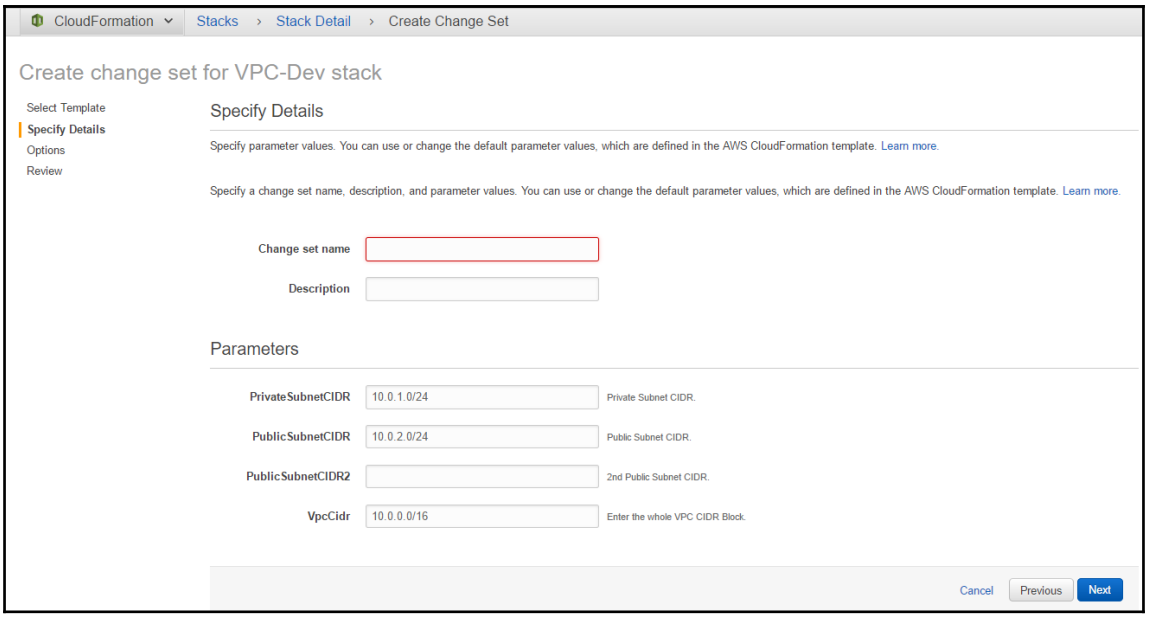

Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and their
Name
Route Table ID
Explicitly Associat
Main
VPC
VPC-Dev
rtb-6aec860c
1 Subnet
No
vpc-8c37dcea | VPC-Dev
VPC-Dev
rtb-54eb8132
1 Subnet
No
vpc-8c37dcea | VPC-Dev
rtb-54eb8132 | VPC-Dev
Summary
Routes
Subnet Associations
Route Propagation
Tags
Route Table ID: rtb-54eb8132 | VPC-Dev
Explicitly Associated With: 1 Subnet
Main: no
VPC: vpc-8c37dcea | VPC-Dev

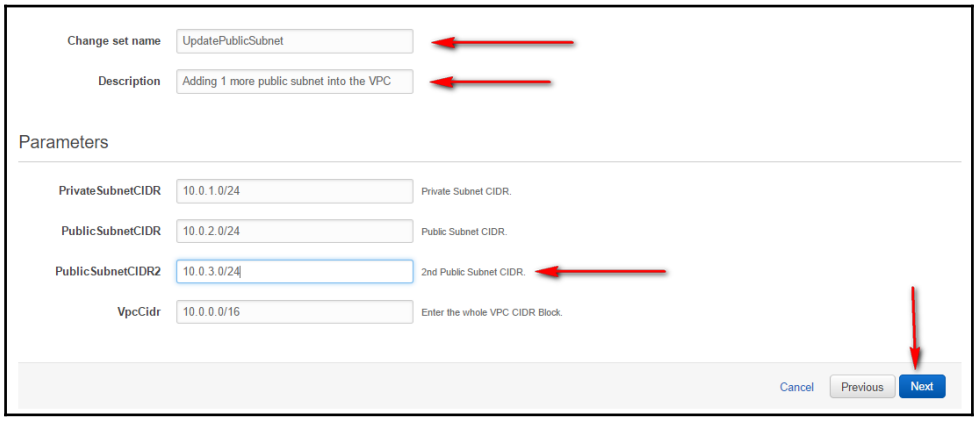

Filter by attributes or search by keyword
1 to 1 of 1
Elastic IP
Allocation ID
Instance
Private IP address
Scope
Public DNS
Network Interface ID
34.211.40.196
eipalloc-f76148cd
-
10.0.2.115
vpc
eipassoc-92d446af
eni-75116a49
Address: 34.211.40.196
Description
Elastic IP 34.211.40.196
Instance -
Scope vpc
Network interface ID eni-75116a49
Allocation ID eipalloc-f76148cd
Private IP address 10.0.2.115
Public DNS eipassoc-92d446af
Network interface owner 766339722297

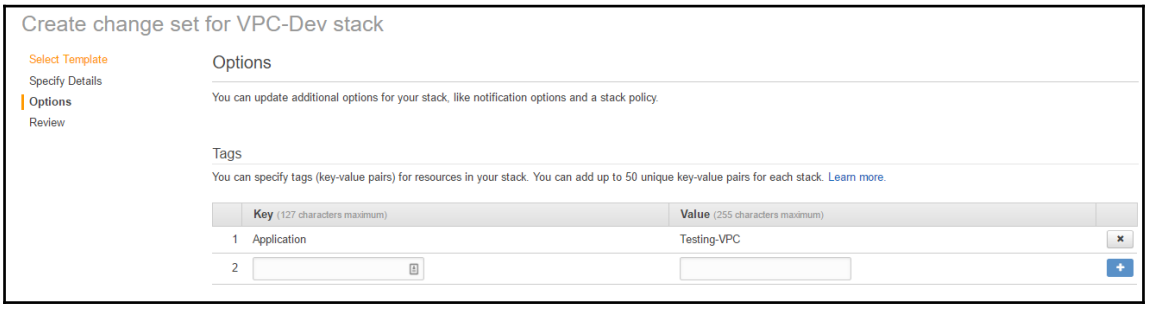

Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 1 stack
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
CREATE_COMPLETE
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.

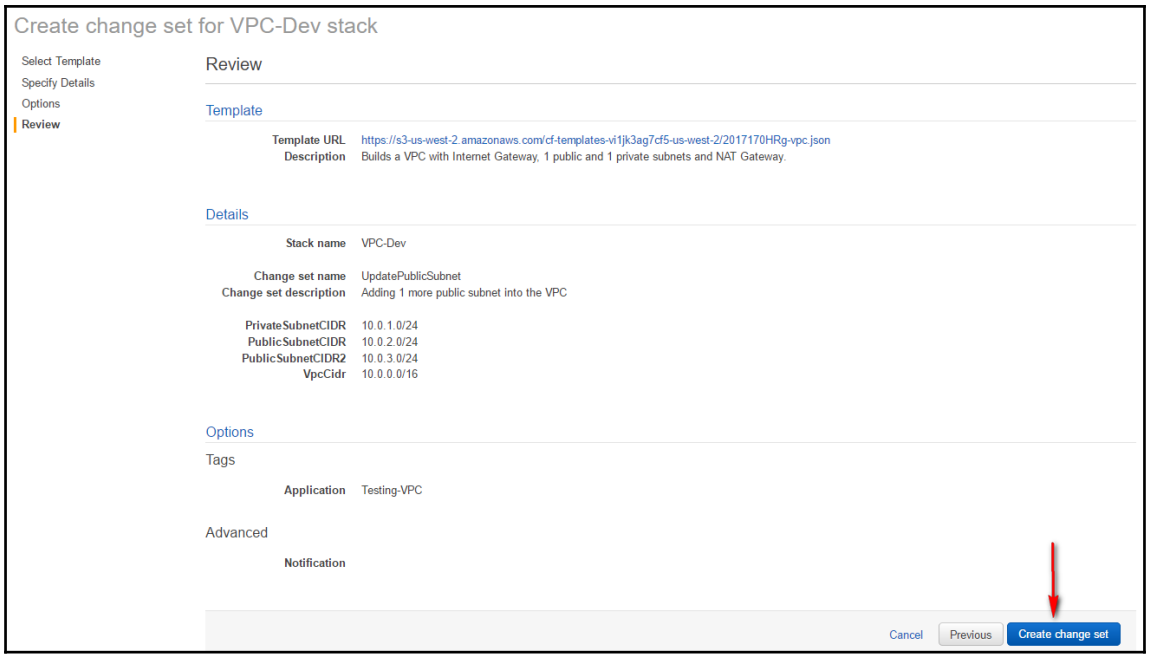

Create Stack
Actions
Design template
Filter: Active
Create Change Set For Current Stack
Update Stack
Delete Stack
View/Edit template in Designer
Stack Name
VPC-Dev


CloudFormation
Stacks
Stack Detail
Create Change Set
Create change set for VPC-Dev stack
Select Template
Specify Details
Options
Review
See your changes before updating your stack
Create a change set to see the changes CloudFormation will make to your stack based on the information that you submitted.
After reviewing the changes, you can execute the change set to apply the changes to your stack. Learn more.
Select Template
To create a change set, provide a template that specifies the changes for the resources and properties that you want to update your stack with. Learn more.
Choose a template
A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.
Use current template
Upload a template to Amazon S3
Choose File
vpc.json
Specify an Amazon S3 template URL
Cancel
Next

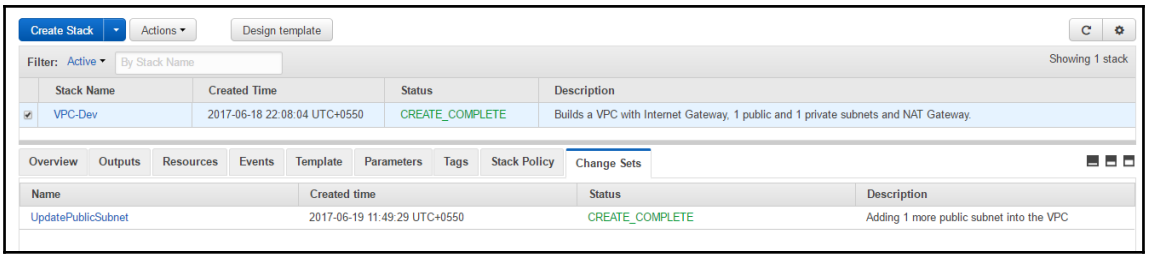

CloudFormation
Stacks
Stack Detail
Create Change Set
Create change set for VPC-Dev stack
Select Template
Specify Details
Options
Review
Specify Details
Specify parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.
Specify a change set name, description, and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.
Change set name
Description
Parameters
PrivateSubnetCIDR
10.0.1.0/24
Private Subnet CIDR.
PublicSubnetCIDR
10.0.2.0/24
Public Subnet CIDR.
PublicSubnetCIDR2
2nd Public Subnet CIDR.
VpcCidr
10.0.0.0/16
Enter the whole VPC CIDR Block.
Cancel
Previous
Next

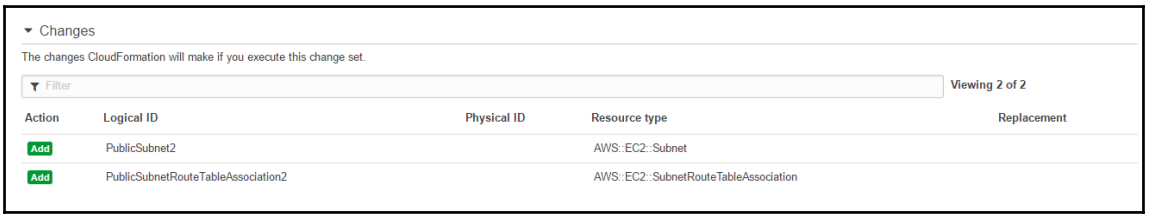

Change set name
UpdatePublicSubnet
Description
Adding 1 more public subnet into the VPC
Parameters
PrivateSubnetCIDR
10.0.1.0/24
Private Subnet CIDR.
PublicSubnetCIDR
10.0.2.0/24
Public Subnet CIDR.
PublicSubnetCIDR2
10.0.3.0/24
2nd Public Subnet CIDR.
VpcCidr
10.0.0.0/16
Enter the whole VPC CIDR Block.
Cancel
Previous
Next

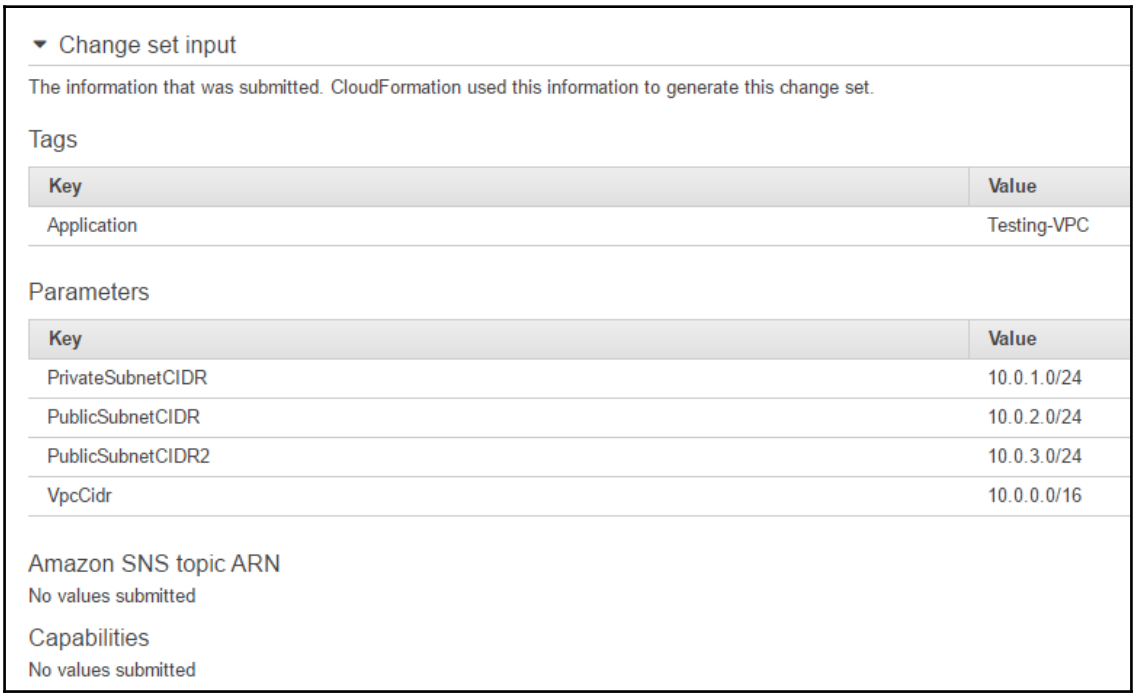

Create change set for VPC-Dev stack
Select Template
Specify Details
Options
Review
Options
You can update additional options for your stack, like notification options and a stack policy.
Tags
You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.
Key (127 characters maximum)
Value (255 characters maximum)
1
Application
Testing-VPC
2


Create change set for VPC-Dev stack
Select Template
Specify Details
Options
Review
Review
Template
Template URL
https://s3-us-west-2.amazonaws.com/cf-templates-vi1jk3ag7cf5-us-west-2/2017170HRg-vpc.json
Description
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Details
Stack name
VPC-Dev
Change set name
UpdatePublicSubnet
Change set description
Adding 1 more public subnet into the VPC
PrivateSubnetCIDR
10.0.1.0/24
PublicSubnetCIDR
10.0.2.0/24
PublicSubnetCIDR2
10.0.3.0/24
VpcCidr
10.0.0.0/16
Options
Tags
Application
Testing-VPC
Advanced
Notification
Cancel
Previous
Create change set

UpdatePublicSubnet
Other Actions
Execute
Overview
ID
arn:aws:cloudformation:us-west-2:766339722297:changeSet/UpdatePublicSubnet/825573c1-66aa-4fc2-a95d-aa28f00a8332
Description
Adding 1 more public subnet into the VPC
Created time
2017-06-19 11:49:29 UTC+0550
Status
CREATE_COMPLETE
Stack name
VPC-Dev
Change set input
Changes
Details
Template


Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 1 stack
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
CREATE_COMPLETE
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Name
Created time
Status
Description
UpdatePublicSubnet
2017-06-19 11:49:29 UTC+0550
CREATE_COMPLETE
Adding 1 more public subnet into the VPC

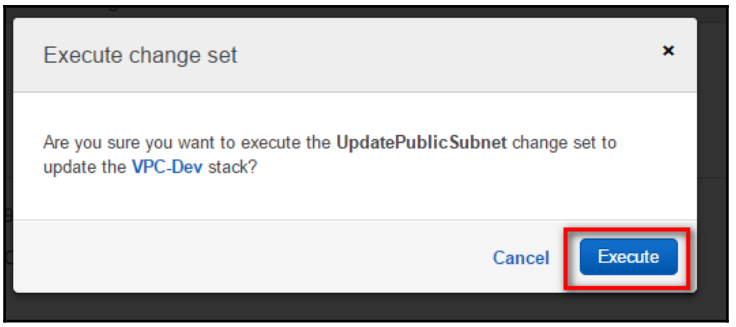

Changes
The changes CloudFormation will make if you execute this change set.
Filter
Viewing 2 of 2
Action
Logical ID
Physical ID
Resource type
Replacement
Add
PublicSubnet2
AWS::EC2::Subnet
Add
PublicSubnetRouteTableAssociation2
AWS::EC2::SubnetRouteTableAssociation

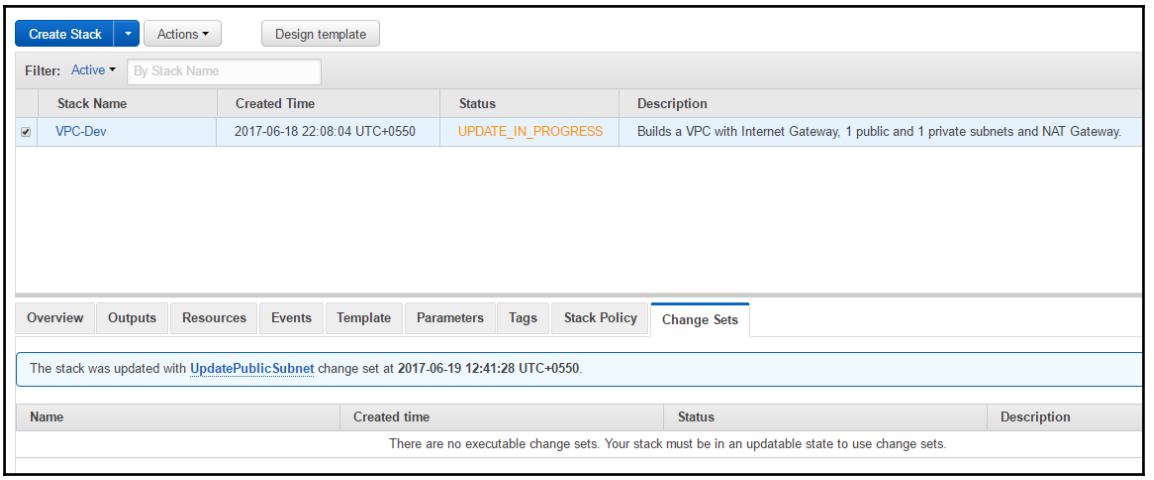

Change set input
The information that was submitted. CloudFormation used this information to generate this change set.
Tags
Key
Value
Application
Testing-VPC
Parameters
Key
Value
PrivateSubnetCIDR
10.0.1.0/24
PublicSubnetCIDR
10.0.2.0/24
PublicSubnetCIDR2
10.0.3.0/24
VpcCidr
10.0.0.0/16
Amazon SNS topic ARN
No values submitted
Capabilities
No values submitted

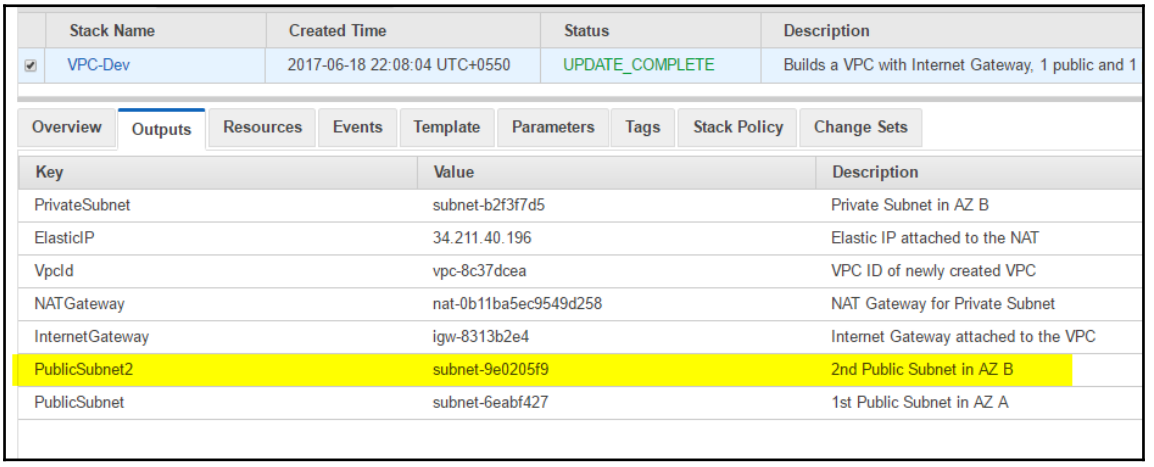
Details

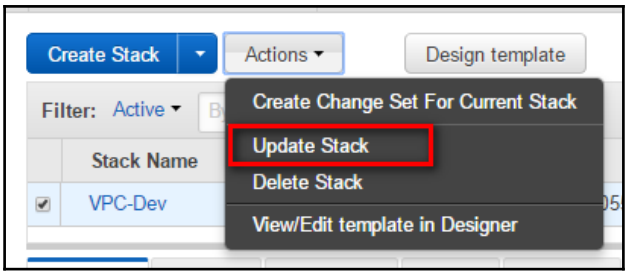
Detailed information about each change. For descriptions of each field, see the Change data type.

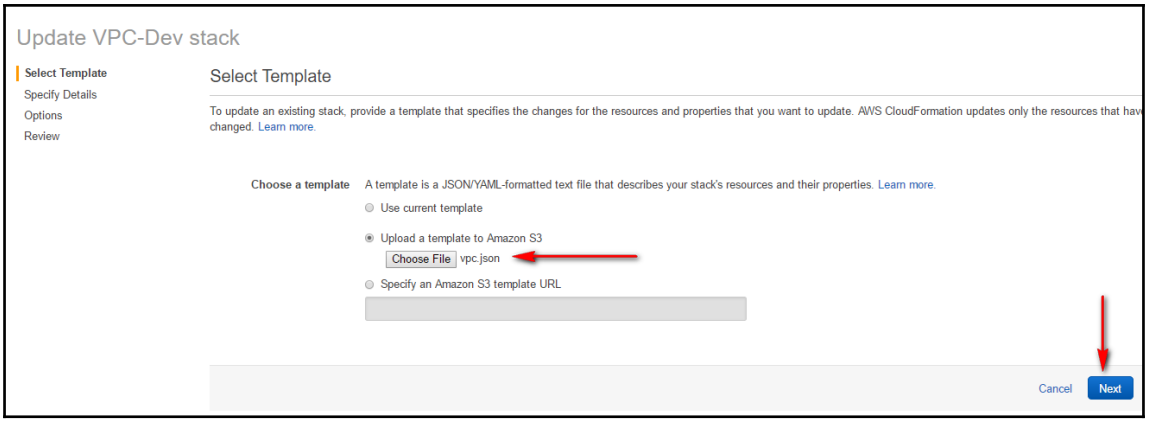

```
[
  {
    "resourceChange": {
      "logicalResourceId": "PublicSubnet2",
      "action": "Add",
      "physicalResourceId": null,
      "resourceType": "AWS::EC2::Subnet",
      "replacement": null,
      "details": [],
      "scope": []
    },
    "type": "Resource"
  },
  {
    "resourceChange": {
      "logicalResourceId": "PublicSubnetRouteTableAssociation2",
      "action": "Add",
      "physicalResourceId": null,
      "resourceType": "AWS::EC2::SubnetRouteTableAssociation",
      "replacement": null,
      "details": [],
      "scope": []
    },
    "type": "Resource"
  }
]
```

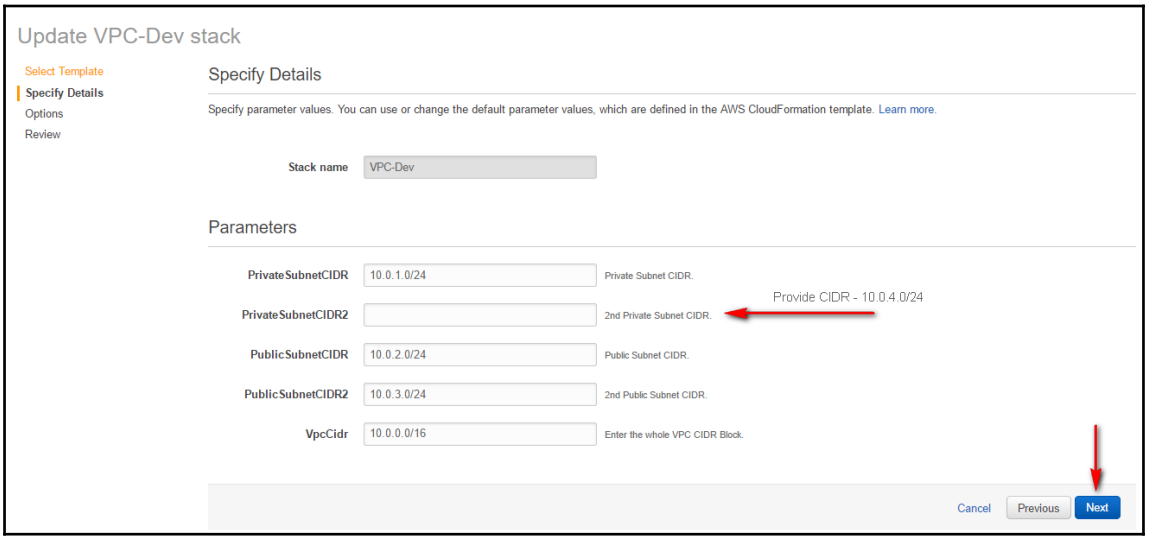

Execute change set
Are you sure you want to execute the UpdatePublicSubnet change set to update the VPC-Dev stack?
Cancel
Execute

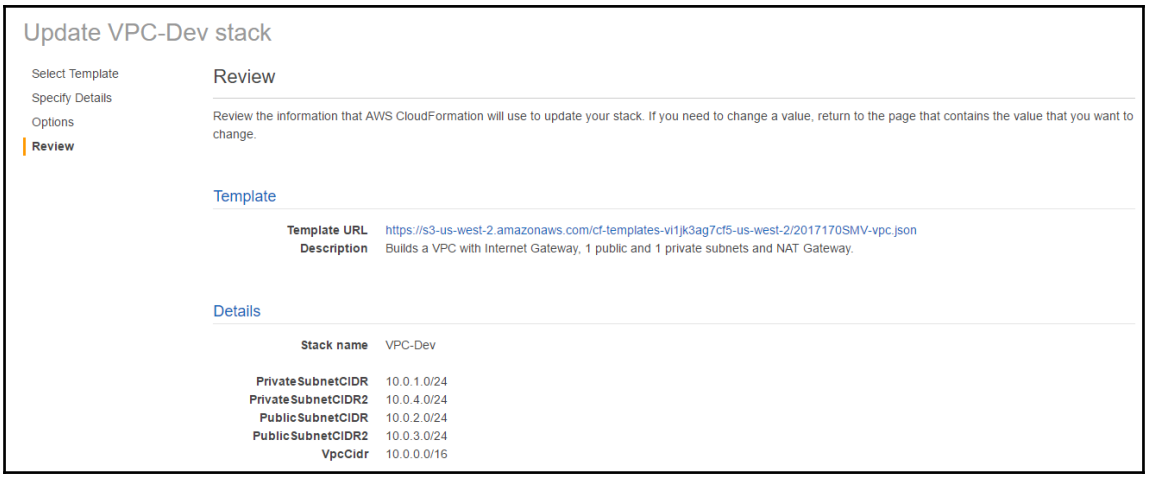

Create Stack
Actions
Design template
Filter: Active
By Stack Name
Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
UPDATE_IN_PROGRESS
Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
The stack was updated with UpdatePublicSubnet change set at 2017-06-19 12:41:28 UTC+0550.
Name
Created time
Status
Description
There are no executable change sets. Your stack must be in an updatable state to use change sets.

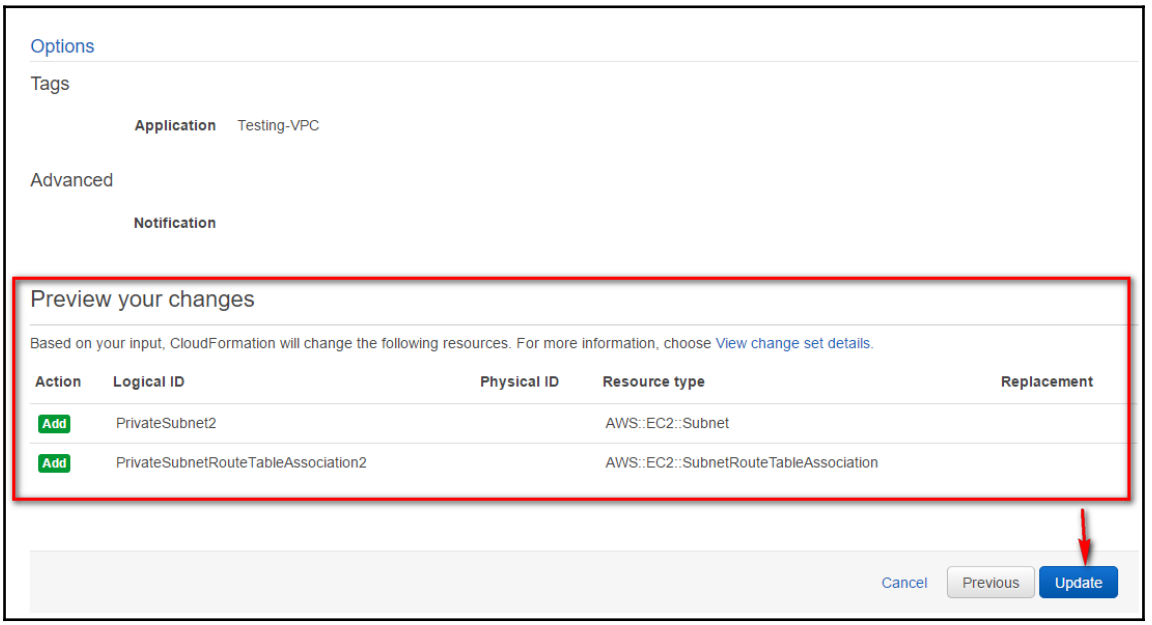

Stack Name
Created Time
Status
Description
VPC-Dev
2017-06-18 22:08:04 UTC+0550
UPDATE_COMPLETE
Builds a VPC with Internet Gateway, 1 public and 1
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Key
Value
Description
PrivateSubnet
subnet-b2f3f7d5
Private Subnet in AZ B
ElasticIP
34.211.40.196
Elastic IP attached to the NAT
VpcId
vpc-8c37dcea
VPC ID of newly created VPC
NATGateway
nat-0b11ba5ec9549d258
NAT Gateway for Private Subnet
InternetGateway
igw-8313b2e4
Internet Gateway attached to the VPC
PublicSubnet2
subnet-9e0205f9
2nd Public Subnet in AZ B
PublicSubnet
subnet-6eabf427
1st Public Subnet in AZ A

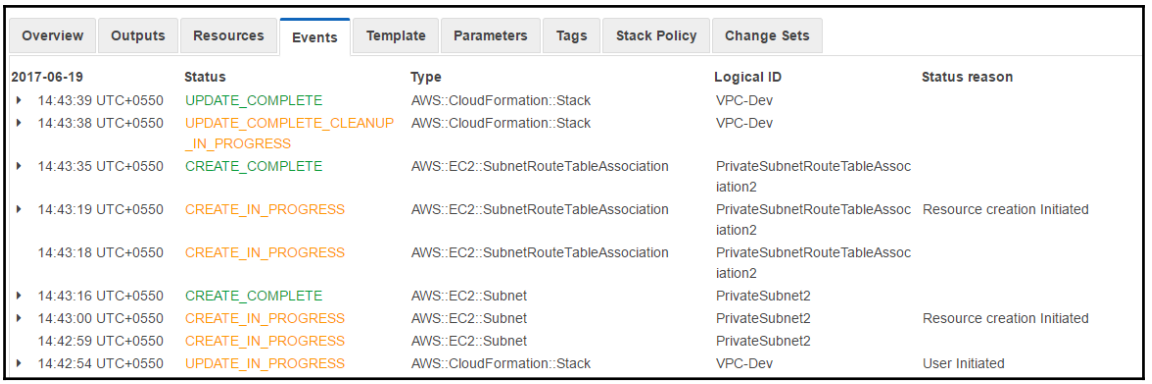

Create Stack
Actions
Design template
Filter: Active
Create Change Set For Current Stack
Update Stack
Delete Stack
View/Edit template in Designer
Stack Name
VPC-Dev


Update VPC-Dev stack
Select Template
Specify Details
Options
Review
Select Template
To update an existing stack, provide a template that specifies the changes for the resources and properties that you want to update. AWS CloudFormation updates only the resources that have changed. Learn more.
Choose a template
A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.
Use current template
Upload a template to Amazon S3
Choose File
vpc.json
Specify an Amazon S3 template URL
Cancel
Next


Update VPC-Dev stack
Select Template
Specify Details
Options
Review
Specify Details
Specify parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.
Stack name
VPC-Dev
Parameters
PrivateSubnetCIDR
10.0.1.0/24
Private Subnet CIDR.
Provide CIDR - 10.0.4.0/24
PrivateSubnetCIDR2
2nd Private Subnet CIDR.
PublicSubnetCIDR
10.0.2.0/24
Public Subnet CIDR.
PublicSubnetCIDR2
10.0.3.0/24
2nd Public Subnet CIDR.
VpcCidr
10.0.0.0/16
Enter the whole VPC CIDR Block.
Cancel
Previous
Next

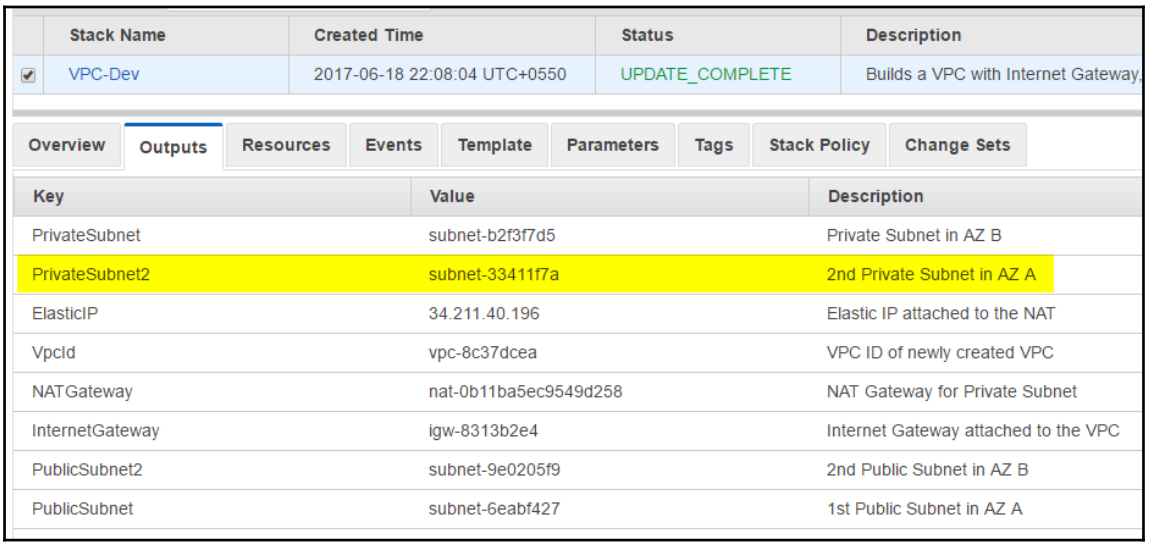

Update VPC-Dev stack
Select Template
Specify Details
Options
Review
Review
Review the information that AWS CloudFormation will use to update your stack. If you need to change a value, return to the page that contains the value that you want to change.
Template
Template URL https://s3-us-west-2.amazonaws.com/cf-templates-vi1jk3ag7cf5-us-west-2/2017170SMV-vpc.json
Description Builds a VPC with Internet Gateway, 1 public and 1 private subnets and NAT Gateway.
Details
Stack name VPC-Dev
PrivateSubnetCIDR 10.0.1.0/24
PrivateSubnetCIDR2 10.0.4.0/24
PublicSubnetCIDR 10.0.2.0/24
PublicSubnetCIDR2 10.0.3.0/24
VpcCidr 10.0.0.0/16


Options
Tags
Application Testing-VPC
Advanced
Notification
Preview your changes
Based on your input, CloudFormation will change the following resources. For more information, choose View change set details.
Action Logical ID Physical ID Resource type Replacement
Add PrivateSubnet2 AWS::EC2::Subnet
Add PrivateSubnetRouteTableAssociation2 AWS::EC2::SubnetRouteTableAssociation
Cancel
Previous
Update



Overview | Outputs | Resources | Events | Template | Parameters | Tags | Stack Policy | Change Sets

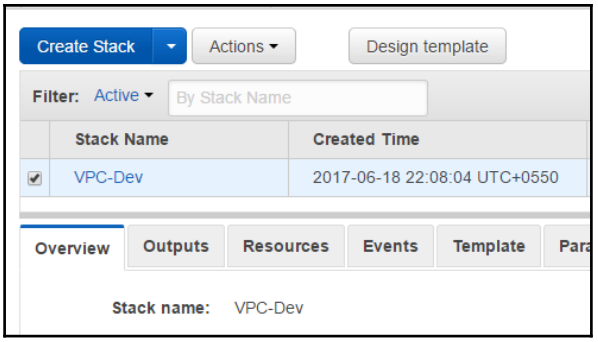
2017-06-19	Status	Type	Logical ID	Status reason
14:43:39 UTC+0550	UPDATE_COMPLETE	AWS::CloudFormation::Stack	VPC-Dev	
14:43:38 UTC+0550	UPDATE_COMPLETE_CLEANUP_IN_PROGRESS	AWS::CloudFormation::Stack	VPC-Dev	
14:43:35 UTC+0550	CREATE_COMPLETE	AWS::EC2::SubnetRouteTableAssociation	PrivateSubnetRouteTableAssociation2	
14:43:19 UTC+0550	CREATE_IN_PROGRESS	AWS::EC2::SubnetRouteTableAssociation	PrivateSubnetRouteTableAssociation2	Resource creation Initiated
14:43:18 UTC+0550	CREATE_IN_PROGRESS	AWS::EC2::SubnetRouteTableAssociation	PrivateSubnetRouteTableAssociation2	
14:43:16 UTC+0550	CREATE_COMPLETE	AWS::EC2::Subnet	PrivateSubnet2	
14:43:00 UTC+0550	CREATE_IN_PROGRESS	AWS::EC2::Subnet	PrivateSubnet2	Resource creation Initiated
14:42:59 UTC+0550	CREATE_IN_PROGRESS	AWS::EC2::Subnet	PrivateSubnet2	
14:42:54 UTC+0550	UPDATE_IN_PROGRESS	AWS::CloudFormation::Stack	VPC-Dev	User Initiated

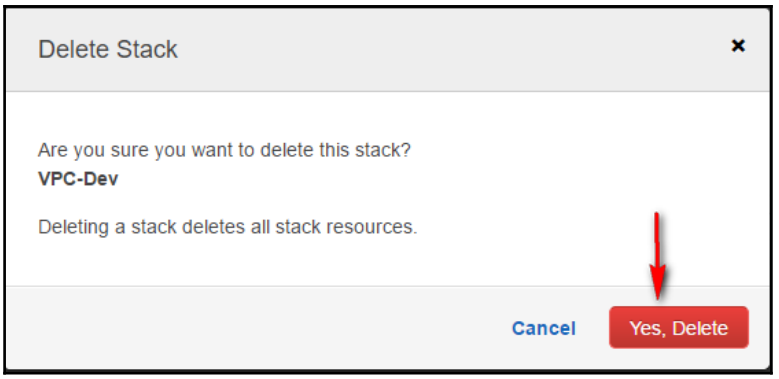


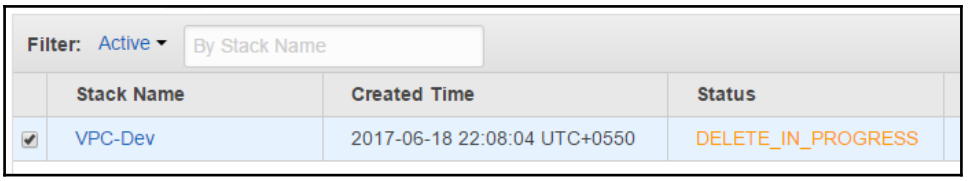
Stack Name	Created Time	Status	Description
VPC-Dev	2017-06-18 22:08:04 UTC+0550	UPDATE_COMPLETE	Builds a VPC with Internet Gateway,

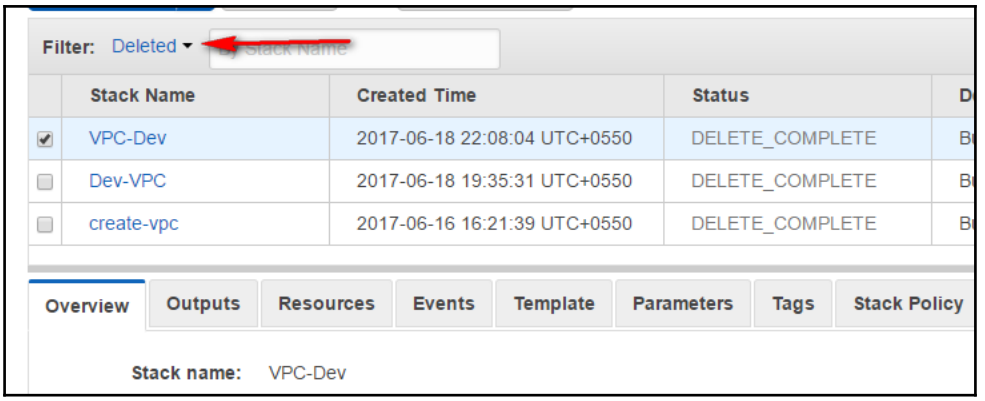
Overview | Outputs | Resources | Events | Template | Parameters | Tags | Stack Policy | Change Sets

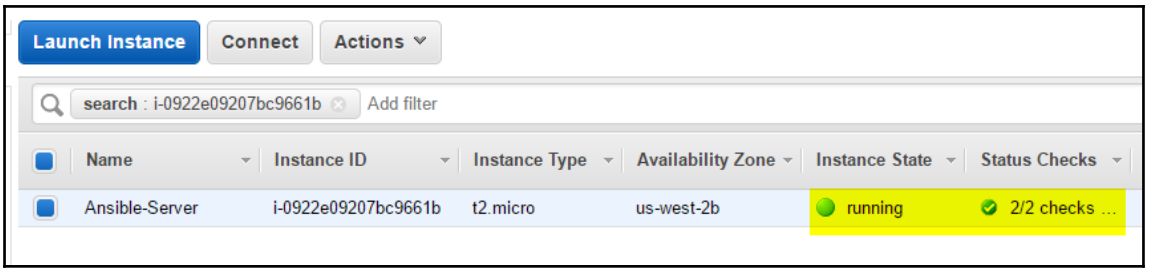
Key	Value	Description
PrivateSubnet	subnet-b2f3f7d5	Private Subnet in AZ B
PrivateSubnet2	subnet-33411f7a	2nd Private Subnet in AZ A
ElasticIP	34.211.40.196	Elastic IP attached to the NAT
VpcId	vpc-8c37dcea	VPC ID of newly created VPC
NATGateway	nat-0b11ba5ec9549d258	NAT Gateway for Private Subnet
InternetGateway	igw-8313b2e4	Internet Gateway attached to the VPC
PublicSubnet2	subnet-9e0205f9	2nd Public Subnet in AZ B
PublicSubnet	subnet-6eabf427	1st Public Subnet in AZ A

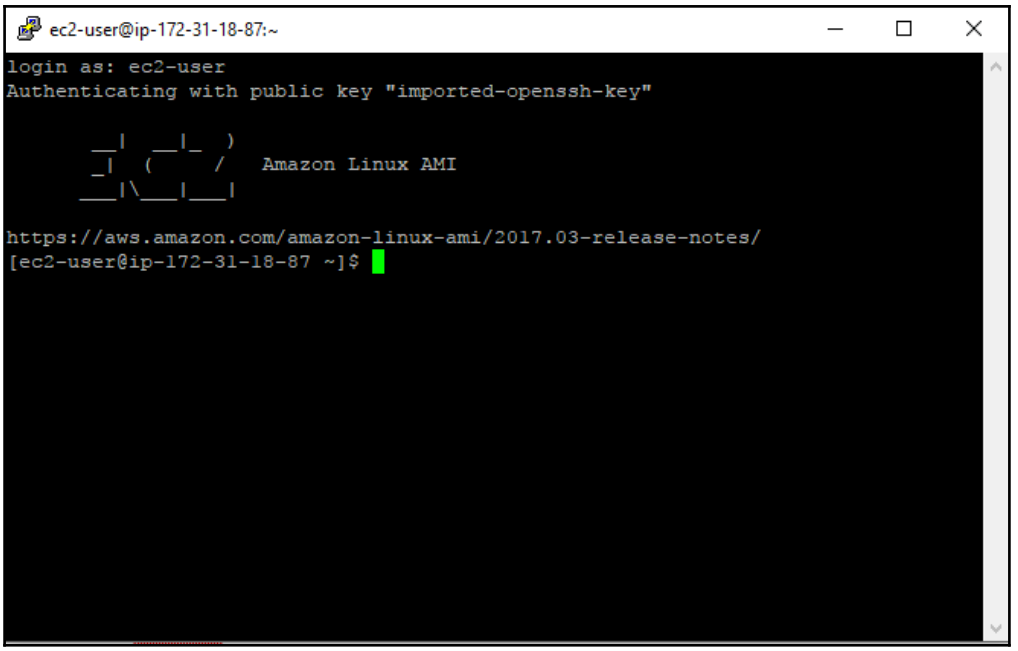


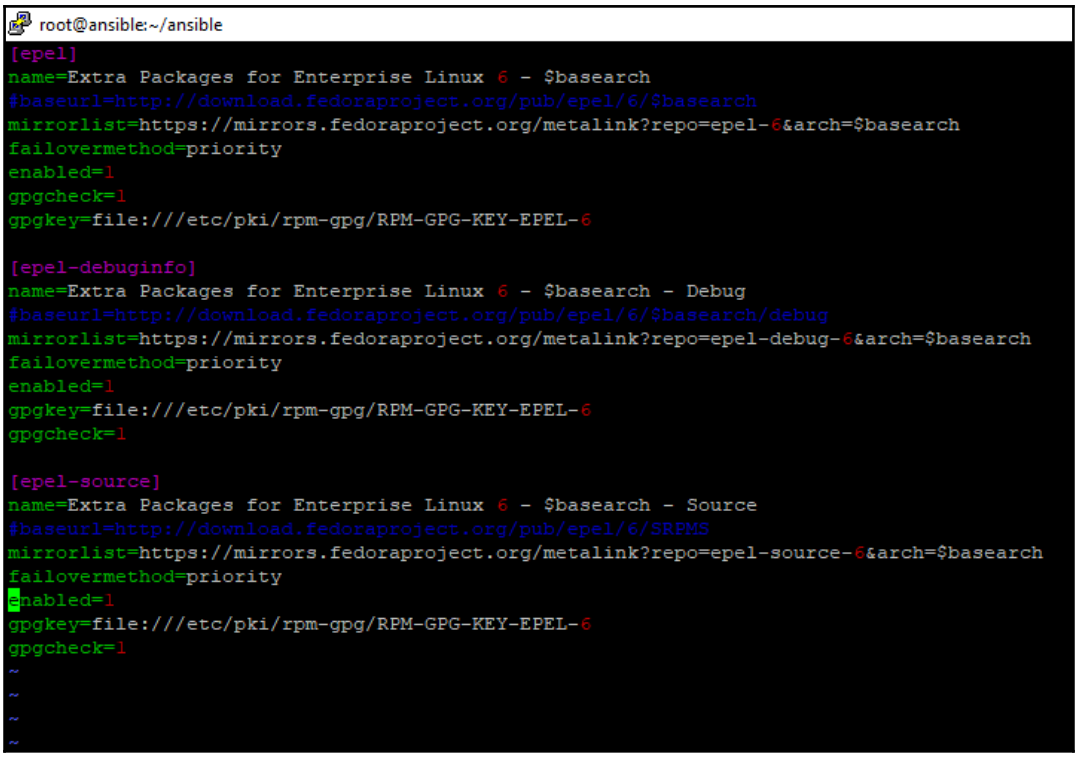

Delete Stack
Are you sure you want to delete this stack?
VPC-Dev
Deleting a stack deletes all stack resources.
Cancel
Yes, Delete

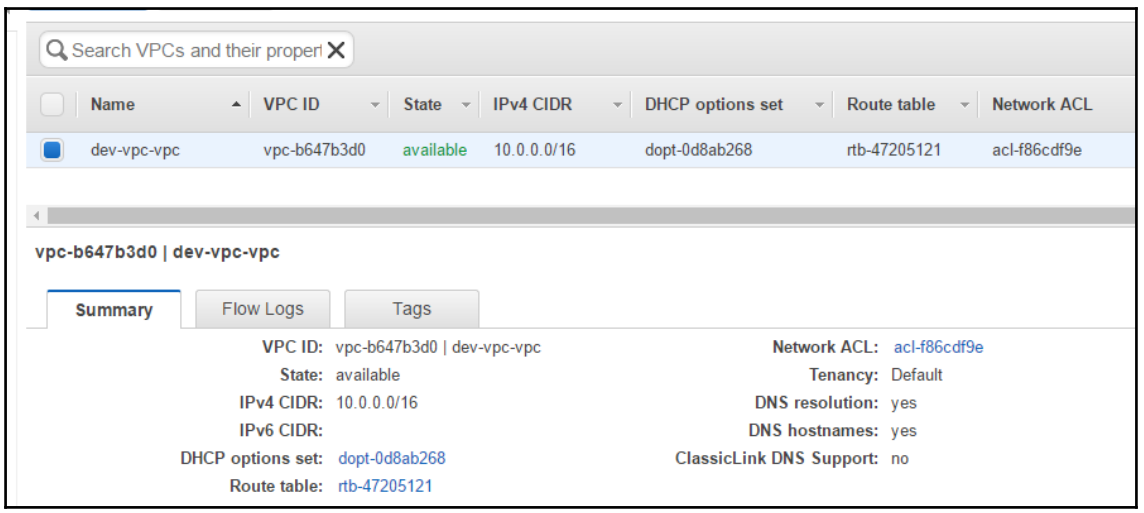

Filter: Active
By Stack Name
Stack Name
Created Time
Status
VPC-Dev
2017-06-18 22:08:04 UTC+0550
DELETE_IN_PROGRESS

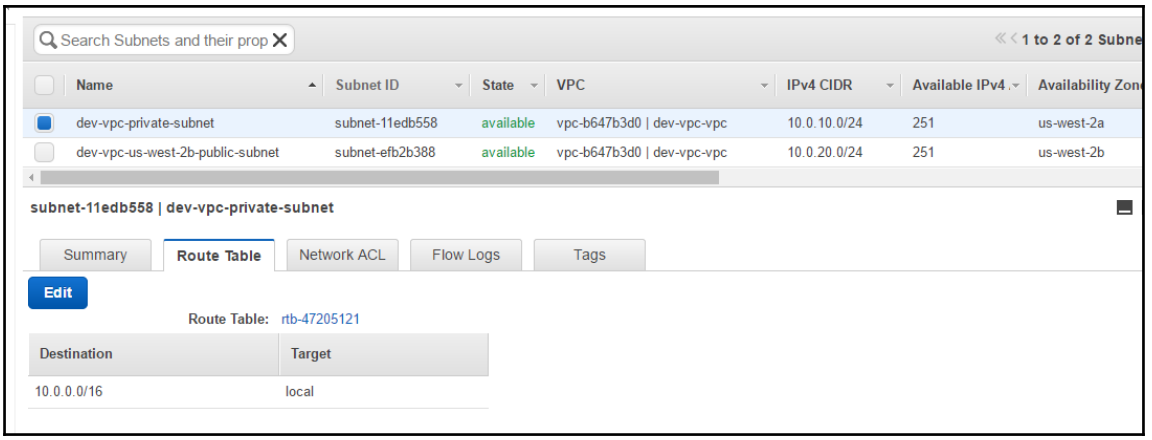

Filter: Deleted
Stack Name
Created Time
Status
VPC-Dev
2017-06-18 22:08:04 UTC+0550
DELETE_COMPLETE
Dev-VPC
2017-06-18 19:35:31 UTC+0550
DELETE_COMPLETE
create-vpc
2017-06-16 16:21:39 UTC+0550
DELETE_COMPLETE
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Stack name: VPC-Dev

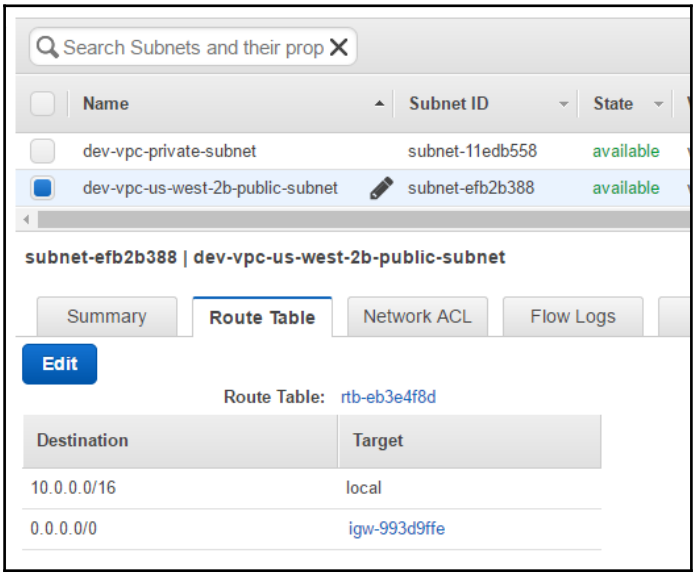

Launch Instance
Connect
Actions
search : i-0922e09207bc9661b
Add filter
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Ansible-Server
i-0922e09207bc9661b
t2.micro
us-west-2b
running
2/2 checks ...


ec2-user@ip-172-31-18-87:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2017.03-release-notes/
[ec2-user@ip-172-31-18-87 ~]$

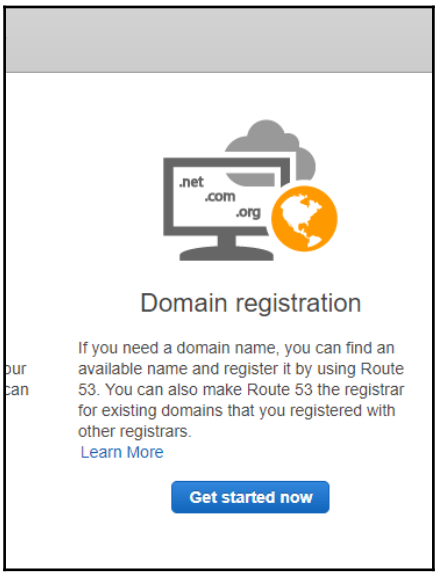

root@ansible:~/ansible
[epel]
name=Extra Packages for Enterprise Linux 6 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearch
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-6&arch=$basearch
failovermethod=priority
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
[epel-debuginfo]
name=Extra Packages for Enterprise Linux 6 - $basearch - Debug
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearch/debug
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-debug-6&arch=$basearch
failovermethod=priority
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
gpgcheck=1
[epel-source]
name=Extra Packages for Enterprise Linux 6 - $basearch - Source
#baseurl=http://download.fedoraproject.org/pub/epel/6/SRPMS
mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=epel-source-6&arch=$basearch
failovermethod=priority
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
gpgcheck=1

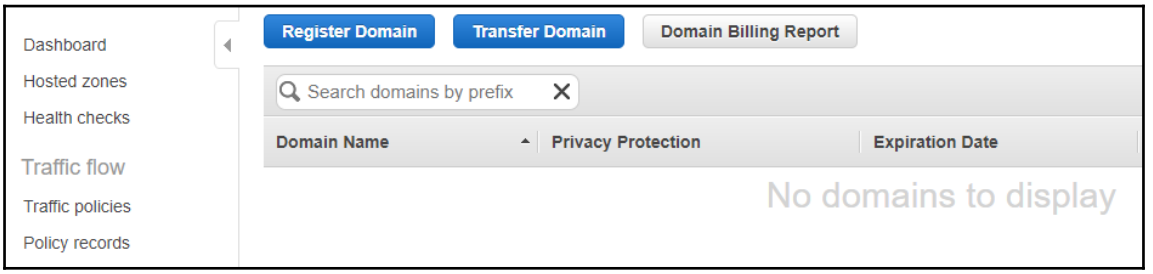

Search VPCs and their properl
Name
VPC ID
State
IPv4 CIDR
DHCP options set
Route table
Network ACL
dev-vpc-vpc
vpc-b647b3d0
available
10.0.0.0/16
dopt-0d8ab268
rtb-47205121
acl-f86cdf9e
vpc-b647b3d0 | dev-vpc-vpc
Summary
Flow Logs
Tags
VPC ID: vpc-b647b3d0 | dev-vpc-vpc
State: available
IPv4 CIDR: 10.0.0.0/16
IPv6 CIDR:
DHCP options set: dopt-0d8ab268
Route table: rtb-47205121
Network ACL: acl-f86cdf9e
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

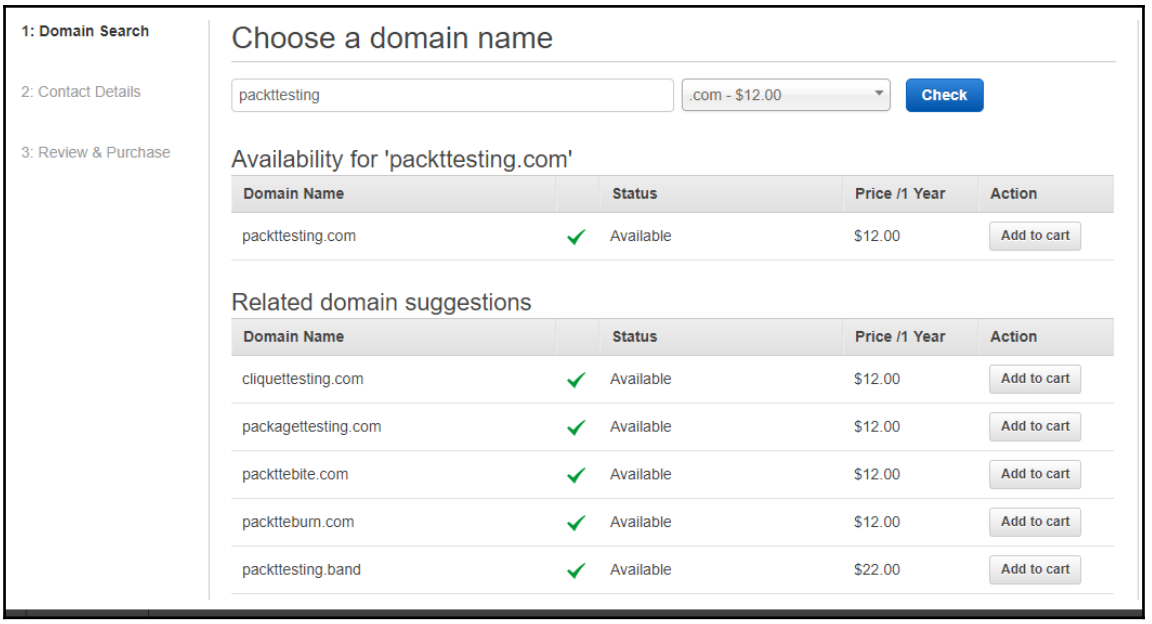

Search Subnets and their prop
1 to 2 of 2 Subne
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
Availability Zone
dev-vpc-private-subnet
subnet-11edb558
available
vpc-b647b3d0 | dev-vpc-vpc
10.0.10.0/24
251
us-west-2a
dev-vpc-us-west-2b-public-subnet
subnet-efb2b388
available
vpc-b647b3d0 | dev-vpc-vpc
10.0.20.0/24
251
us-west-2b
subnet-11edb558 | dev-vpc-private-subnet
Summary
Route Table
Network ACL
Flow Logs
Tags
Edit
Route Table: rtb-47205121
Destination
Target
10.0.0.0/16
local

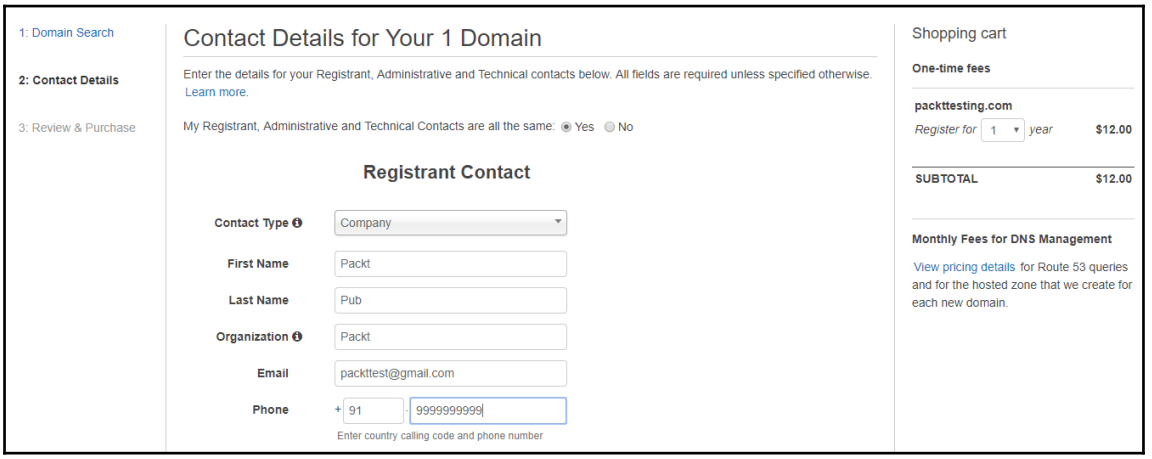

Search Subnets and their prop
Name
Subnet ID
State
dev-vpc-private-subnet
subnet-11edb558
available
dev-vpc-us-west-2b-public-subnet
subnet-efb2b388
available
subnet-efb2b388 | dev-vpc-us-west-2b-public-subnet
Summary
Route Table
Network ACL
Flow Logs
Edit
Route Table: rtb-eb3e4f8d
Destination
Target
10.0.0.0/16
local
0.0.0.0/0
igw-993d9ffe

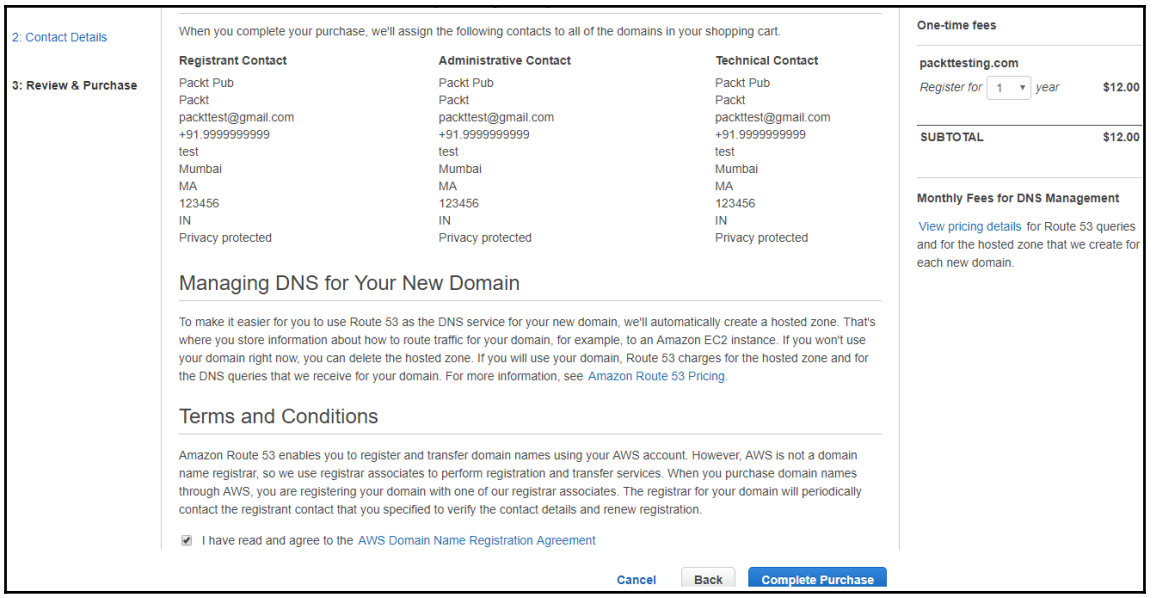
Chapter 6: Working with Route 53

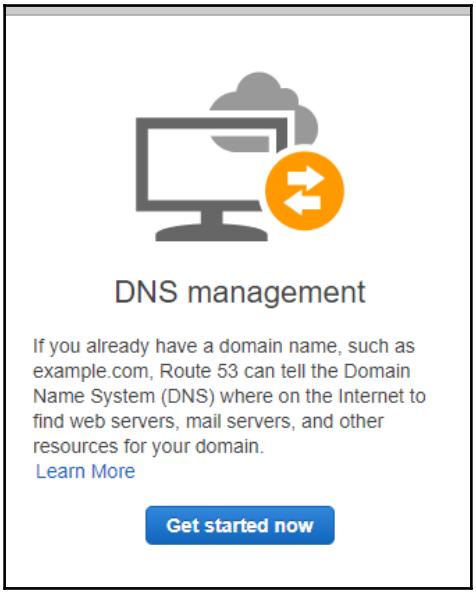


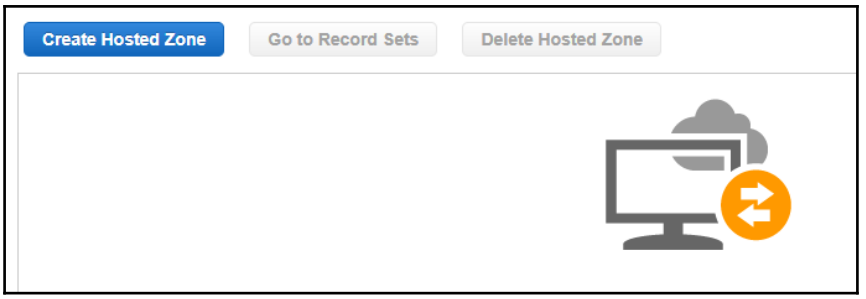


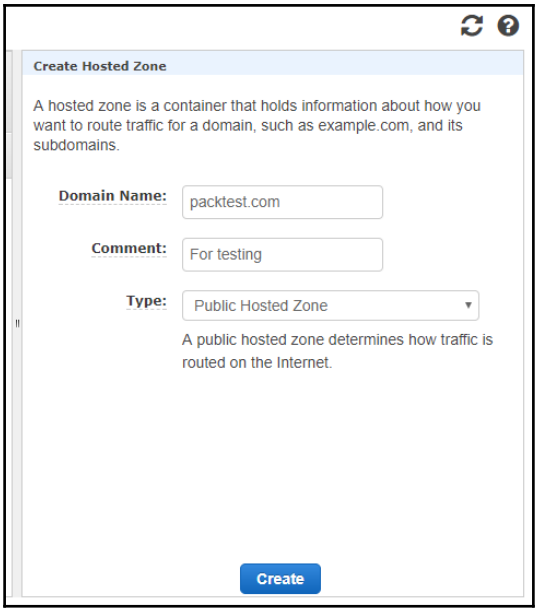

1: Domain Search
2: Contact Details
3: Review & Purchase
Choose a domain name
packttesting
.com - $12.00
Check
Availability for 'packttesting.com'
Domain Name
Status
Price /1 Year
Action
packttesting.com
Available
$12.00
Add to cart
Related domain suggestions
Domain Name
Status
Price /1 Year
Action
cliquettesting.com
Available
$12.00
Add to cart
packagettesting.com
Available
$12.00
Add to cart
packttebite.com
Available
$12.00
Add to cart
packtteburn.com
Available
$12.00
Add to cart
packttesting.band
Available
$22.00
Add to cart

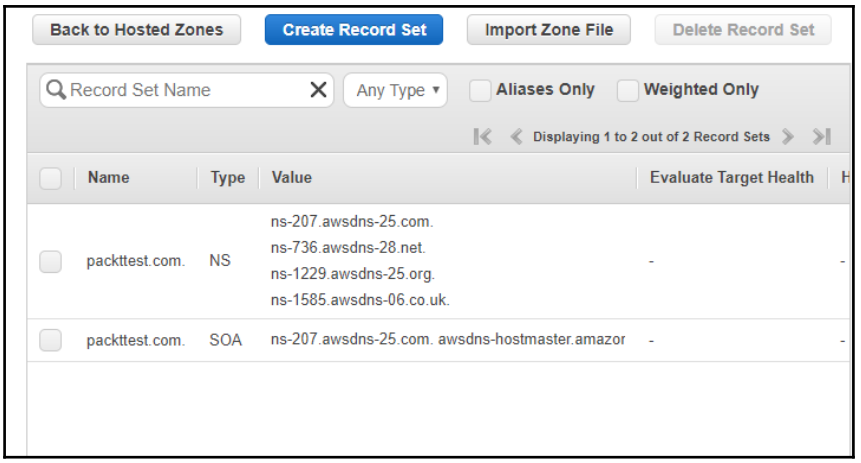

1: Domain Search
2: Contact Details
3: Review & Purchase
Contact Details for Your 1 Domain
Enter the details for your Registrant, Administrative and Technical contacts below. All fields are required unless specified otherwise.
Learn more.
My Registrant, Administrative and Technical Contacts are all the same: Yes No
Registrant Contact
Contact Type
Company
First Name
Packt
Last Name
Pub
Organization
Packt
Email
packttest@gmail.com
Phone
+ 91 9999999999
Enter country calling code and phone number
Shopping cart
One-time fees
packttesting.com
Register for 1 year
$12.00
SUBTOTAL
$12.00
Monthly Fees for DNS Management
View pricing details for Route 53 queries and for the hosted zone that we create for each new domain.

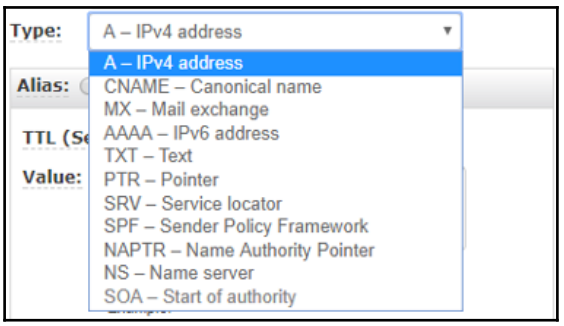

2: Contact Details
3: Review & Purchase
When you complete your purchase, we'll assign the following contacts to all of the domains in your shopping cart.
Registrant Contact
Packt Pub
Packt
packttest@gmail.com
+91.9999999999
test
Mumbai
MA
123456
IN
Privacy protected
Administrative Contact
Packt Pub
Packt
packttest@gmail.com
+91.9999999999
test
Mumbai
MA
123456
IN
Privacy protected
Technical Contact
Packt Pub
Packt
packttest@gmail.com
+91.9999999999
test
Mumbai
MA
123456
IN
Privacy protected
Managing DNS for Your New Domain
To make it easier for you to use Route 53 as the DNS service for your new domain, we'll automatically create a hosted zone. That's where you store information about how to route traffic for your domain, for example, to an Amazon EC2 instance. If you won't use your domain right now, you can delete the hosted zone. If you will use your domain, Route 53 charges for the hosted zone and for the DNS queries that we receive for your domain. For more information, see Amazon Route 53 Pricing.
Terms and Conditions
Amazon Route 53 enables you to register and transfer domain names using your AWS account. However, AWS is not a domain name registrar, so we use registrar associates to perform registration and transfer services. When you purchase domain names through AWS, you are registering your domain with one of our registrar associates. The registrar for your domain will periodically contact the registrant contact that you specified to verify the contact details and renew registration.
I have read and agree to the AWS Domain Name Registration Agreement
Cancel
Back
Complete Purchase
One-time fees
packttesting.com
Register for 1 year
$12.00
SUBTOTAL
$12.00
Monthly Fees for DNS Management
View pricing details for Route 53 queries and for the hosted zone that we create for each new domain.

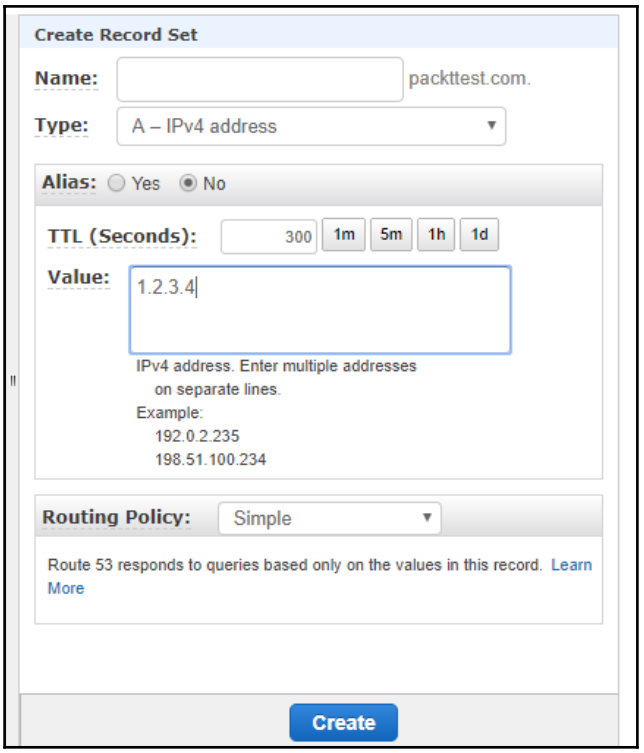

DNS management
If you already have a domain name, such as example.com, Route 53 can tell the Domain Name System (DNS) where on the Internet to find web servers, mail servers, and other resources for your domain.
Learn More
Get started now

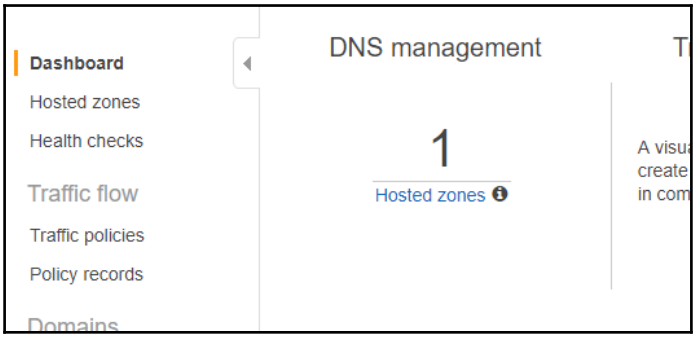

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone

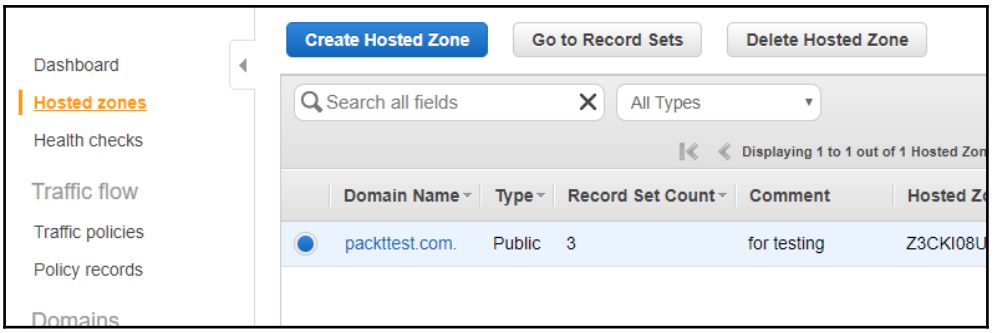

Create Hosted Zone
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.
Domain Name:
packtest.com
Comment:
For testing
Type:
Public Hosted Zone
A public hosted zone determines how traffic is routed on the Internet.
Create

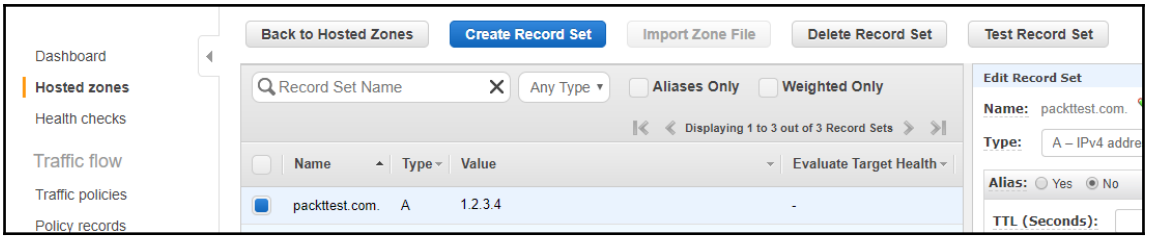

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 2 out of 2 Record Sets
Name
Type
Value
Evaluate Target Health
packttest.com.
NS
ns-207.awsdns-25.com.
ns-736.awsdns-28.net.
ns-1229.awsdns-25.org.
ns-1585.awsdns-06.co.uk.
packttest.com.
SOA
ns-207.awsdns-25.com. awsdns-hostmaster.amazor

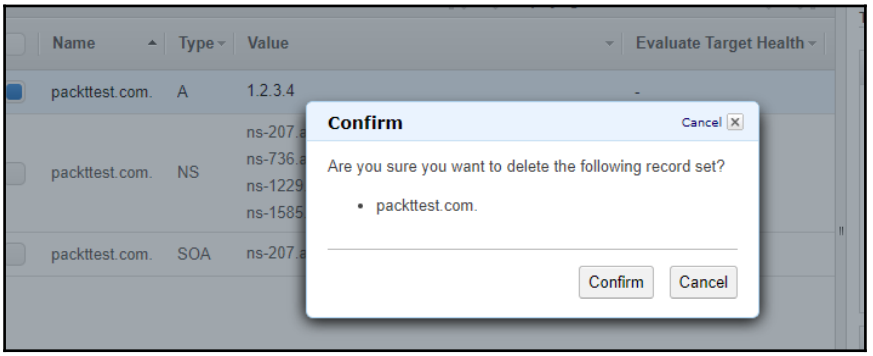

Type:
A – IPv4 address
Alias:
TTL (Se
Value:
A – IPv4 address
CNAME – Canonical name
MX – Mail exchange
AAAA – IPv6 address
TXT – Text
PTR – Pointer
SRV – Service locator
SPF – Sender Policy Framework
NAPTR – Name Authority Pointer
NS – Name server
SOA – Start of authority

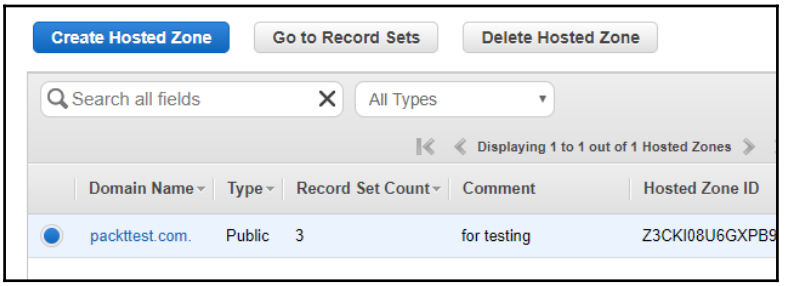

Create Record Set
Name:
packttest.com.
Type:
A – IPv4 address
Alias:
Yes
No
TTL (Seconds):
300
1m
5m
1h
1d
Value:
1.2.3.4
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234
Routing Policy:
Simple
Route 53 responds to queries based only on the values in this record. Learn More
Create

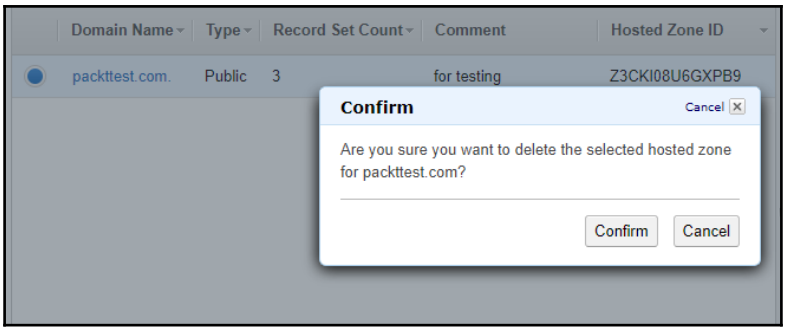

Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
DNS management
1
Hosted zones

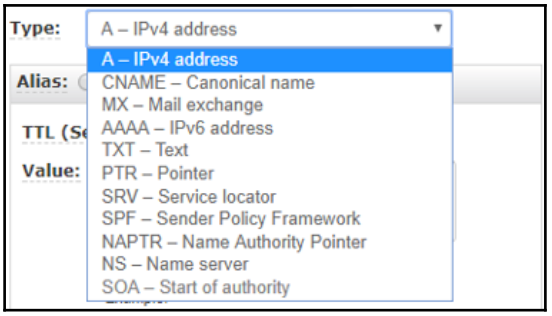

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Domains
Search all fields
All Types
Displaying 1 to 1 out of 1 Hosted Zon
Domain Name
Type
Record Set Count
Comment
Hosted Z
packttest.com.
Public
3
for testing
Z3CKI08U

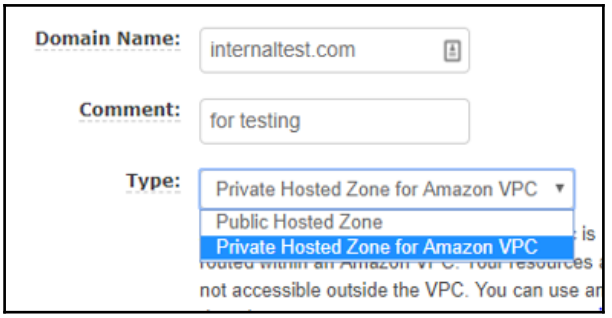

Back to Hosted Zones
Create Record Set
Import Zone File
Delete Record Set
Test Record Set
Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Record Set Name
Any Type
Aliases Only
Weighted Only
Displaying 1 to 3 out of 3 Record Sets
Name
Type
Value
Evaluate Target Health
packttest.com.
A
1.2.3.4
-
Edit Record Set
Name:
packttest.com.
Type:
A – IPv4 addre
Alias:
Yes
No
TTL (Seconds):

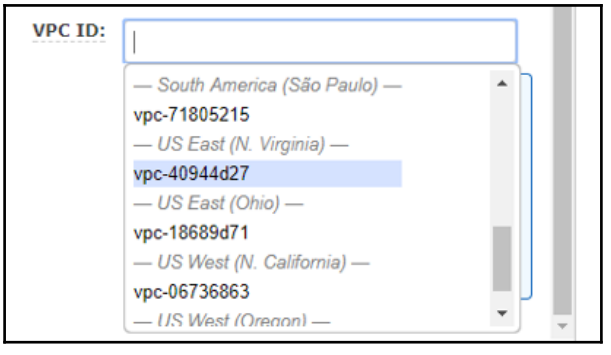

Name
Type
Value
Evaluate Target Health
packttest.com.
A
1.2.3.4
-
packttest.com.
NS
packttest.com.
SOA
Confirm
Cancel
Are you sure you want to delete the following record set?
packttest.com.
Confirm
Cancel

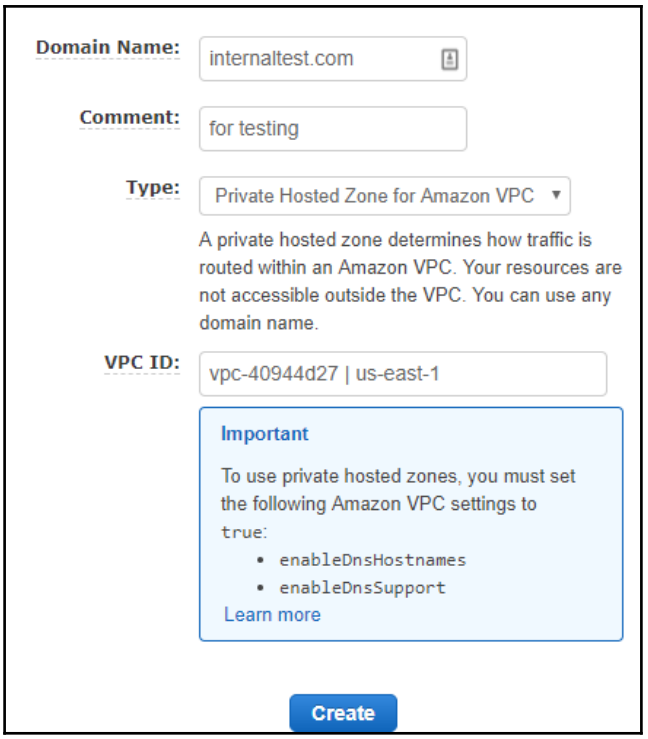

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Search all fields
All Types
Displaying 1 to 1 out of 1 Hosted Zones
Domain Name
Type
Record Set Count
Comment
Hosted Zone ID
packttest.com.
Public
3
for testing
Z3CKI08U6GXPB9

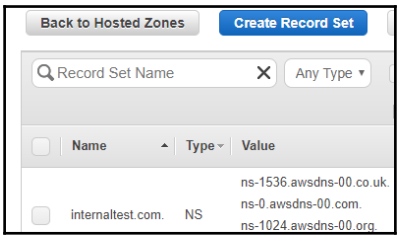

Domain Name
Type
Record Set Count
Comment
Hosted Zone ID
packttest.com.
Public
3
for testing
Z3CKI08U6GXPB9
Confirm
Cancel
Are you sure you want to delete the selected hosted zone for packttest.com?
Confirm
Cancel

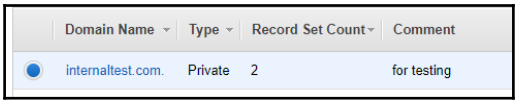

Type:
A – IPv4 address
Alias:
TTL (Se
Value:
A – IPv4 address
CNAME – Canonical name
MX – Mail exchange
AAAA – IPv6 address
TXT – Text
PTR – Pointer
SRV – Service locator
SPF – Sender Policy Framework
NAPTR – Name Authority Pointer
NS – Name server
SOA – Start of authority

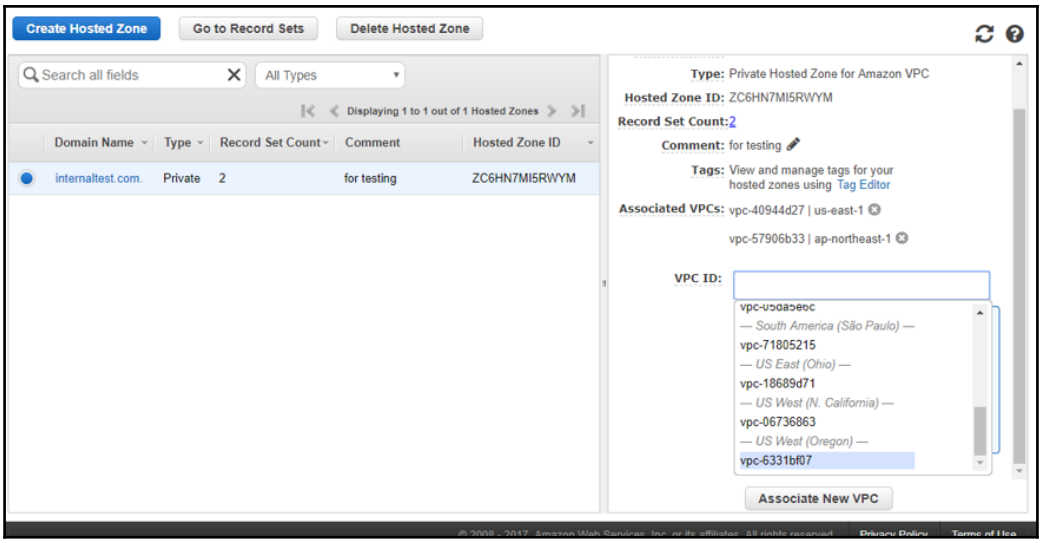

Domain Name:
internaltest.com
Comment:
for testing
Type:
Private Hosted Zone for Amazon VPC
Public Hosted Zone
Private Hosted Zone for Amazon VPC
not accessible outside the VPC. You can use ar

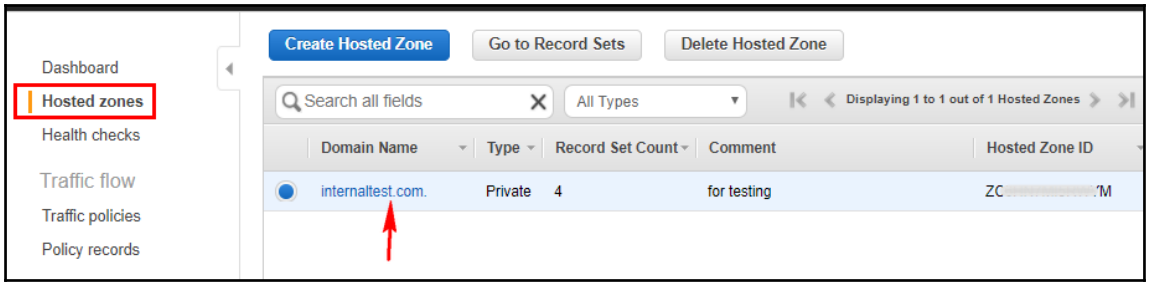

VPC ID:
— South America (São Paulo) —
vpc-71805215
— US East (N. Virginia) —
vpc-40944d27
— US East (Ohio) —
vpc-18689d71
— US West (N. California) —
vpc-06736863
— US West (Oregon) —

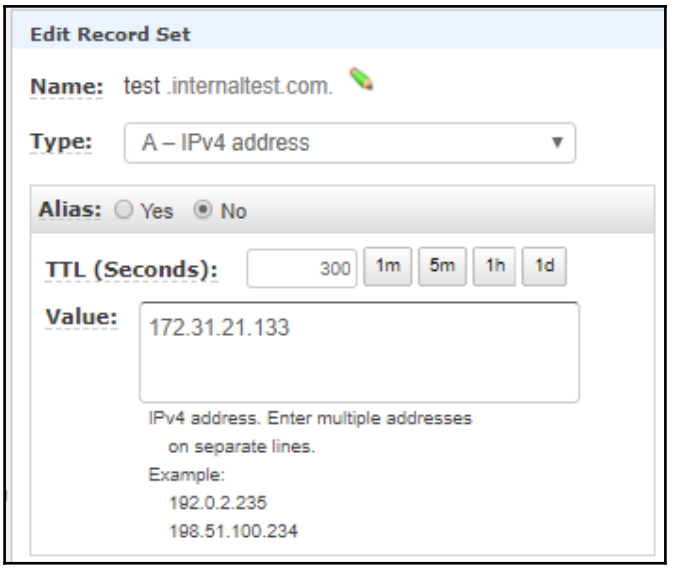

Domain Name:
internaltest.com
Comment:
for testing
Type:
Private Hosted Zone for Amazon VPC
A private hosted zone determines how traffic is routed within an Amazon VPC. Your resources are not accessible outside the VPC. You can use any domain name.
VPC ID:
vpc-40944d27 | us-east-1
Important
To use private hosted zones, you must set the following Amazon VPC settings to true:
enableDnsHostnames
enableDnsSupport
Learn more
Create

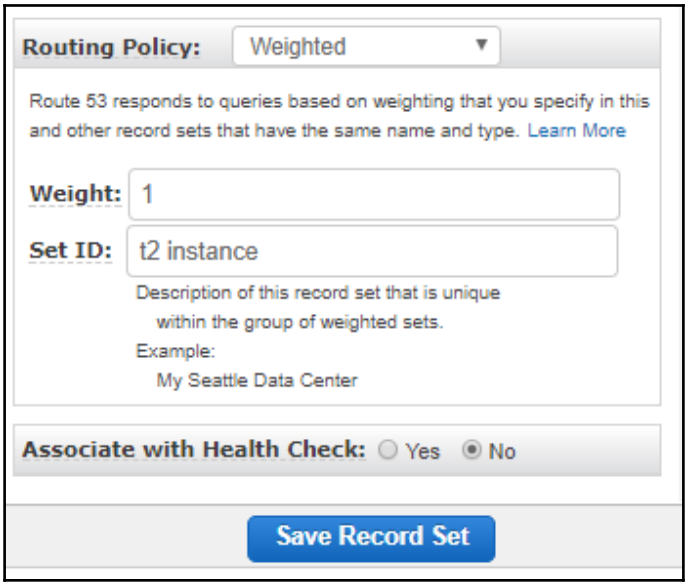

Back to Hosted Zones
Create Record Set
Record Set Name
Any Type
Name
Type
Value
internaltest.com.
NS
ns-1536.awsdns-00.co.uk.
ns-0.awsdns-00.com.
ns-1024.awsdns-00.org.

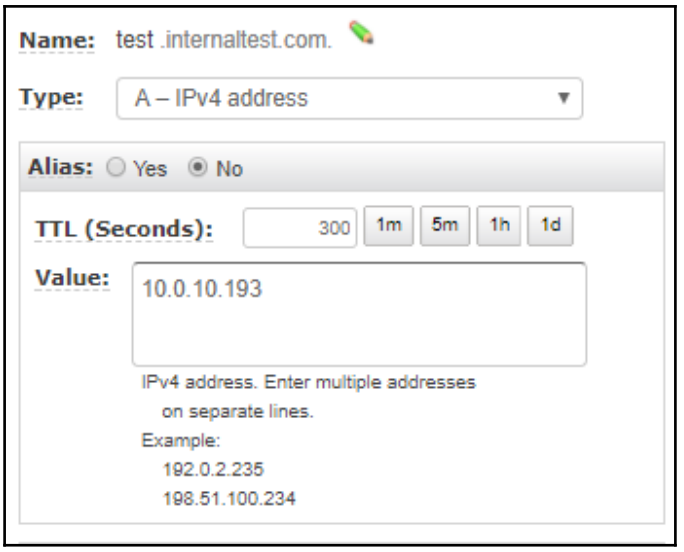

Domain Name
Type
Record Set Count
Comment
internaltest.com.
Private
2
for testing

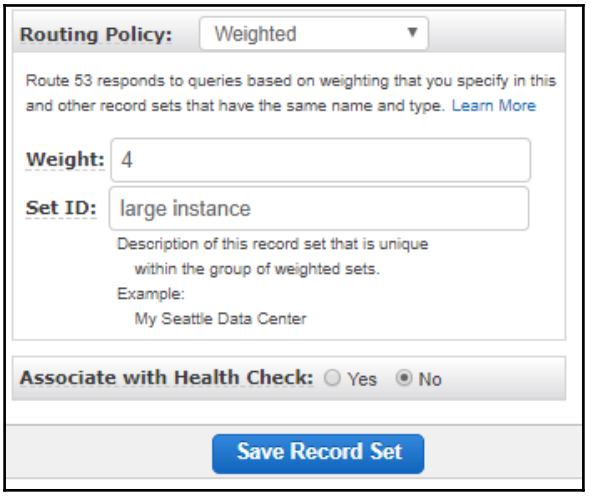

Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Search all fields
All Types
Displaying 1 to 1 out of 1 Hosted Zones
Domain Name
Type
Record Set Count
Comment
Hosted Zone ID
internaltest.com.
Private
2
for testing
ZC6HN7MI5RWYM
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: ZC6HN7MI5RWYM
Record Set Count: 2
Comment: for testing
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: vpc-40944d27 | us-east-1
vpc-57906b33 | ap-northeast-1
VPC ID:
— South America (São Paulo) —
vpc-71805215
— US East (Ohio) —
vpc-18689d71
— US West (N. California) —
vpc-06736863
— US West (Oregon) —
vpc-6331bf07
Associate New VPC


Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Create Hosted Zone
Go to Record Sets
Delete Hosted Zone
Search all fields
All Types
Displaying 1 to 1 out of 1 Hosted Zones
Domain Name
Type
Record Set Count
Comment
Hosted Zone ID
internaltest.com.
Private
4
for testing

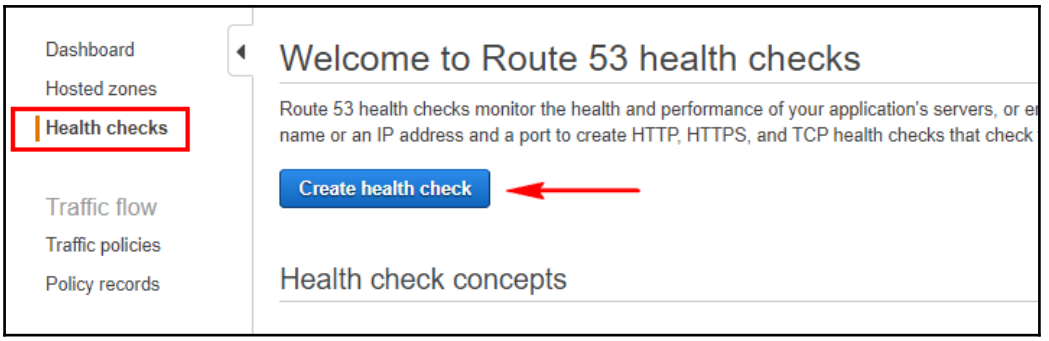

Edit Record Set
Name: test .internaltest.com.
Type: A – IPv4 address
Alias: Yes No
TTL (Seconds): 300 1m 5m 1h 1d
Value: 172.31.21.133
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234

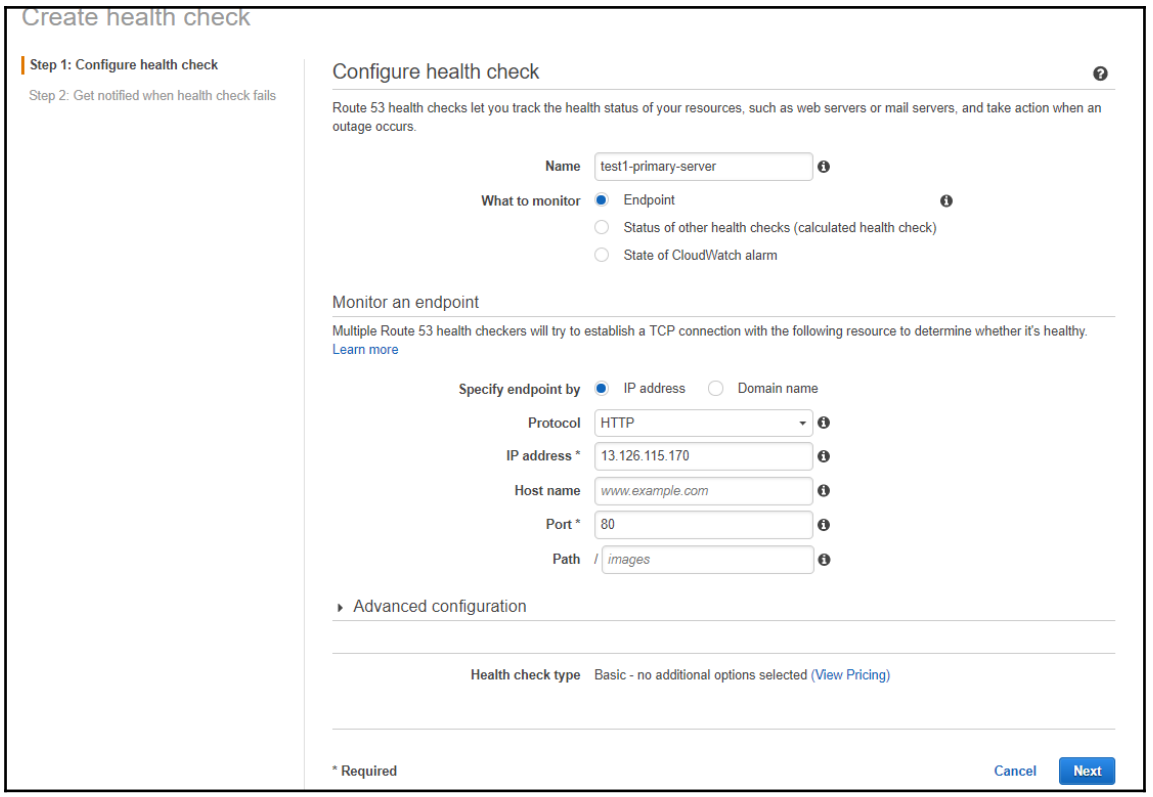

Routing Policy: Weighted
Route 53 responds to queries based on weighting that you specify in this and other record sets that have the same name and type. Learn More
Weight: 1
Set ID: t2 instance
Description of this record set that is unique within the group of weighted sets.
Example:
My Seattle Data Center
Associate with Health Check: Yes No
Save Record Set

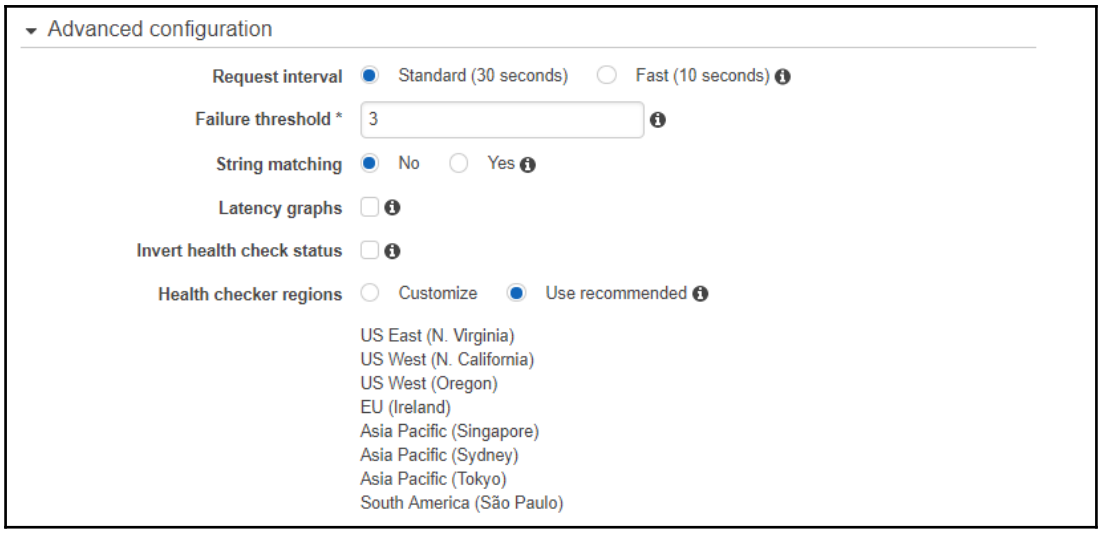


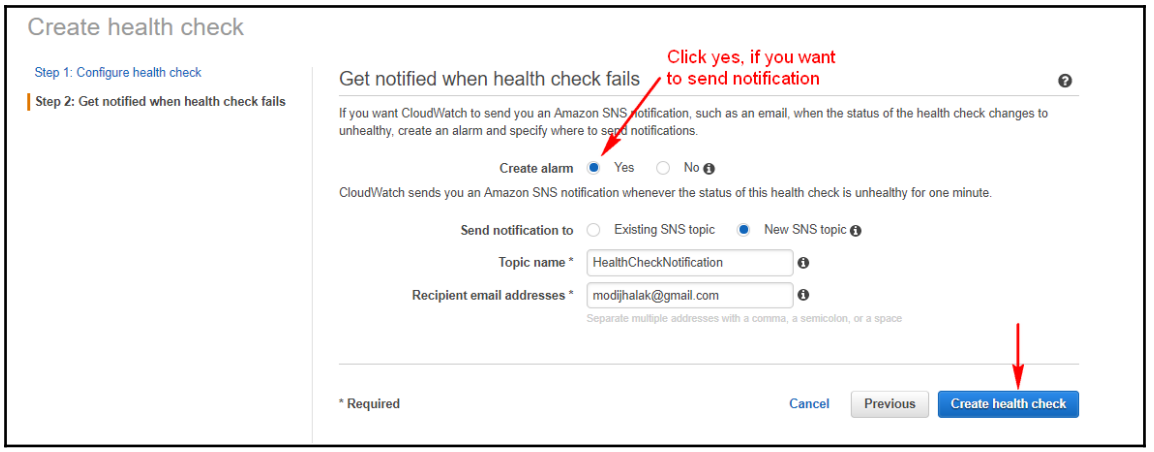


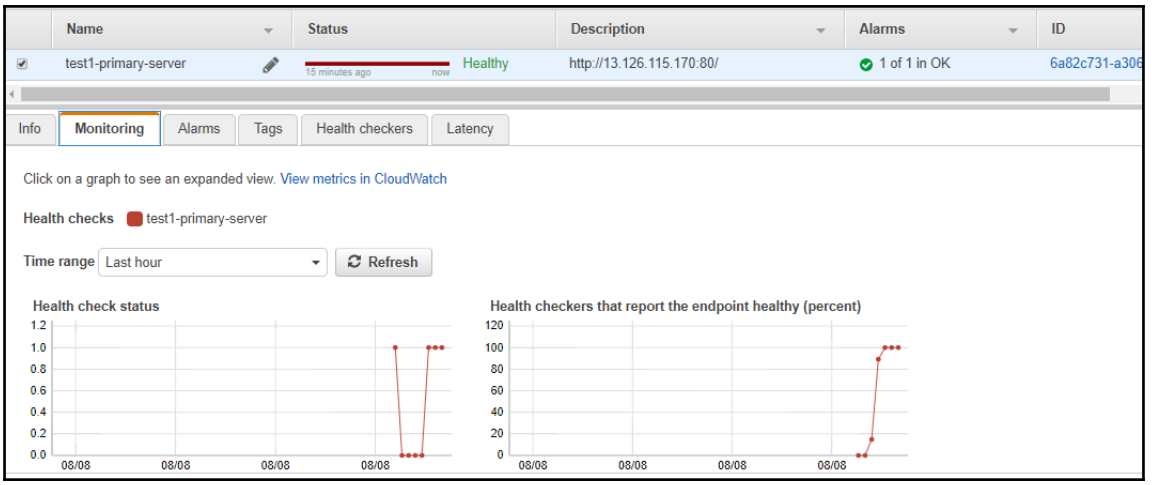
Name	Type	Value	TTL	Weight	Set ID
test.internaltest.com.	A	172.31.21.133	300	1	t2 instance
test.internaltest.com.	A	10.0.10.193	300	4	large instace

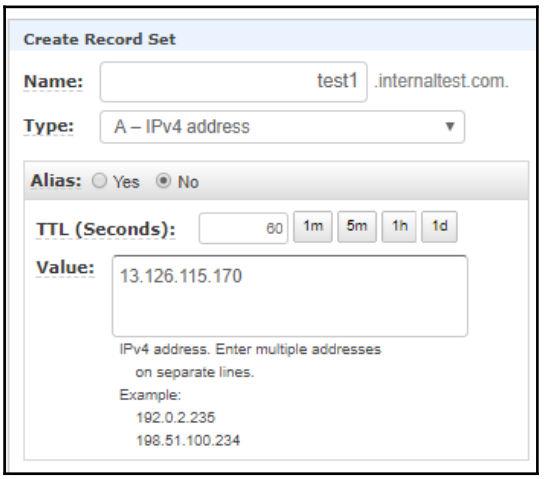

Dashboard
Hosted zones
Health checks
Traffic flow
Traffic policies
Policy records
Welcome to Route 53 health checks
Route 53 health checks monitor the health and performance of your application's servers, or e
name or an IP address and a port to create HTTP, HTTPS, and TCP health checks that check
Create health check
Health check concepts

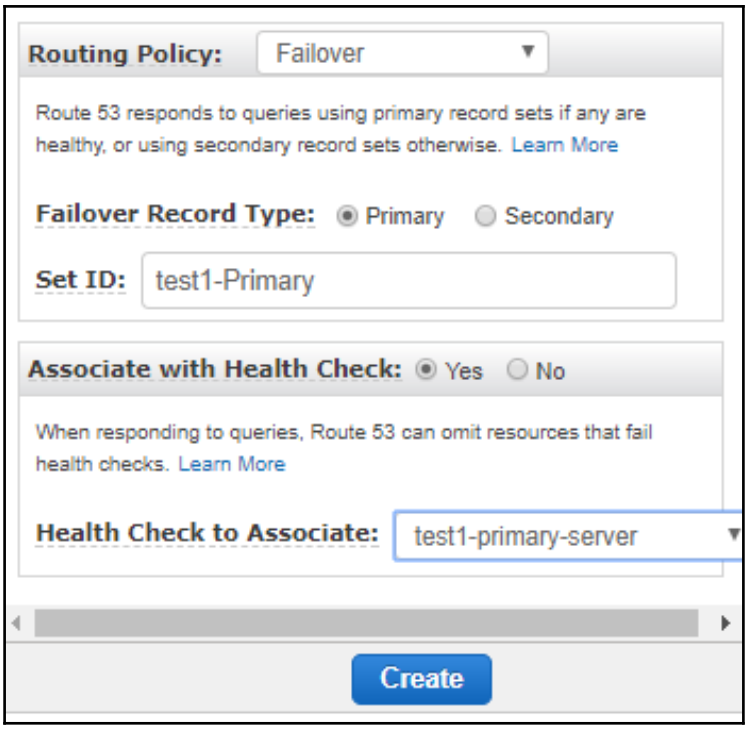

Create health check
Step 1: Configure health check
Step 2: Get notified when health check fails
Configure health check
Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.
Name
test1-primary-server
What to monitor
Endpoint
Status of other health checks (calculated health check)
State of CloudWatch alarm
Monitor an endpoint
Multiple Route 53 health checkers will try to establish a TCP connection with the following resource to determine whether it's healthy.
Learn more
Specify endpoint by
IP address
Domain name
Protocol
HTTP
IP address *
13.126.115.170
Host name
www.example.com
Port *
80
Path
/ images
Advanced configuration
Health check type
Basic - no additional options selected (View Pricing)
* Required
Cancel
Next

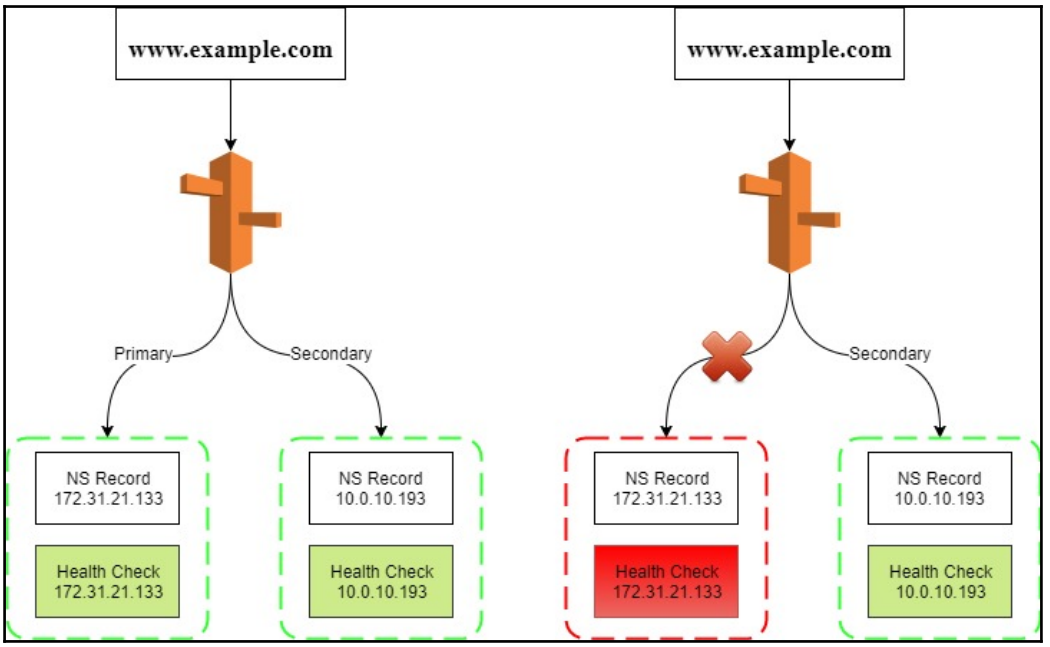

Advanced configuration
Request interval
Standard (30 seconds)
Fast (10 seconds)
Failure threshold *
3
String matching
No
Yes
Latency graphs
Invert health check status
Health checker regions
Customize
Use recommended
US East (N. Virginia)
US West (N. California)
US West (Oregon)
EU (Ireland)
Asia Pacific (Singapore)
Asia Pacific (Sydney)
Asia Pacific (Tokyo)
South America (São Paulo)

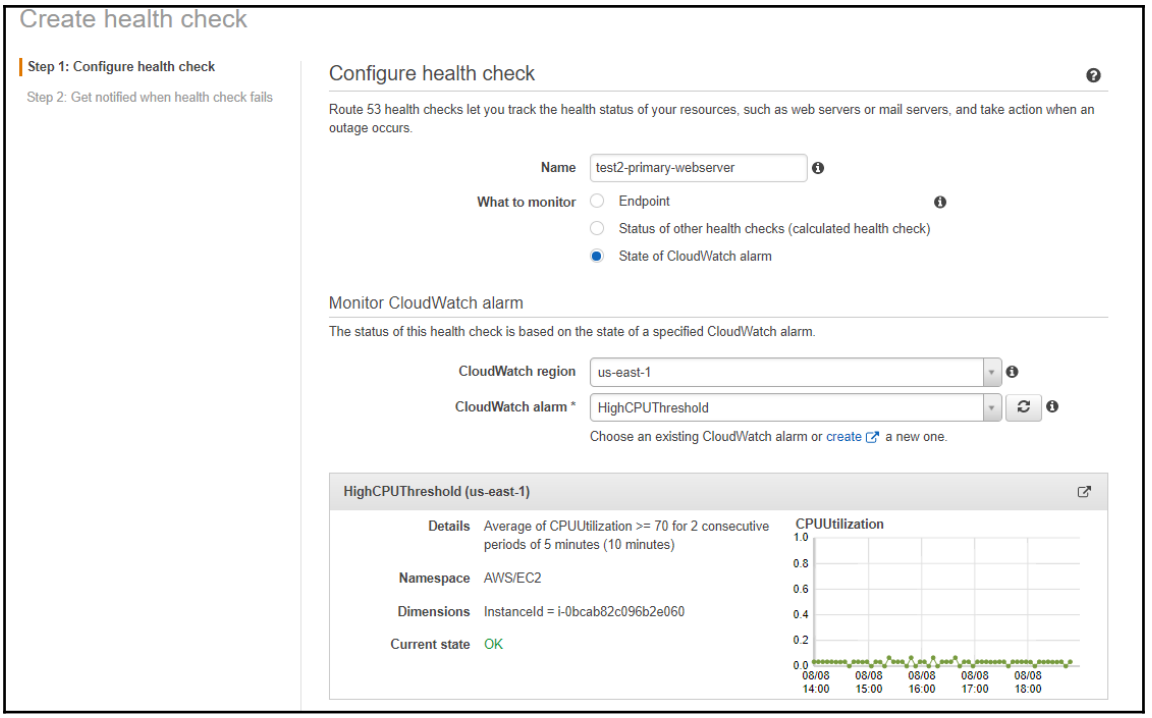

Create health check
Step 1: Configure health check
Step 2: Get notified when health check fails
Get notified when health check fails
Click yes, if you want to send notification
If you want CloudWatch to send you an Amazon SNS notification, such as an email, when the status of the health check changes to unhealthy, create an alarm and specify where to send notifications.
Create alarm
Yes
No
CloudWatch sends you an Amazon SNS notification whenever the status of this health check is unhealthy for one minute.
Send notification to
Existing SNS topic
New SNS topic
Topic name *
HealthCheckNotification
Recipient email addresses *
modijhalak@gmail.com
Separate multiple addresses with a comma, a semicolon, or a space
* Required
Cancel
Previous
Create health check


Name
Status
Description
Alarms
ID
test1-primary-server
15 minutes ago
now
Healthy
http://13.126.115.170:80/
1 of 1 in OK
6a82c731-a306
Info
Monitoring
Alarms
Tags
Health checkers
Latency
Click on a graph to see an expanded view. View metrics in CloudWatch
Health checks
test1-primary-server
Time range
Last hour
Refresh
Health check status
1.2
1.0
0.8
0.6
0.4
0.2
0.0
08/08
08/08
08/08
08/08
Health checkers that report the endpoint healthy (percent)
120
100
80
60
40
20
0
08/08
08/08
08/08
08/08

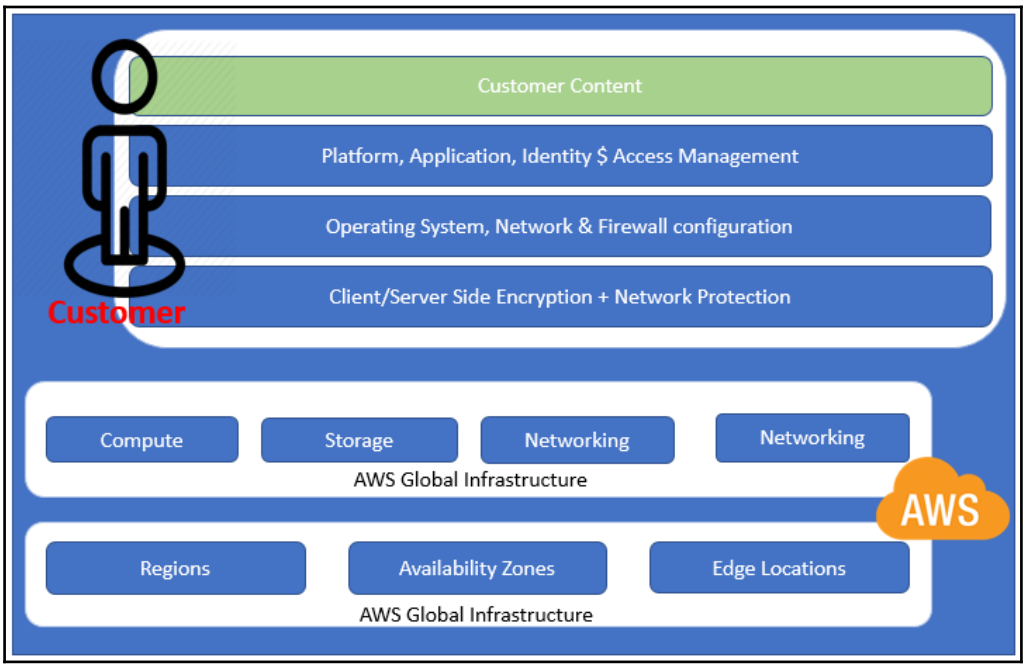

Create Record Set
Name:
test1
.internaltest.com.
Type:
A – IPv4 address
Alias:
Yes
No
TTL (Seconds):
60
1m
5m
1h
1d
Value:
13.126.115.170
IPv4 address. Enter multiple addresses
on separate lines.
Example:
192.0.2.235
198.51.100.234

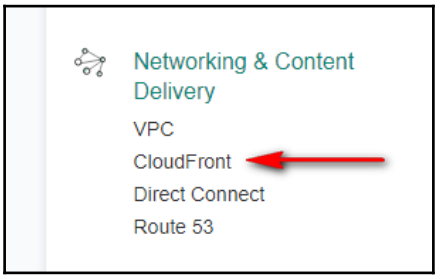

Routing Policy:
Failover
Route 53 responds to queries using primary record sets if any are healthy, or using secondary record sets otherwise. Learn More
Failover Record Type:
Primary
Secondary
Set ID:
test1-Primary
Associate with Health Check:
Yes
No
When responding to queries, Route 53 can omit resources that fail health checks. Learn More
Health Check to Associate:
test1-primary-server
Create

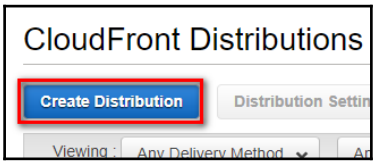

www.example.com
Primary
Secondary
NS Record
172.31.21.133
Health Check
172.31.21.133
NS Record
10.0.10.193
Health Check
10.0.10.193
www.example.com
Secondary
NS Record
172.31.21.133
Health Check
172.31.21.133
NS Record
10.0.10.193
Health Check
10.0.10.193

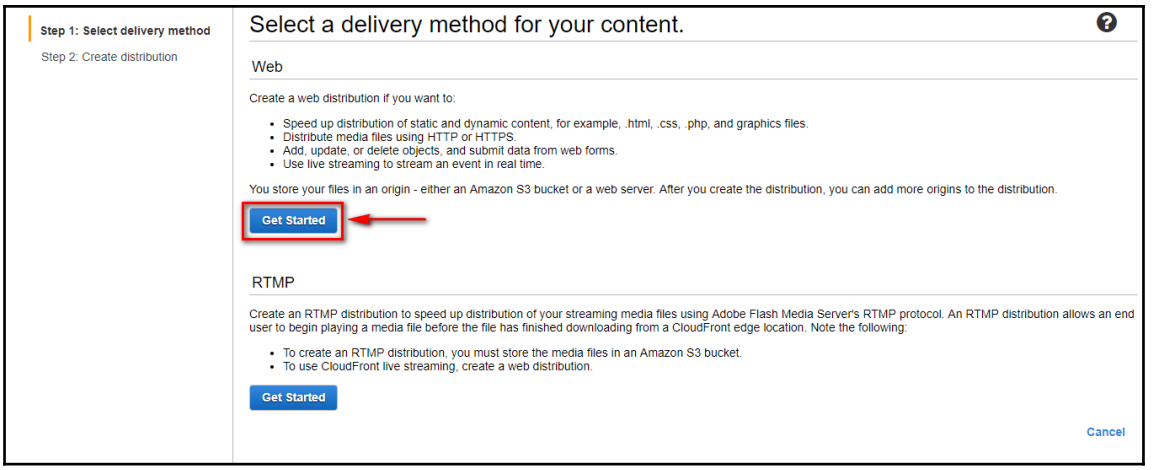

Create health check
Step 1: Configure health check
Step 2: Get notified when health check fails
Configure health check
Route 53 health checks let you track the health status of your resources, such as web servers or mail servers, and take action when an outage occurs.
Name
test2-primary-webserver
What to monitor
Endpoint
Status of other health checks (calculated health check)
State of CloudWatch alarm
Monitor CloudWatch alarm
The status of this health check is based on the state of a specified CloudWatch alarm.
CloudWatch region
us-east-1
CloudWatch alarm *
HighCPUThreshold
Choose an existing CloudWatch alarm or create a new one.
HighCPUThreshold (us-east-1)
Details
Average of CPUUtilization >= 70 for 2 consecutive periods of 5 minutes (10 minutes)
Namespace
AWS/EC2
Dimensions
InstanceId = i-0bcab82c096b2e060
Current state
OK
CPUUtilization
1.0
0.8
0.6
0.4
0.2
0.0
08/08 14:00
08/08 15:00
08/08 16:00
08/08 17:00
08/08 18:00

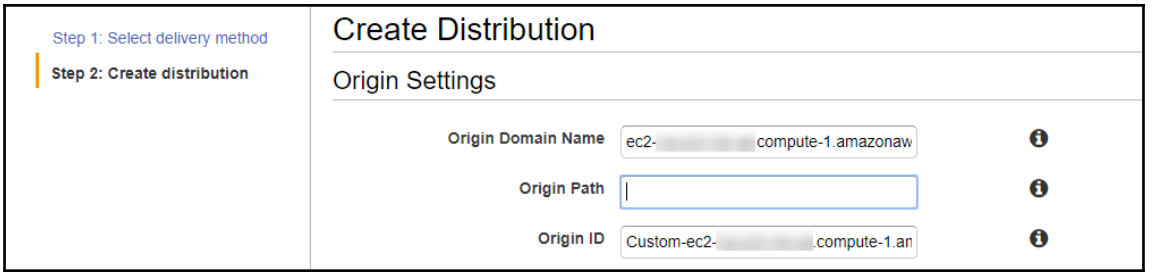
Chapter 7: Cloud Security and Network Compliance

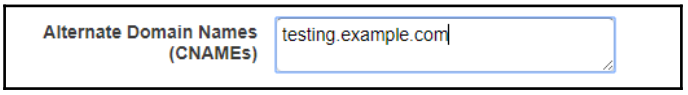


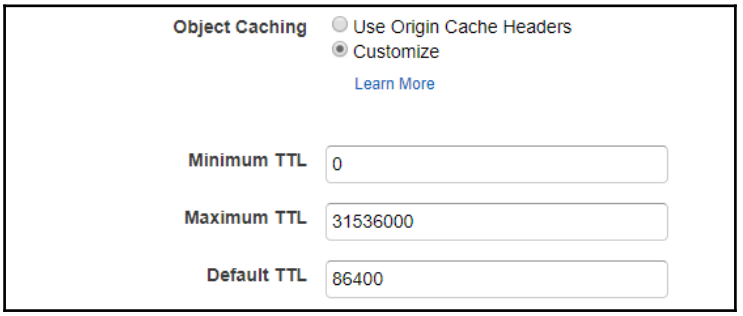


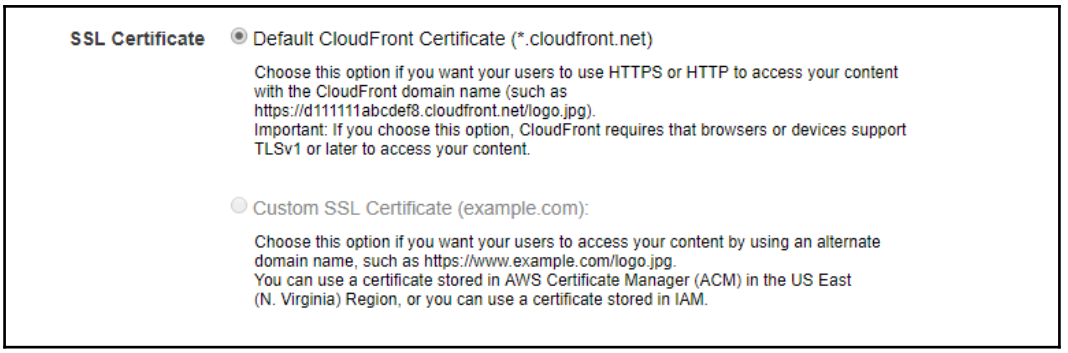


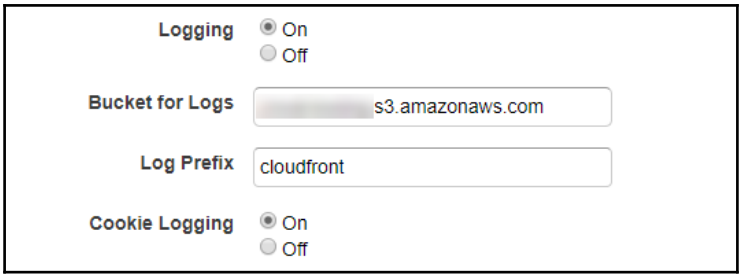

Step 1: Select delivery method
Step 2: Create distribution
Select a delivery method for your content.
Web
Create a web distribution if you want to:
Speed up distribution of static and dynamic content, for example, .html, .css, .php, and graphics files.
Distribute media files using HTTP or HTTPS.
Add, update, or delete objects, and submit data from web forms.
Use live streaming to stream an event in real time.
You store your files in an origin - either an Amazon S3 bucket or a web server. After you create the distribution, you can add more origins to the distribution.
Get Started
RTMP
Create an RTMP distribution to speed up distribution of your streaming media files using Adobe Flash Media Server's RTMP protocol. An RTMP distribution allows an end user to begin playing a media file before the file has finished downloading from a CloudFront edge location. Note the following:
To create an RTMP distribution, you must store the media files in an Amazon S3 bucket.
To use CloudFront live streaming, create a web distribution.
Get Started
Cancel

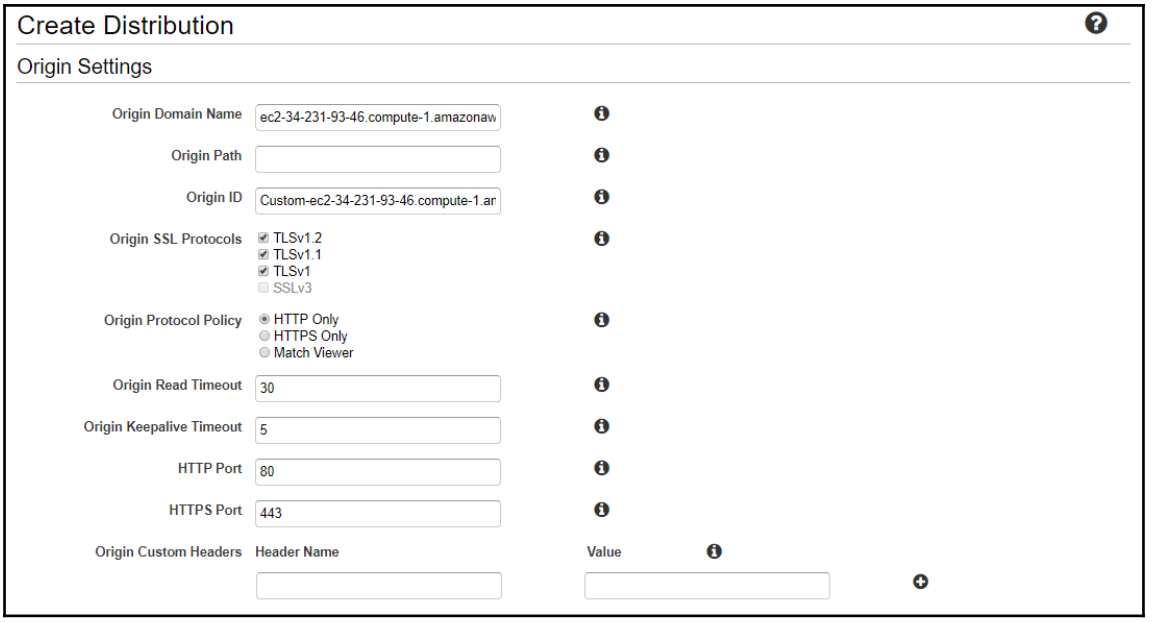

Step 1: Select delivery method
Step 2: Create distribution
Create Distribution
Origin Settings
Origin Domain Name
ec2-
compute-1.amazonaw
Origin Path
Origin ID
Custom-ec2-
.compute-1.an

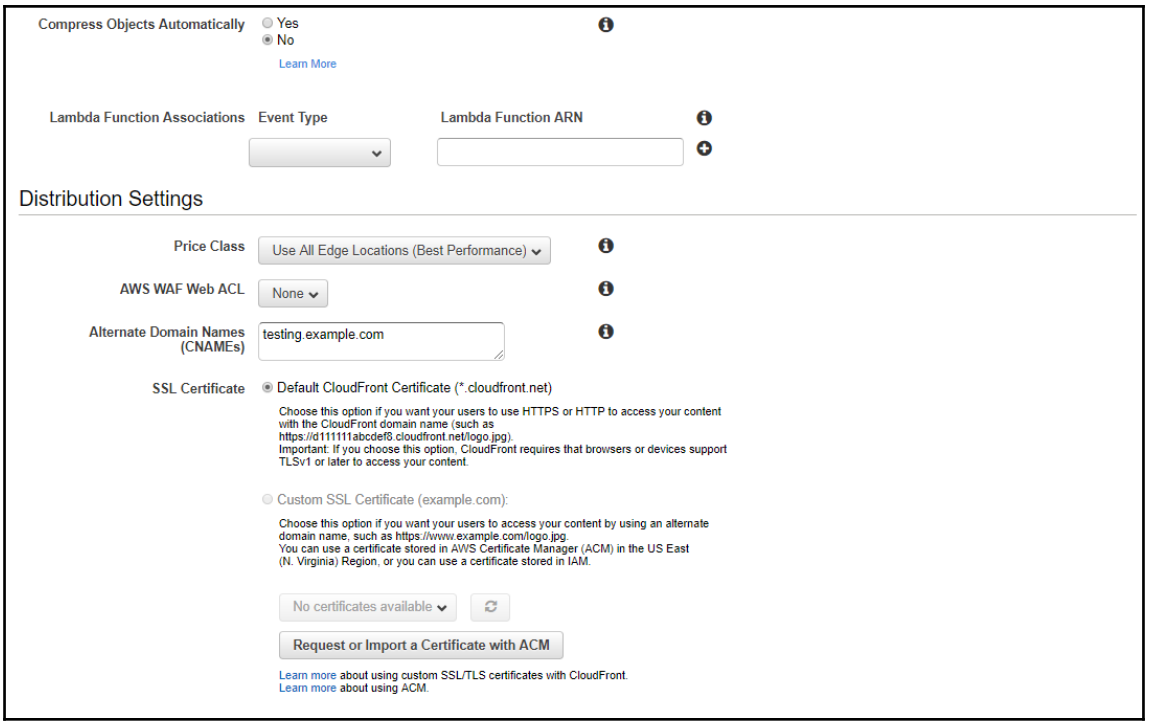

Alternate Domain Names (CNAMEs)
testing.example.com

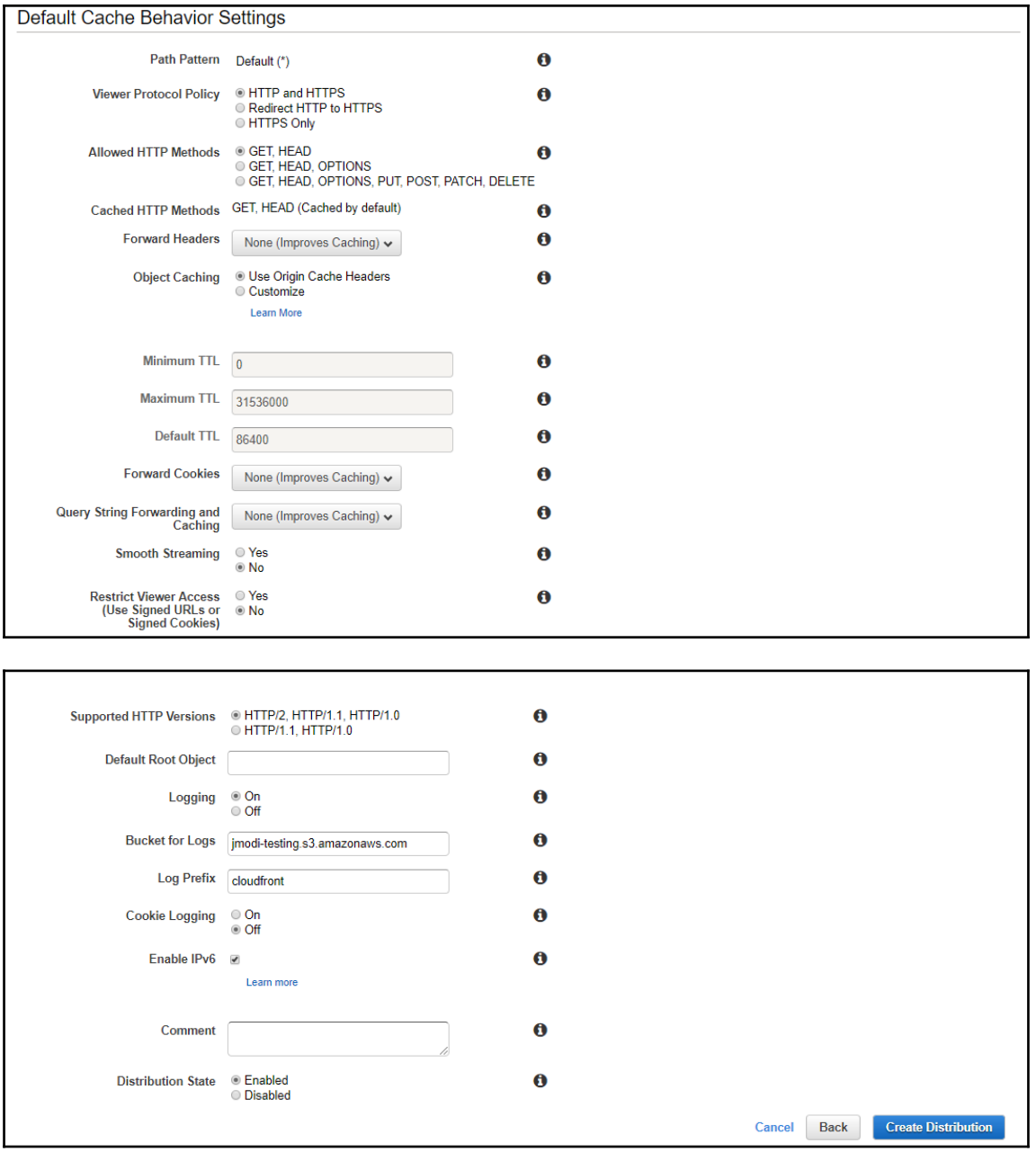

Object Caching
Use Origin Cache Headers
Customize
Learn More
Minimum TTL
0
Maximum TTL
31536000
Default TTL
86400


SSL Certificate
Default CloudFront Certificate (*.cloudfront.net)
Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.
Custom SSL Certificate (example.com):
Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.

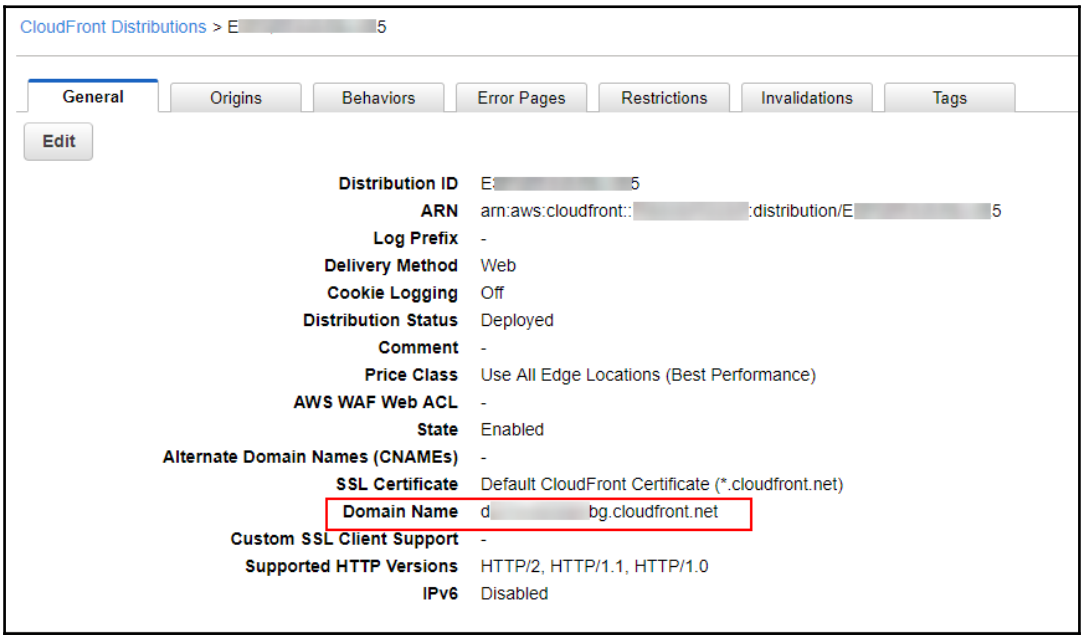

Logging
On
Off
Bucket for Logs
s3.amazonaws.com
Log Prefix
cloudfront
Cookie Logging
On
Off

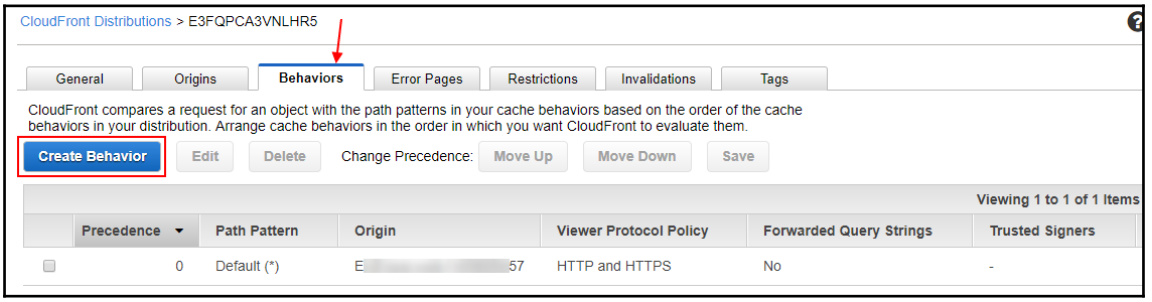

Create Distribution
Origin Settings
Origin Domain Name
ec2-34-231-93-46.compute-1.amazonaw
Origin Path
Origin ID
Custom-ec2-34-231-93-46.compute-1.ar
Origin SSL Protocols
TLSv1.2
TLSv1.1
TLSv1
SSLv3
Origin Protocol Policy
HTTP Only
HTTPS Only
Match Viewer
Origin Read Timeout
30
Origin Keepalive Timeout
5
HTTP Port
80
HTTPS Port
443
Origin Custom Headers
Header Name
Value

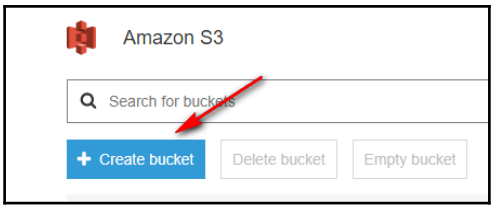

Compress Objects Automatically
Yes
No
Learn More
Lambda Function Associations
Event Type
Lambda Function ARN
Distribution Settings
Price Class
Use All Edge Locations (Best Performance)
AWS WAF Web ACL
None
Alternate Domain Names (CNAMEs)
testing.example.com
SSL Certificate
Default CloudFront Certificate (*.cloudfront.net)
Choose this option if you want your users to use HTTPS or HTTP to access your content with the CloudFront domain name (such as https://d111111abcdef8.cloudfront.net/logo.jpg).
Important: If you choose this option, CloudFront requires that browsers or devices support TLSv1 or later to access your content.
Custom SSL Certificate (example.com):
Choose this option if you want your users to access your content by using an alternate domain name, such as https://www.example.com/logo.jpg.
You can use a certificate stored in AWS Certificate Manager (ACM) in the US East (N. Virginia) Region, or you can use a certificate stored in IAM.
No certificates available
Request or Import a Certificate with ACM
Learn more about using custom SSL/TLS certificates with CloudFront.
Learn more about using ACM.

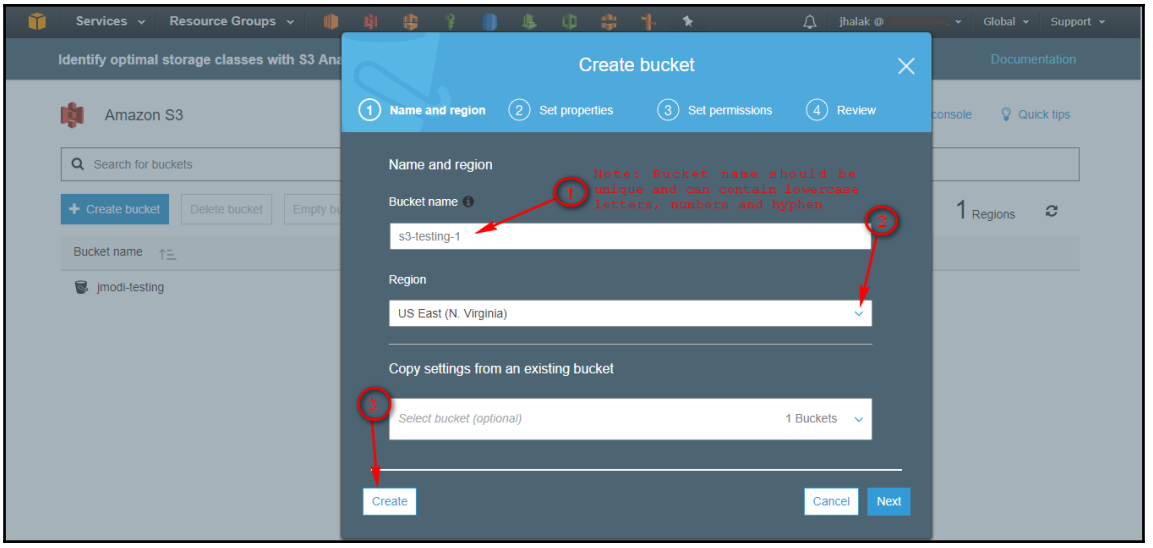

Default Cache Behavior Settings
Path Pattern
Default (*)
Viewer Protocol Policy
HTTP and HTTPS
Redirect HTTP to HTTPS
HTTPS Only
Allowed HTTP Methods
GET, HEAD
GET, HEAD, OPTIONS
GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE
Cached HTTP Methods
GET, HEAD (Cached by default)
Forward Headers
None (Improves Caching)
Object Caching
Use Origin Cache Headers
Customize
Learn More
Minimum TTL
0
Maximum TTL
31536000
Default TTL
86400
Forward Cookies
None (Improves Caching)
Query String Forwarding and Caching
None (Improves Caching)
Smooth Streaming
Yes
No
Restrict Viewer Access (Use Signed URLs or Signed Cookies)
Yes
No
Supported HTTP Versions
HTTP/2, HTTP/1.1, HTTP/1.0
HTTP/1.1, HTTP/1.0
Default Root Object
Logging
On
Off
Bucket for Logs
jmodi-testing.s3.amazonaws.com
Log Prefix
cloudfront
Cookie Logging
On
Off
Enable IPv6
Learn more
Comment
Distribution State
Enabled
Disabled
Cancel
Back
Create Distribution

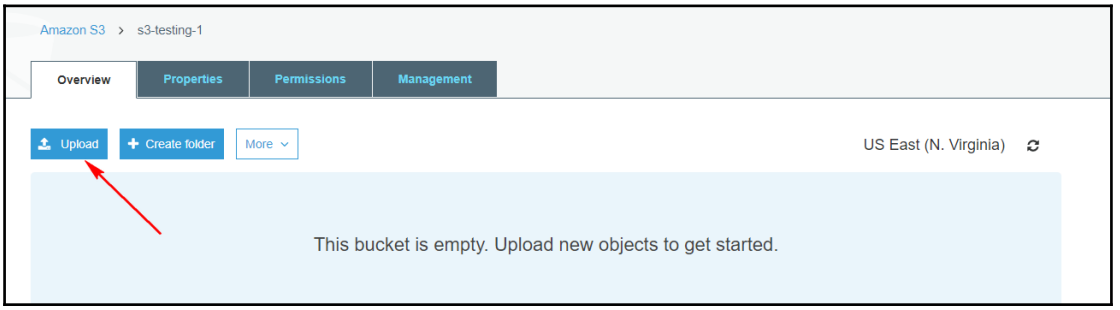
CloudFront Distributions
Create Distribution
Distribution Settings
Delete
Enable
Disable
Viewing :
Any Delivery Method
Any State
Viewing 1 to 1 of 1 Items
Delivery Method
ID
Domain Name
Comment
Origin
CNAMEs
Status
State
Last Modified
Web
aws-web-1
Deployed
Enabled

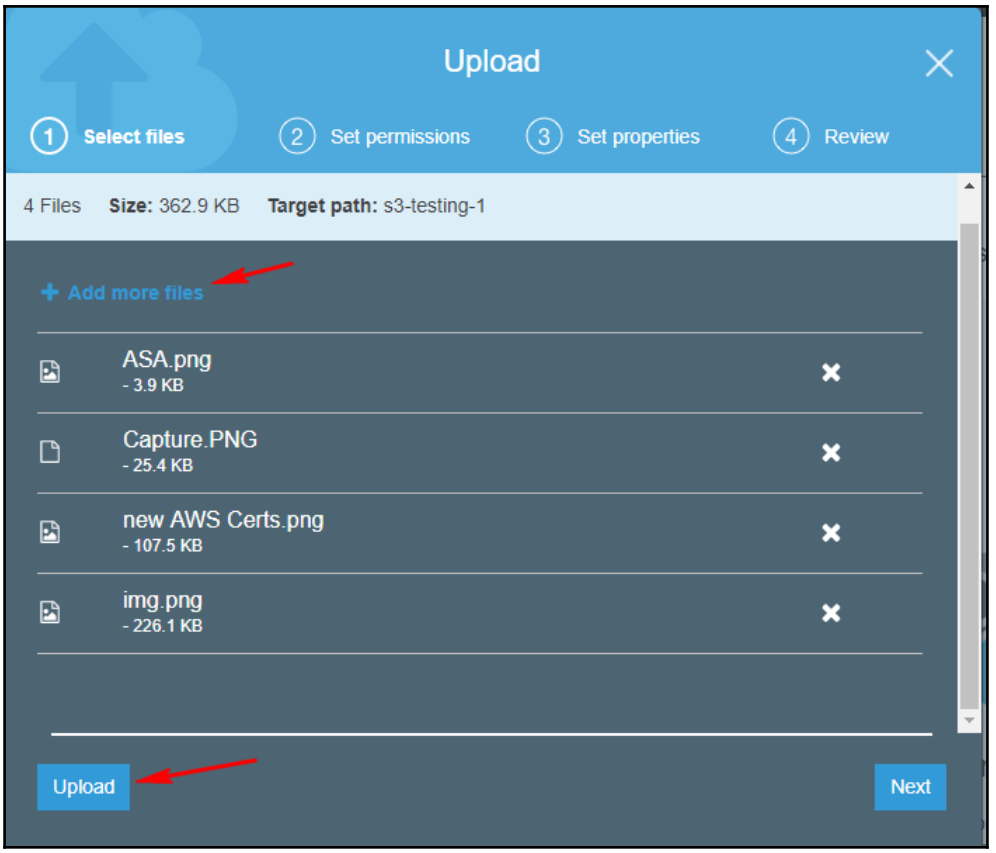

CloudFront Distributions > E
General
Origins
Behaviors
Error Pages
Restrictions
Invalidations
Tags
Edit
Distribution ID
ARN
Log Prefix
Delivery Method
Cookie Logging
Distribution Status
Comment
Price Class
AWS WAF Web ACL
State
Alternate Domain Names (CNAMEs)
SSL Certificate
Domain Name
Custom SSL Client Support
Supported HTTP Versions
IPv6
arn:aws:cloudfront::
:distribution/E
Web
Off
Deployed
-
Use All Edge Locations (Best Performance)
Enabled
Default CloudFront Certificate (*.cloudfront.net)
bg.cloudfront.net
HTTP/2, HTTP/1.1, HTTP/1.0
Disabled

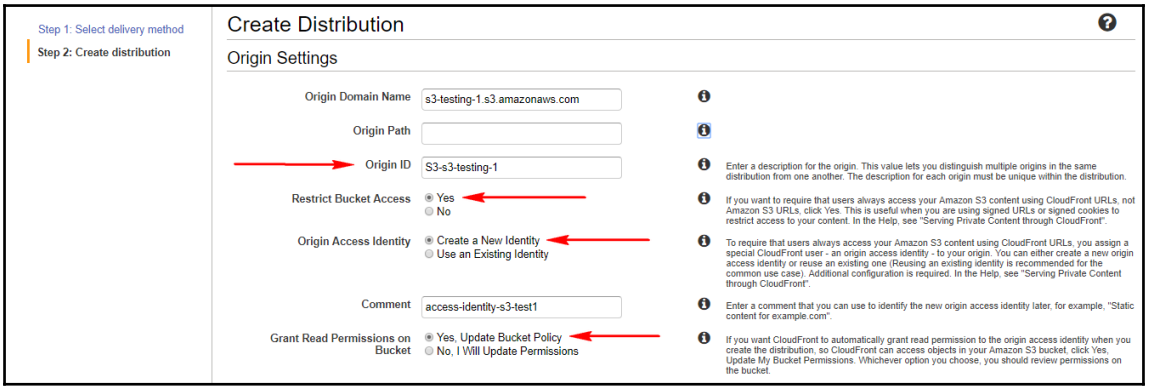

CloudFront Distributions > E3FQPCA3VNLHR5
General
Origins
Behaviors
Error Pages
Restrictions
Invalidations
Tags
CloudFront compares a request for an object with the path patterns in your cache behaviors based on the order of the cache behaviors in your distribution. Arrange cache behaviors in the order in which you want CloudFront to evaluate them.
Create Behavior
Edit
Delete
Change Precedence:
Move Up
Move Down
Save
Viewing 1 to 1 of 1 Items
Precedence
Path Pattern
Origin
Viewer Protocol Policy
Forwarded Query Strings
Trusted Signers
0
Default (*)
HTTP and HTTPS
No

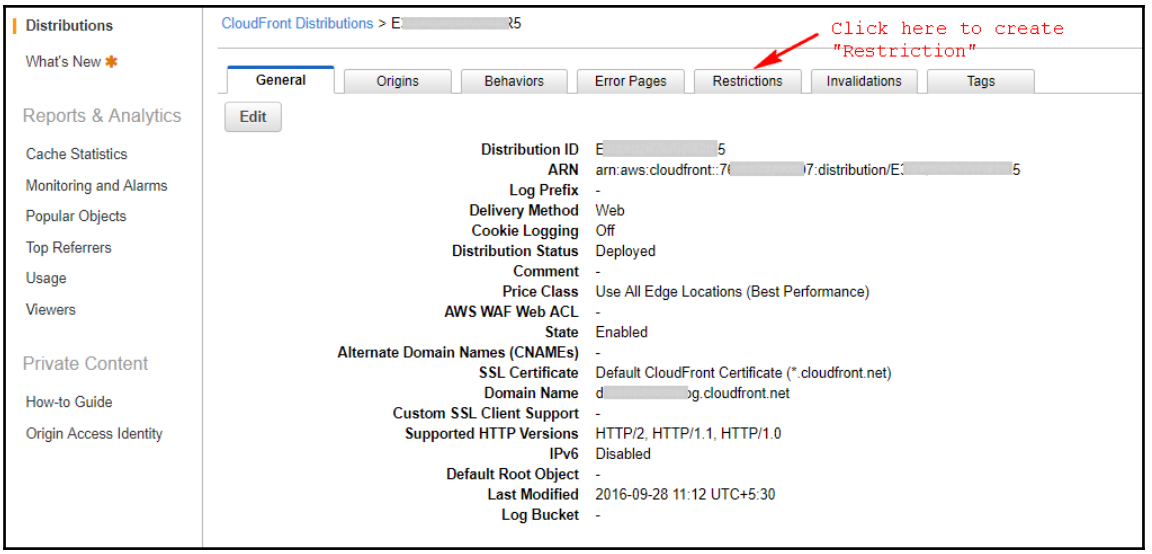

Amazon S3
Search for buckets
Create bucket
Delete bucket
Empty bucket

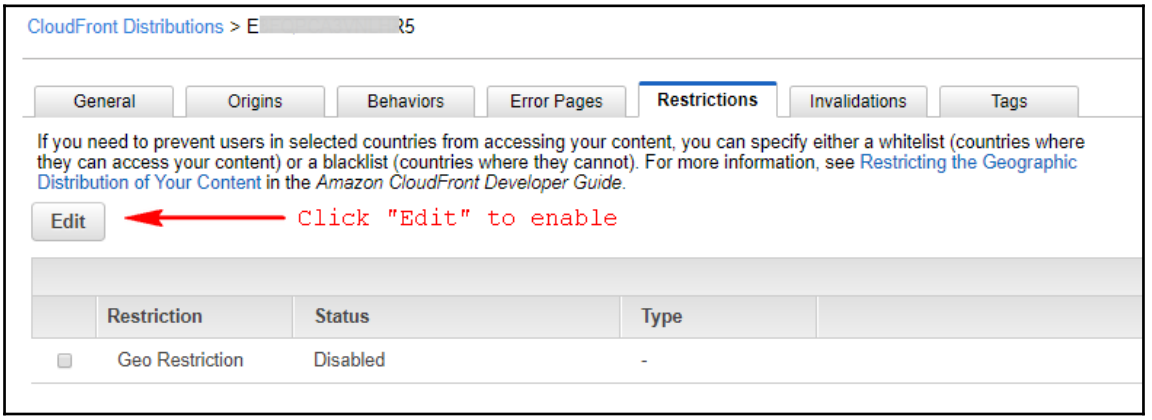

Services
Resource Groups
jhalak
Global
Support
Identify optimal storage classes with S3 Ana
Documentation
Amazon S3
Search for buckets
Create bucket
Delete bucket
Bucket name
jmodi-testing
Quick tips
1 Regions
Create bucket
Name and region
Set properties
Set permissions
Review
Name and region
Bucket name
Note: Bucket name should be unique and can contain lowercase letters, numbers and hyphen
s3-testing-1
Region
US East (N. Virginia)
Copy settings from an existing bucket
Select bucket (optional)
1 Buckets
Create
Cancel
Next

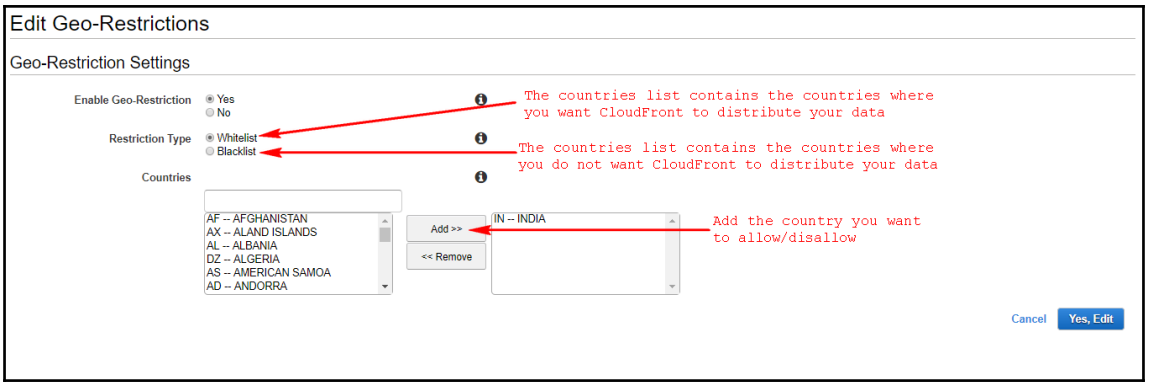

Amazon S3
s3-testing-1
Overview
Properties
Permissions
Management
Upload
Create folder
More
US East (N. Virginia)
This bucket is empty. Upload new objects to get started.

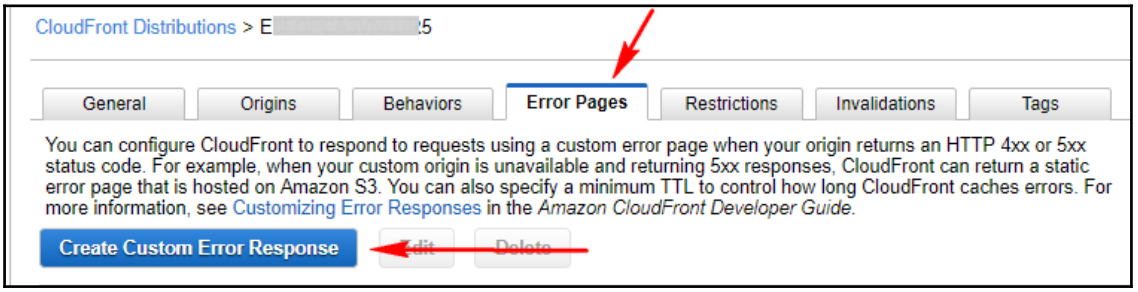

Upload
1 Select files
2 Set permissions
3 Set properties
4 Review
4 Files Size: 362.9 KB Target path: s3-testing-1
+ Add more files
ASA.png
- 3.9 KB
Capture.PNG
- 25.4 KB
new AWS Certs.png
- 107.5 KB
img.png
- 226.1 KB
Upload
Next

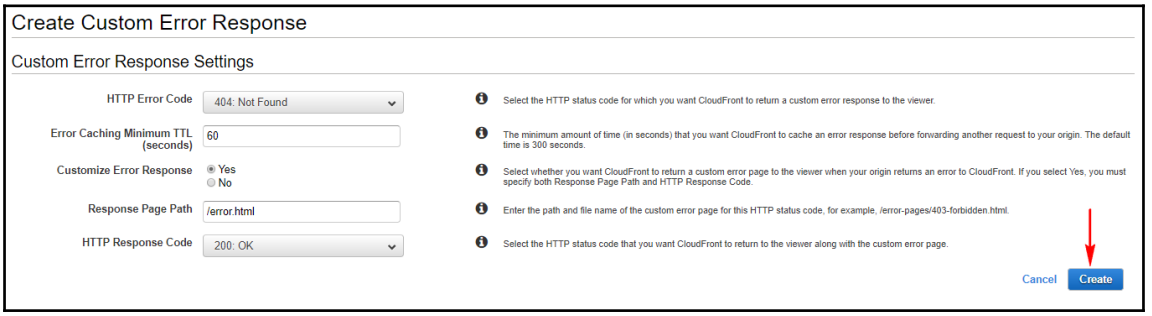

Step 1: Select delivery method
Step 2: Create distribution
Create Distribution
Origin Settings
Origin Domain Name
s3-testing-1.s3.amazonaws.com
Origin Path
Origin ID
S3-s3-testing-1
Enter a description for the origin. This value lets you distinguish multiple origins in the same distribution from one another. The description for each origin must be unique within the distribution.
Restrict Bucket Access
Yes
No
If you want to require that users always access your Amazon S3 content using CloudFront URLs, not Amazon S3 URLs, click Yes. This is useful when you are using signed URLs or signed cookies to restrict access to your content. In the Help, see "Serving Private Content through CloudFront".
Origin Access Identity
Create a New Identity
Use an Existing Identity
To require that users always access your Amazon S3 content using CloudFront URLs, you assign a special CloudFront user - an origin access identity - to your origin. You can either create a new origin access identity or reuse an existing one (Reusing an existing identity is recommended for the common use case). Additional configuration is required. In the Help, see "Serving Private Content through CloudFront".
Comment
access-identity-s3-test1
Enter a comment that you can use to identify the new origin access identity later, for example, "Static content for example.com".
Grant Read Permissions on Bucket
Yes, Update Bucket Policy
No, I Will Update Permissions
If you want CloudFront to automatically grant read permission to the origin access identity when you create the distribution, so CloudFront can access objects in your Amazon S3 bucket, click Yes, Update My Bucket Permissions. Whichever option you choose, you should review permissions on the bucket.

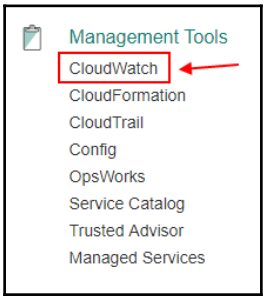

Distributions
What's New
Reports & Analytics
Cache Statistics
Monitoring and Alarms
Popular Objects
Top Referrers
Usage
Viewers
Private Content
How-to Guide
Origin Access Identity
CloudFront Distributions > E
Click here to create "Restriction"
General
Origins
Behaviors
Error Pages
Restrictions
Invalidations
Tags
Edit
Distribution ID
ARN
Log Prefix
Delivery Method
Cookie Logging
Distribution Status
Comment
Price Class
AWS WAF Web ACL
State
Alternate Domain Names (CNAMEs)
SSL Certificate
Domain Name
Custom SSL Client Support
Supported HTTP Versions
IPv6
Default Root Object
Last Modified
Log Bucket
Web
Off
Deployed
Use All Edge Locations (Best Performance)
Enabled
Default CloudFront Certificate (*.cloudfront.net)
2016-09-28 11:12 UTC+5:30

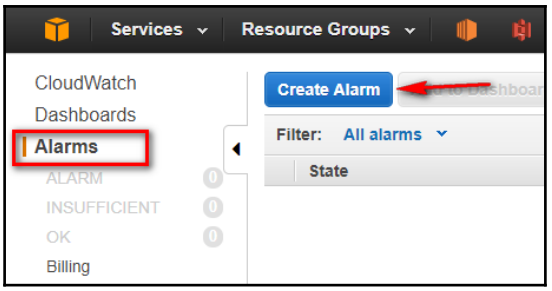

CloudFront Distributions > E
General
Origins
Behaviors
Error Pages
Restrictions
Invalidations
Tags
If you need to prevent users in selected countries from accessing your content, you can specify either a whitelist (countries where they can access your content) or a blacklist (countries where they cannot). For more information, see Restricting the Geographic Distribution of Your Content in the Amazon CloudFront Developer Guide.
Edit
Click "Edit" to enable
Restriction
Status
Type
Geo Restriction
Disabled
-

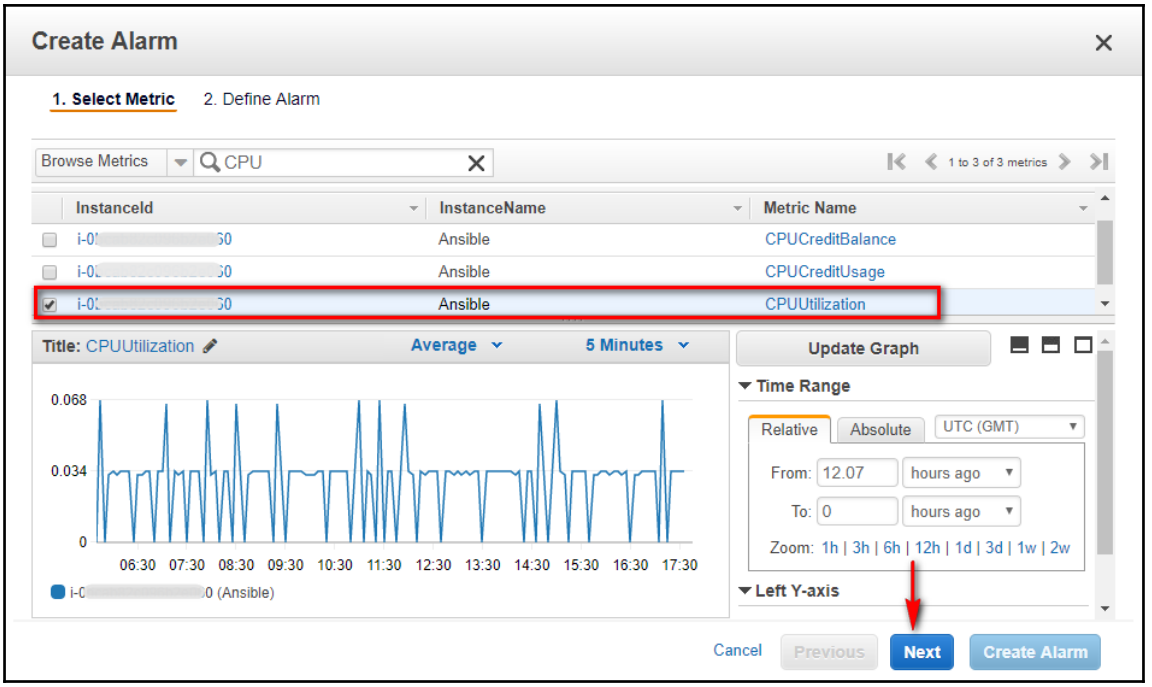

Edit Geo-Restrictions
Geo-Restriction Settings
Enable Geo-Restriction
Yes
No
Restriction Type
Whitelist
Blacklist
Countries
AF -- AFGHANISTAN
AX -- ALAND ISLANDS
AL -- ALBANIA
DZ -- ALGERIA
AS -- AMERICAN SAMOA
AD -- ANDORRA
Add >>
<< Remove
IN -- INDIA
The countries list contains the countries where you want CloudFront to distribute your data
The countries list contains the countries where you do not want CloudFront to distribute your data
Add the country you want to allow/disallow
Cancel
Yes, Edit

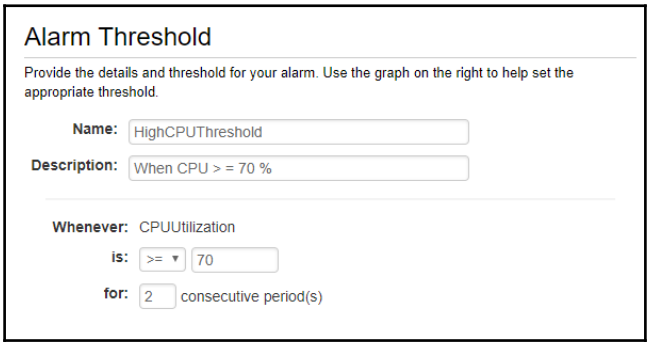

CloudFront Distributions > E
General
Origins
Behaviors
Error Pages
Restrictions
Invalidations
Tags
You can configure CloudFront to respond to requests using a custom error page when your origin returns an HTTP 4xx or 5xx status code. For example, when your custom origin is unavailable and returning 5xx responses, CloudFront can return a static error page that is hosted on Amazon S3. You can also specify a minimum TTL to control how long CloudFront caches errors. For more information, see Customizing Error Responses in the Amazon CloudFront Developer Guide.
Create Custom Error Response
Edit
Delete

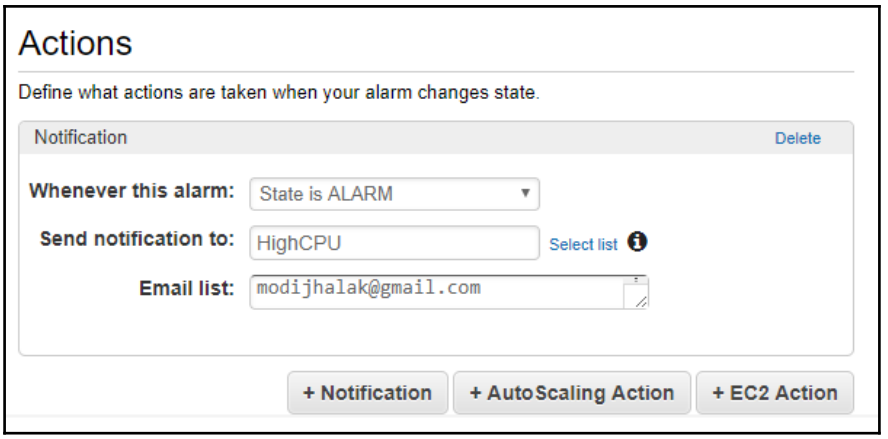

Create Custom Error Response
Custom Error Response Settings
HTTP Error Code
404: Not Found
Select the HTTP status code for which you want CloudFront to return a custom error response to the viewer.
Error Caching Minimum TTL (seconds)
60
The minimum amount of time (in seconds) that you want CloudFront to cache an error response before forwarding another request to your origin. The default time is 300 seconds.
Customize Error Response
Yes
No
Select whether you want CloudFront to return a custom error page to the viewer when your origin returns an error to CloudFront. If you select Yes, you must specify both Response Page Path and HTTP Response Code.
Response Page Path
/error.html
Enter the path and file name of the custom error page for this HTTP status code, for example, /error-pages/403-forbidden.html.
HTTP Response Code
200: OK
Select the HTTP status code that you want CloudFront to return to the viewer along with the custom error page.
Cancel
Create

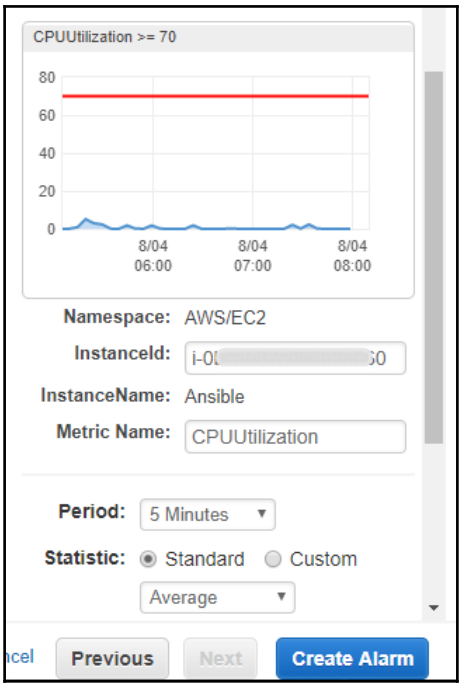

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services

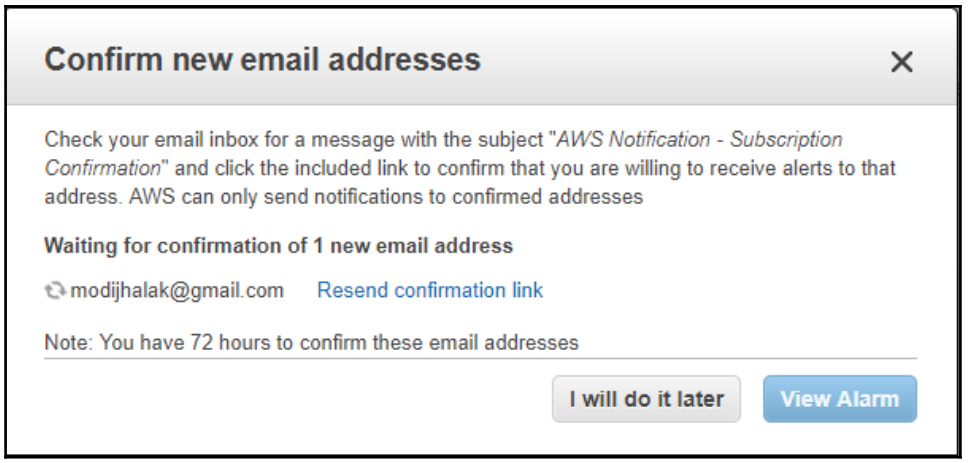

Services
Resource Groups
CloudWatch
Dashboards
Alarms
ALARM
INSUFFICIENT
OK
Billing
Create Alarm
Filter:
All alarms
State

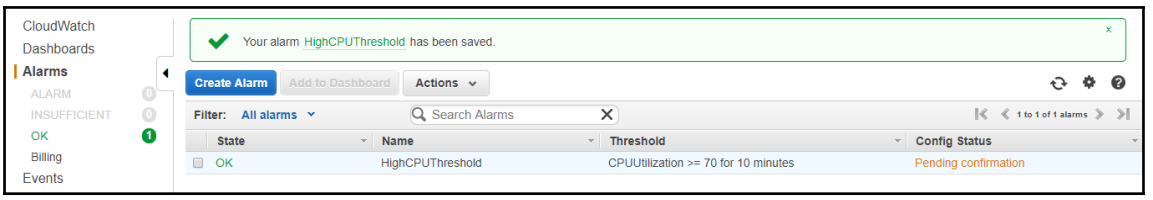

Create Alarm
1. Select Metric
2. Define Alarm
Browse Metrics
CPU
1 to 3 of 3 metrics
InstanceId
InstanceName
Metric Name
Ansible
CPUCreditBalance
CPUCreditUsage
CPUUtilization
Title: CPUUtilization
Average
5 Minutes
Update Graph
0.068
0.034
0
06:30 07:30 08:30 09:30 10:30 11:30 12:30 13:30 14:30 15:30 16:30 17:30
(Ansible)
Time Range
Relative
Absolute
UTC (GMT)
From: 12.07 hours ago
To: 0 hours ago
Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w
Left Y-axis
Cancel
Previous
Next
Create Alarm

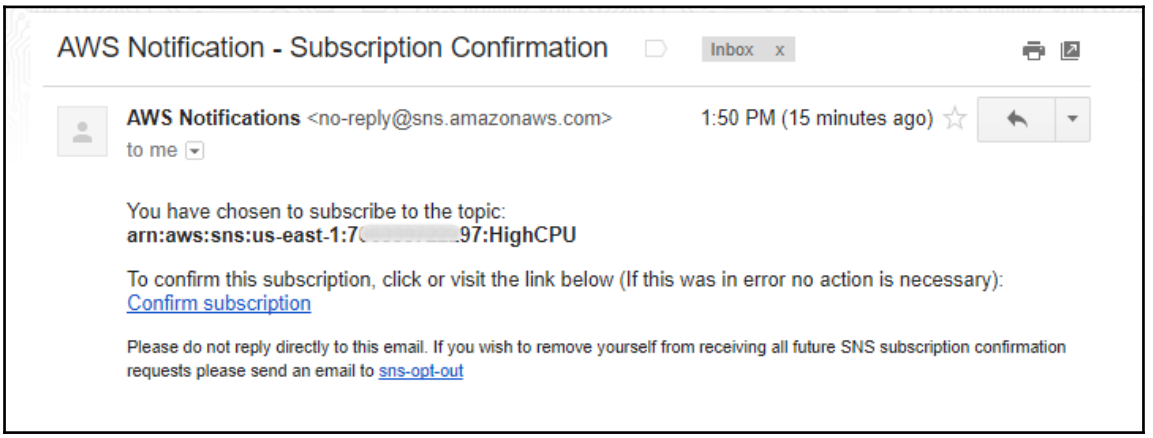

Alarm Threshold
Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.
Name: HighCPUThreshold
Description: When CPU > = 70 %
Whenever: CPUUtilization
is: >= 70
for: 2 consecutive period(s)

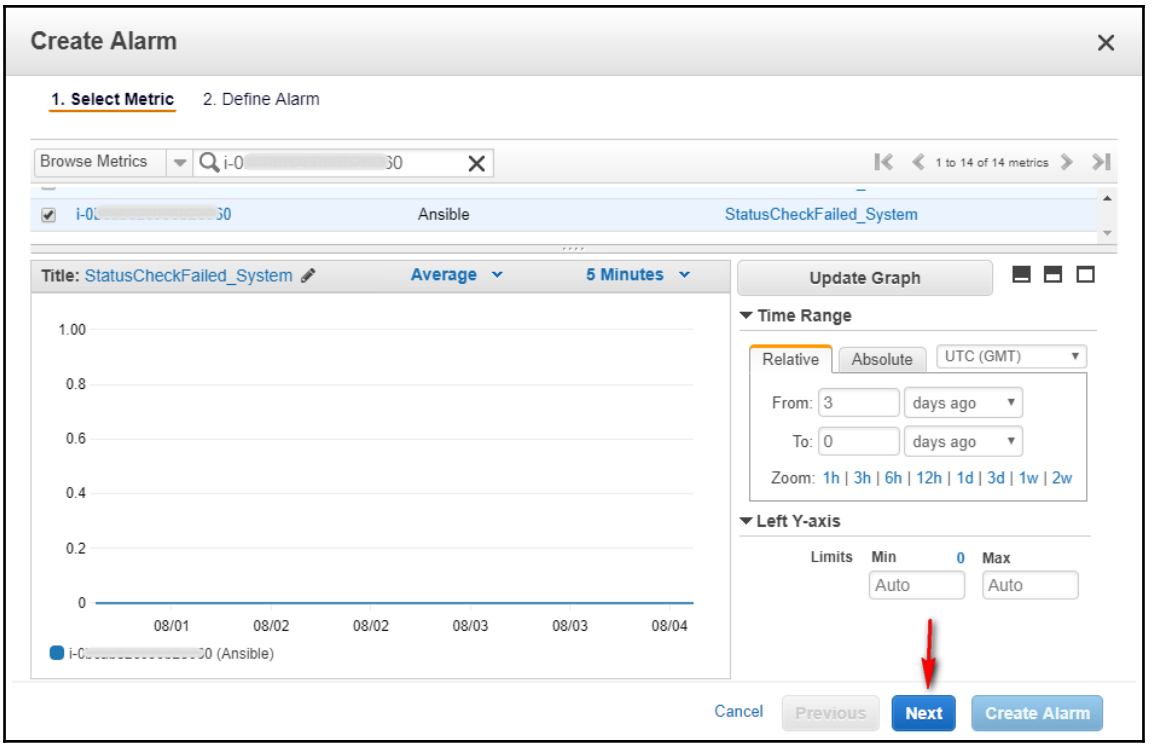

Actions
Define what actions are taken when your alarm changes state.
Notification
Delete
Whenever this alarm:
State is ALARM
Send notification to:
HighCPU
Select list
Email list:
modijhalak@gmail.com
+ Notification
+ AutoScaling Action
+ EC2 Action

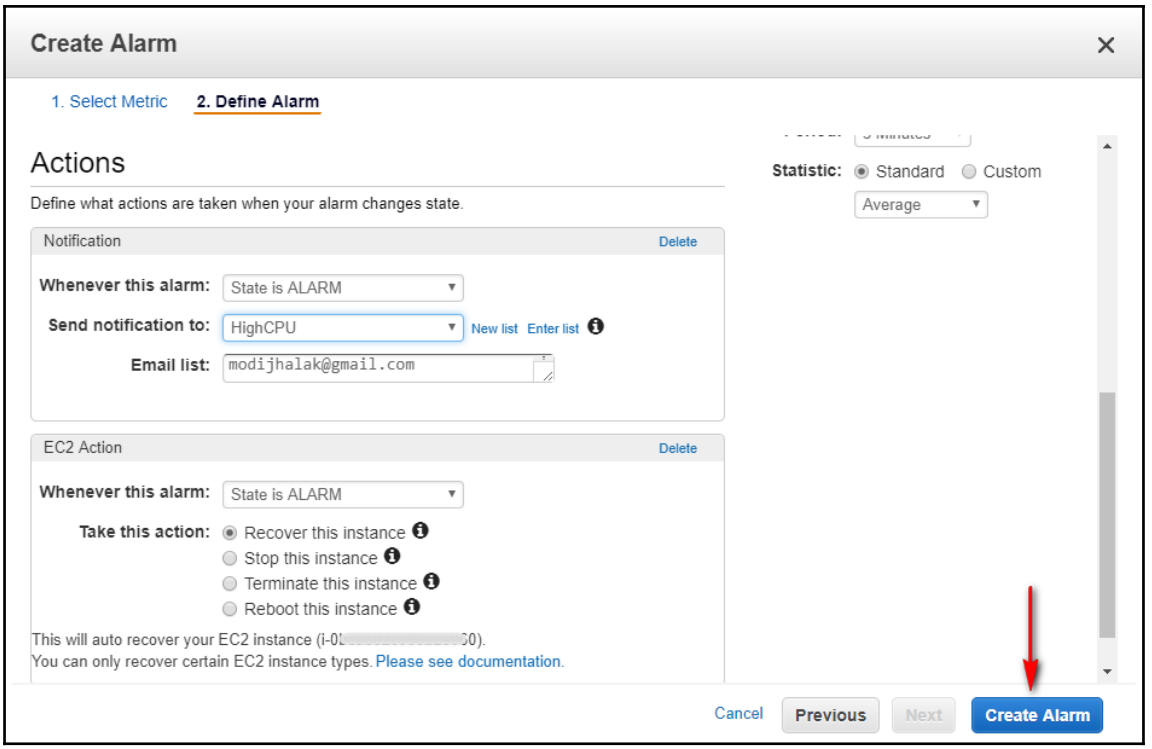

CPUUtilization >= 70
80
60
40
20
0
8/04 06:00
8/04 07:00
8/04 08:00
Namespace: AWS/EC2
InstanceId: i-0
InstanceName: Ansible
Metric Name: CPUUtilization
Period: 5 Minutes
Statistic: Standard Custom
Average
Previous
Next
Create Alarm

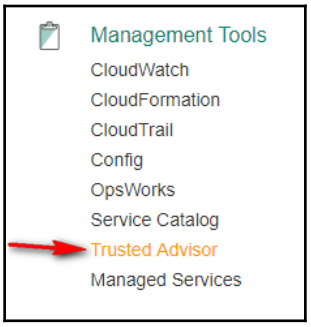

Confirm new email addresses
Check your email inbox for a message with the subject "AWS Notification - Subscription Confirmation" and click the included link to confirm that you are willing to receive alerts to that address. AWS can only send notifications to confirmed addresses
Waiting for confirmation of 1 new email address
modijhalak@gmail.com
Resend confirmation link
Note: You have 72 hours to confirm these email addresses
I will do it later
View Alarm

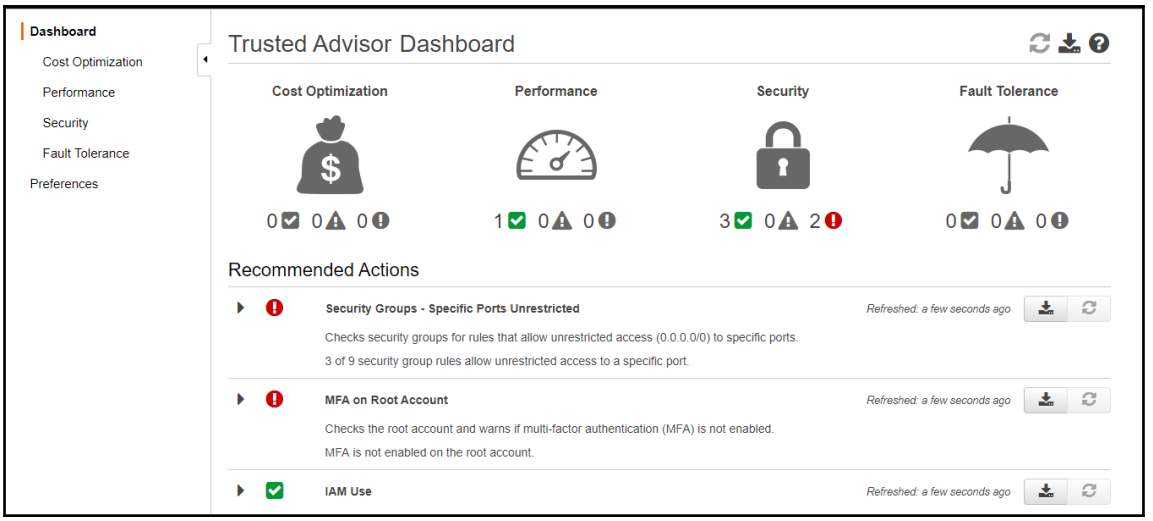

CloudWatch
Dashboards
Alarms
ALARM
INSUFFICIENT
OK
Billing
Events
Your alarm HighCPUThreshold has been saved.
Create Alarm
Add to Dashboard
Actions
Filter: All alarms
Search Alarms
1 to 1 of 1 alarms
State
Name
Threshold
Config Status
OK
HighCPUThreshold
CPUUtilization >= 70 for 10 minutes
Pending confirmation

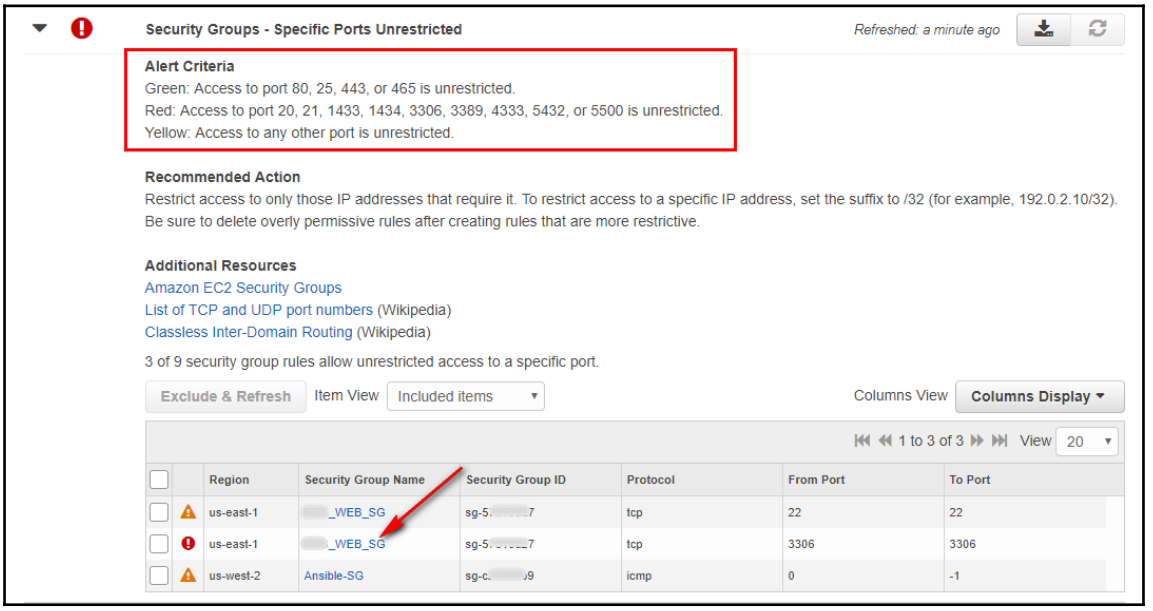

AWS Notification - Subscription Confirmation
Inbox x
AWS Notifications <no-reply@sns.amazonaws.com>
1:50 PM (15 minutes ago)
to me
You have chosen to subscribe to the topic:
arn:aws:sns:us-east-1:7
97:HighCPU
To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
Confirm subscription
Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to sns-opt-out

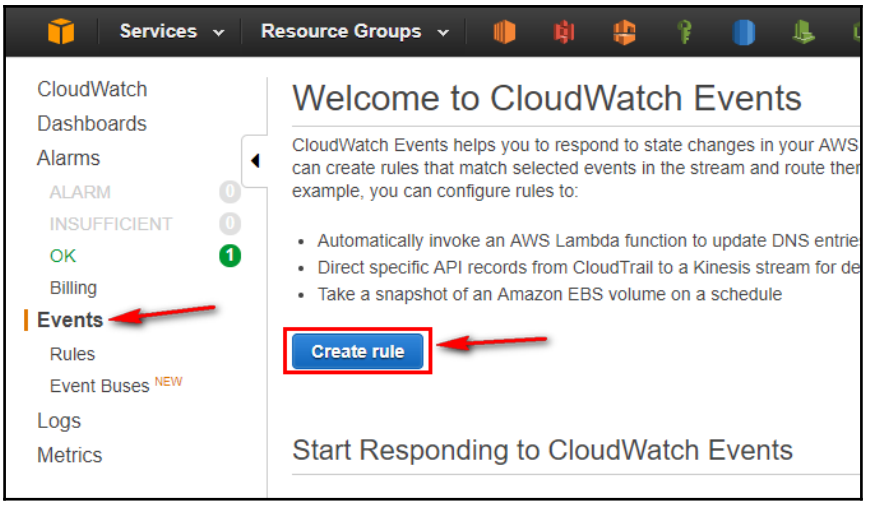

Create Alarm
1. Select Metric
2. Define Alarm
Browse Metrics
1 to 14 of 14 metrics
Ansible
StatusCheckFailed_System
Title: StatusCheckFailed_System
Average
5 Minutes
Update Graph
1.00
0.8
0.6
0.4
0.2
0
08/01
08/02
08/02
08/03
08/03
08/04
(Ansible)
Time Range
Relative
Absolute
UTC (GMT)
From: 3
days ago
To: 0
days ago
Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w
Left Y-axis
Limits
Min
0
Max
Auto
Auto
Cancel
Previous
Next
Create Alarm

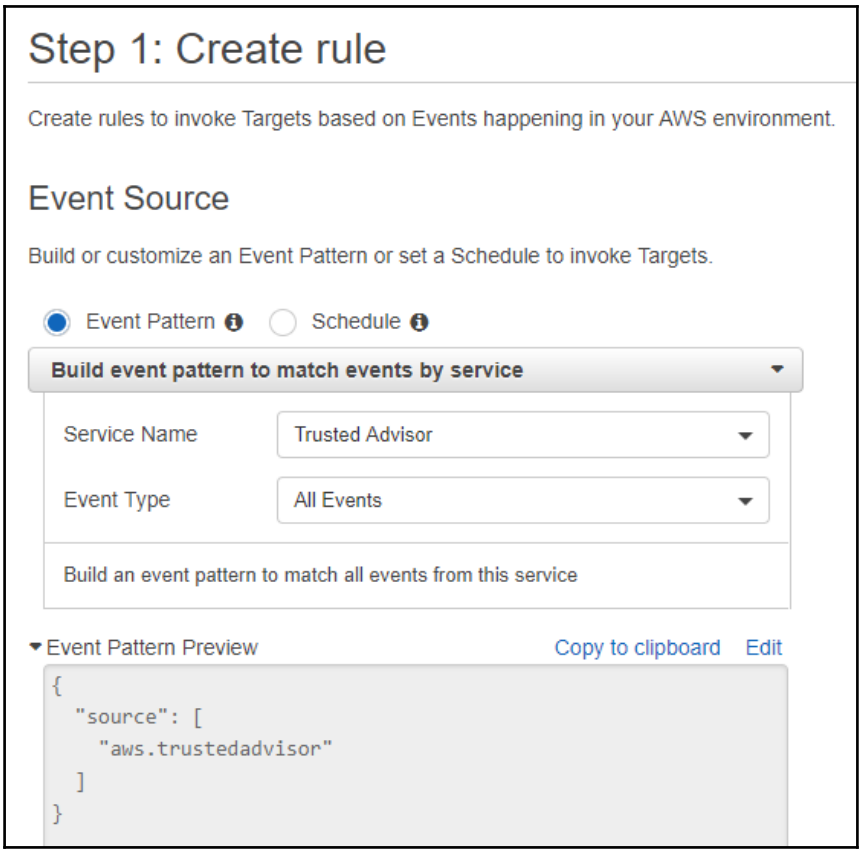

Create Alarm
1. Select Metric
2. Define Alarm
Actions
Define what actions are taken when your alarm changes state.
Notification
Delete
Whenever this alarm:
State is ALARM
Send notification to:
HighCPU
New list
Enter list
Email list:
modijhalak@gmail.com
EC2 Action
Delete
Whenever this alarm:
State is ALARM
Take this action:
Recover this instance
Stop this instance
Terminate this instance
Reboot this instance
This will auto recover your EC2 instance (i-0
0).
You can only recover certain EC2 instance types. Please see documentation.
Statistic:
Standard
Custom
Average
Cancel
Previous
Next
Create Alarm

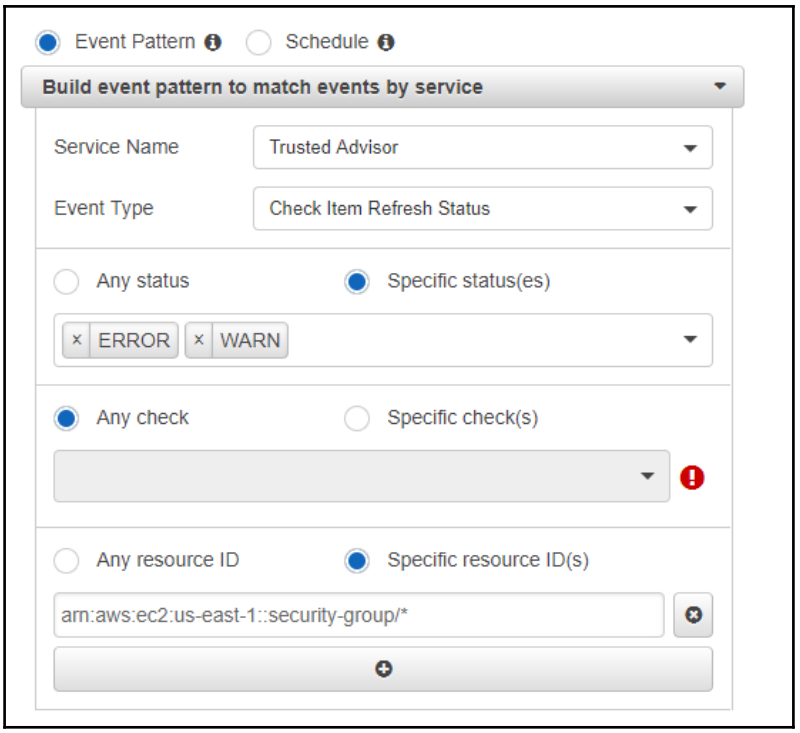

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services

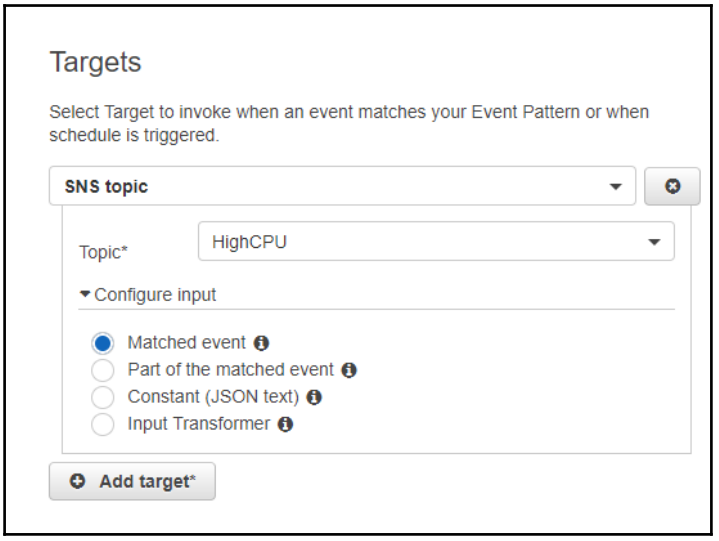

Dashboard
Cost Optimization
Performance
Security
Fault Tolerance
Preferences
Trusted Advisor Dashboard
Cost Optimization
Performance
Security
Fault Tolerance
0 0 0
1 0 0
3 0 2
0 0 0
Recommended Actions
Security Groups - Specific Ports Unrestricted
Refreshed: a few seconds ago
Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.
3 of 9 security group rules allow unrestricted access to a specific port.
MFA on Root Account
Refreshed: a few seconds ago
Checks the root account and warns if multi-factor authentication (MFA) is not enabled.
MFA is not enabled on the root account.
IAM Use
Refreshed: a few seconds ago


Security Groups - Specific Ports Unrestricted
Refreshed: a minute ago
Alert Criteria
Green: Access to port 80, 25, 443, or 465 is unrestricted.
Red: Access to port 20, 21, 1433, 1434, 3306, 3389, 4333, 5432, or 5500 is unrestricted.
Yellow: Access to any other port is unrestricted.
Recommended Action
Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.
Additional Resources
Amazon EC2 Security Groups
List of TCP and UDP port numbers (Wikipedia)
Classless Inter-Domain Routing (Wikipedia)
3 of 9 security group rules allow unrestricted access to a specific port.
Exclude & Refresh
Item View
Included items
Columns View
Columns Display
1 to 3 of 3
View
20
Region
Security Group Name
Security Group ID
Protocol
From Port
To Port
us-east-1
_WEB_SG
tcp
22
22
us-east-1
_WEB_SG
tcp
3306
3306
us-west-2
Ansible-SG
icmp
0
-1

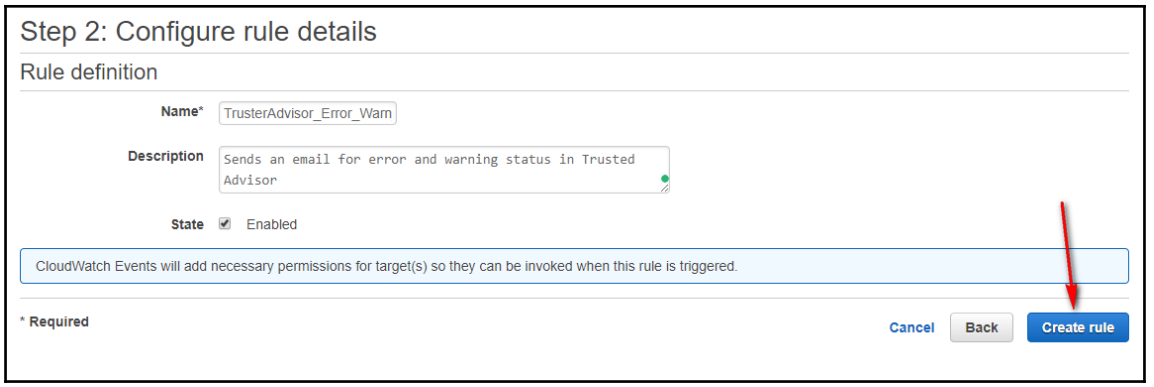

Services
Resource Groups
CloudWatch
Dashboards
Alarms
ALARM 0
INSUFFICIENT 0
OK 1
Billing
Events
Rules
Event Buses NEW
Logs
Metrics
Welcome to CloudWatch Events
CloudWatch Events helps you to respond to state changes in your AWS
can create rules that match selected events in the stream and route ther
example, you can configure rules to:
Automatically invoke an AWS Lambda function to update DNS entrie
Direct specific API records from CloudTrail to a Kinesis stream for de
Take a snapshot of an Amazon EBS volume on a schedule
Create rule
Start Responding to CloudWatch Events

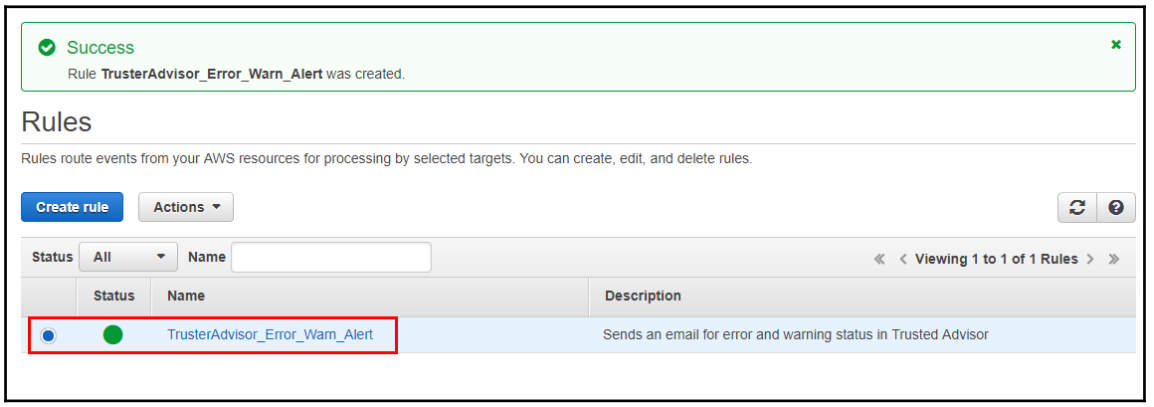

Step 1: Create rule
Create rules to invoke Targets based on Events happening in your AWS environment.
Event Source
Build or customize an Event Pattern or set a Schedule to invoke Targets.
Event Pattern
Schedule
Build event pattern to match events by service
Service Name
Trusted Advisor
Event Type
All Events
Build an event pattern to match all events from this service
Event Pattern Preview
Copy to clipboard
Edit
{
"source": [
"aws.trustedadvisor"
]
}

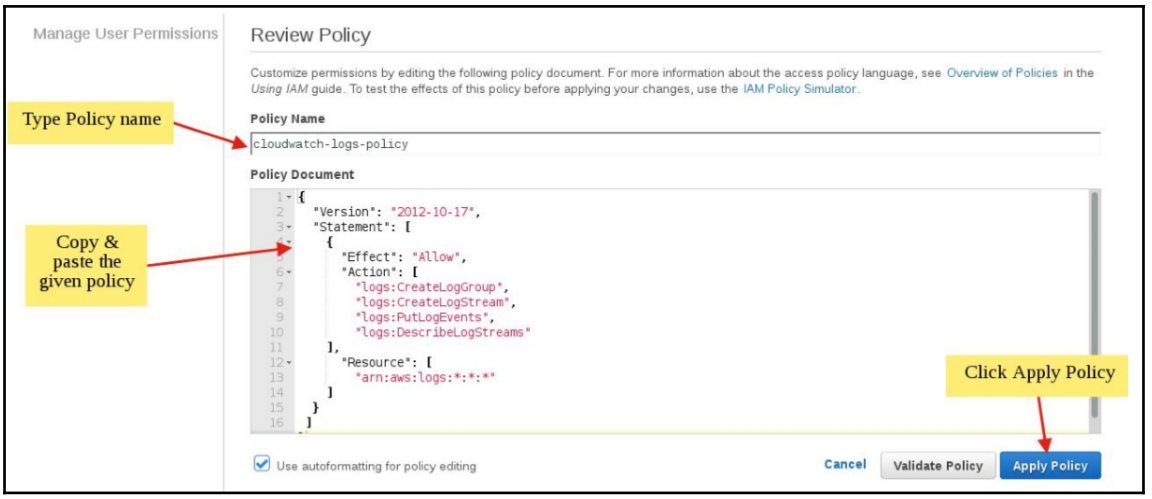

Event Pattern
Schedule
Build event pattern to match events by service
Service Name
Trusted Advisor
Event Type
Check Item Refresh Status
Any status
Specific status(es)
ERROR
WARN
Any check
Specific check(s)
Any resource ID
Specific resource ID(s)
arn:aws:ec2:us-east-1::security-group/*

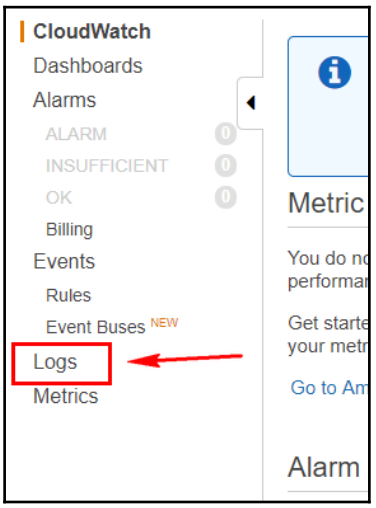

Targets
Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.
SNS topic
Topic*
HighCPU
Configure input
Matched event
Part of the matched event
Constant (JSON text)
Input Transformer
Add target*

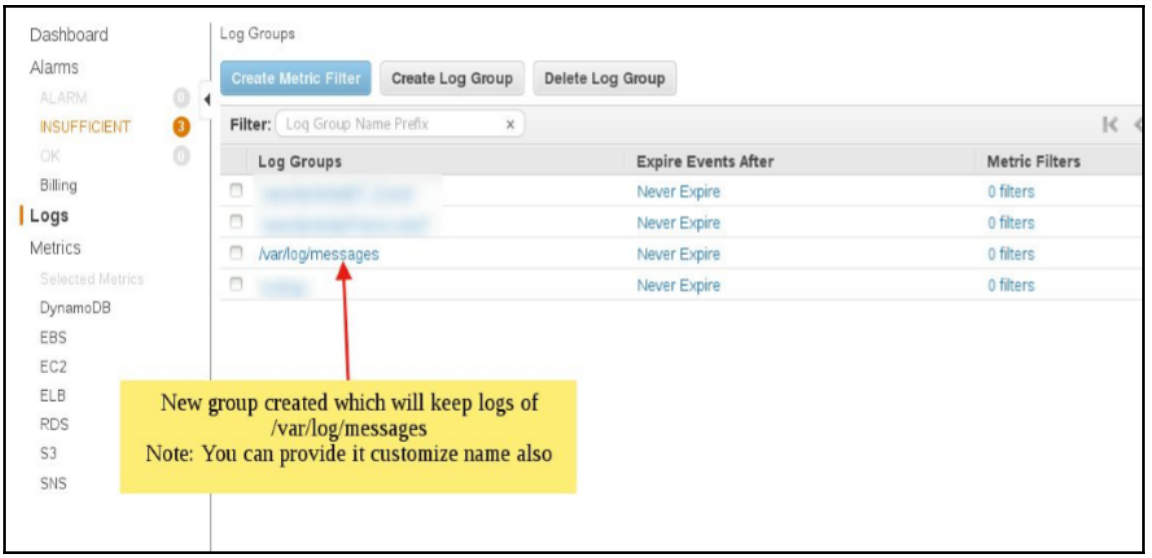
Cancel
Configure details

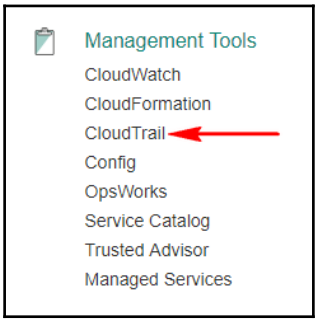

Step 2: Configure rule details
Rule definition
Name*
TrusterAdvisor_Error_Warn
Description
Sends an email for error and warning status in Trusted Advisor
State
Enabled
CloudWatch Events will add necessary permissions for target(s) so they can be invoked when this rule is triggered.
* Required
Cancel
Back
Create rule


Success
Rule TrusterAdvisor_Error_Warn_Alert was created.
Rules
Rules route events from your AWS resources for processing by selected targets. You can create, edit, and delete rules.
Create rule
Actions
Status
All
Name
Viewing 1 to 1 of 1 Rules
Status
Name
Description
TrusterAdvisor_Error_Warn_Alert
Sends an email for error and warning status in Trusted Advisor

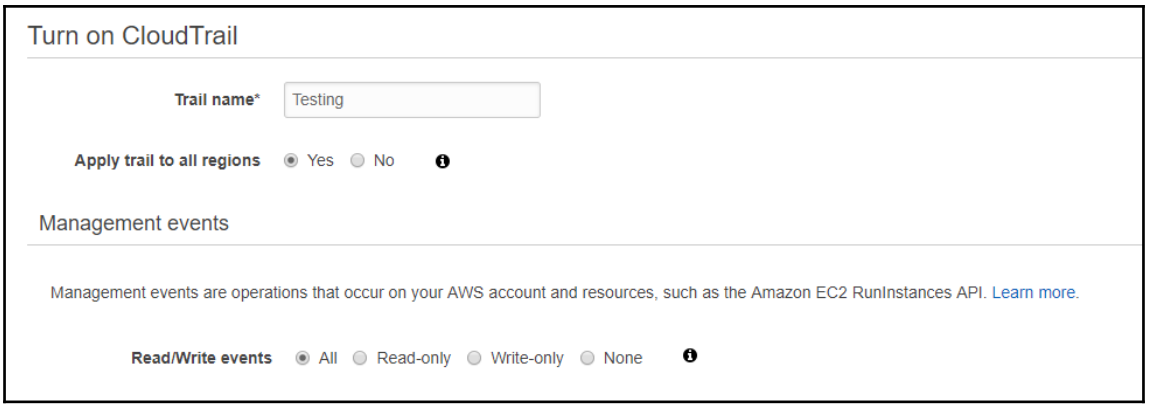

Manage User Permissions
Review Policy
Customize permissions by editing the following policy document. For more information about the access policy language, see Overview of Policies in the Using IAM guide. To test the effects of this policy before applying your changes, use the IAM Policy Simulator.
Type Policy name
Policy Name
cloudwatch-logs-policy
Policy Document
Copy & paste the given policy
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents",
"logs:DescribeLogStreams"
],
"Resource": [
"arn:aws:logs:*:*:*"
]
}
]
Click Apply Policy
Use autoformatting for policy editing
Cancel
Validate Policy
Apply Policy


CloudWatch
Dashboards
Alarms
ALARM
INSUFFICIENT
OK
Billing
Events
Rules
Event Buses NEW
Logs
Metrics
Metric
Alarm

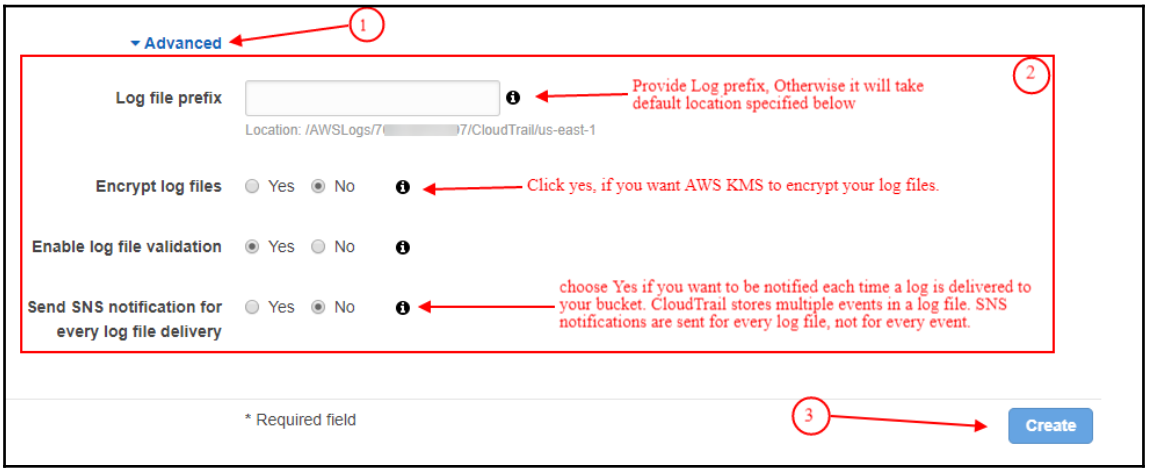

Dashboard
Alarms
ALARM
INSUFFICIENT
OK
Billing
Logs
Metrics
Selected Metrics
DynamoDB
EBS
EC2
ELB
RDS
S3
SNS
Log Groups
Create Metric Filter
Create Log Group
Delete Log Group
Filter:
Log Group Name Prefix
Log Groups
Expire Events After
Metric Filters
Never Expire
0 filters
/var/log/messages
New group created which will keep logs of /var/log/messages
Note: You can provide it customize name also

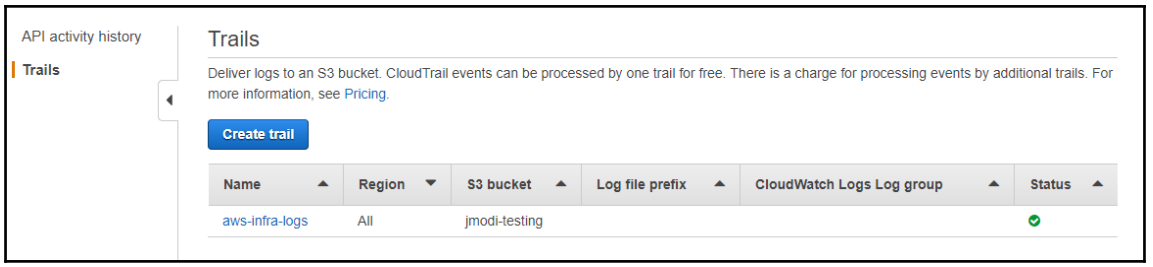

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services

AWS CloudTrail
AWS CloudTrail provides a record of your AWS API calls. You can use this data to gain visibility into user activity, troubleshoot operational and security incidents, or to help demonstrate compliance with internal policies or regulatory standards.
Get Started Now


Turn on CloudTrail
Trail name*
Testing
Apply trail to all regions
Yes
No
Management events
Management events are operations that occur on your AWS account and resources, such as the Amazon EC2 RunInstances API. Learn more.
Read/Write events
All
Read-only
Write-only
None

Create a new S3 bucket
Yes
No
S3 bucket*
jmodi-testing


1
Advanced
2
Log file prefix
Provide Log prefix, Otherwise it will take default location specified below
Location: /AWSLogs/7
7/CloudTrail/us-east-1
Encrypt log files
Yes
No
Click yes, if you want AWS KMS to encrypt your log files.
Enable log file validation
Yes
No
Send SNS notification for every log file delivery
Yes
No
choose Yes if you want to be notified each time a log is delivered to your bucket. CloudTrail stores multiple events in a log file. SNS notifications are sent for every log file, not for every event.
* Required field
3
Create



Contact Information

Please provide the email address and the associated name of the AWS account owner with which you have used to log into this form. The AWS Account ID number of the account used to log into this form will be sent along with your submission. If you would like to request testing for a different account, please log out and log back in with the account for which you want to test.

Your Name:*

Company Name*

Email Address

Additional Email Address

Additional Email Address

Additional Email Address

Third Party Contact Information

Scan Information

IP Addresses to be scanned (Destination)*

Are the instances the source of the scan or the target of the scan?*

- [ ] Source
- [ ] Target

Instance IDs*

Scanning IP addresses (Source)*

Total Bandwidth (Please provide expected Gbps)*

What region are these instances in?*

Asia Pacific (Seoul)
Asia Pacific (Singapore)
Asia Pacific (Tokyo)
Asia Pacific (Sydney)

Time Zone

GMT -11

Start Date and Time (YYYY-MM-DD HH:MM)*

End Date and Time (YYYY-MM-DD HH:MM)*

Additional Comments

Terms and Conditions

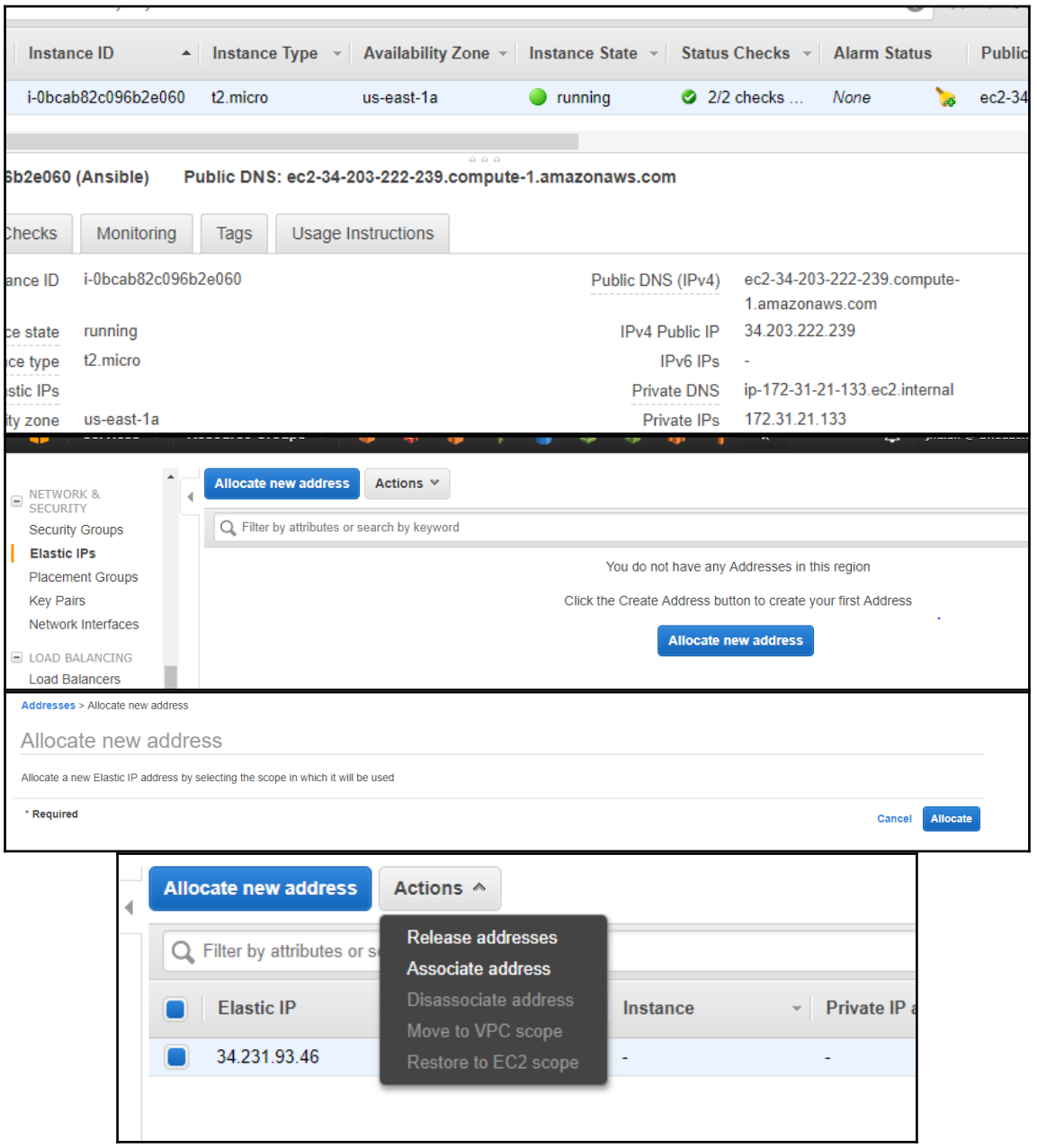
Furthermore, you are responsible for any damages to AWS or other AWS customers that are caused by your penetration testing activities.

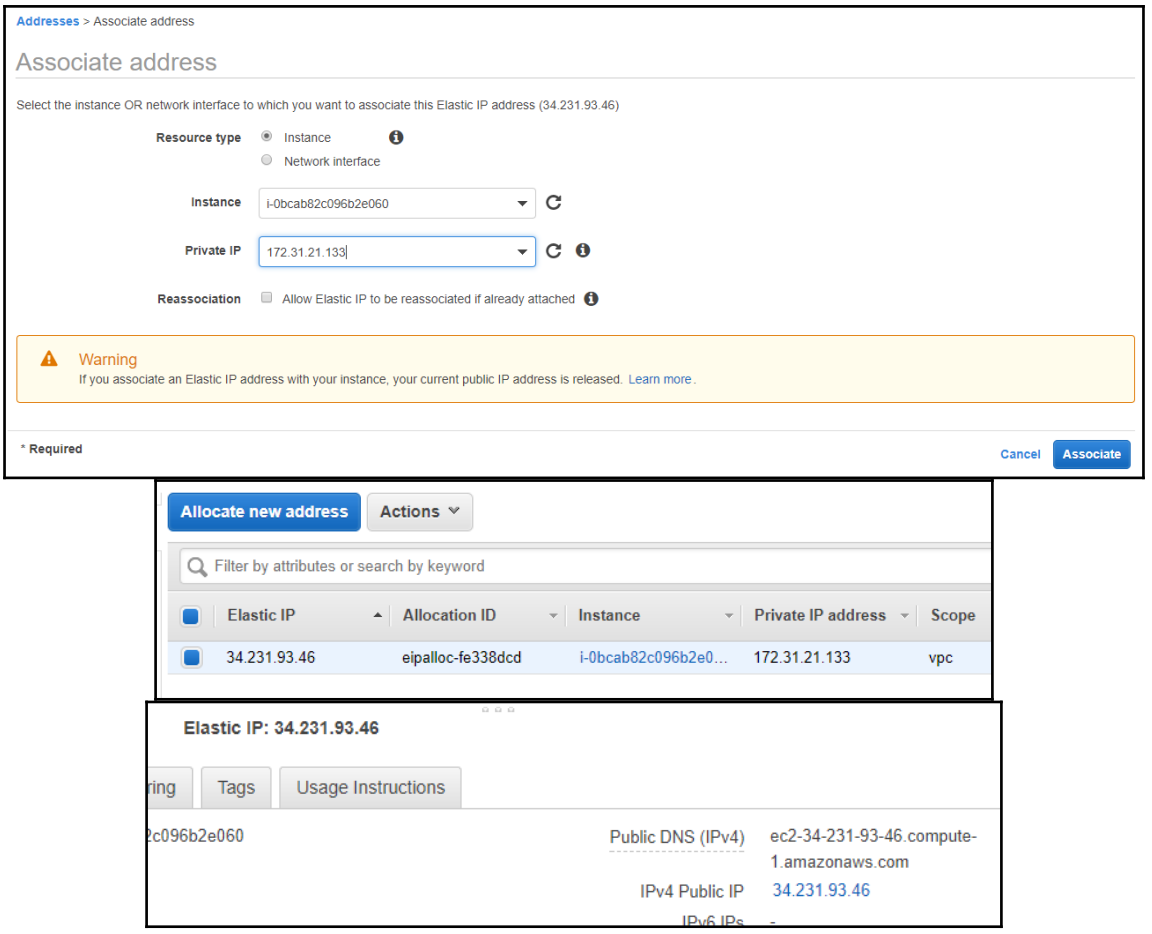
AWS Policy Regarding the Use of Security Assessment Tools and Services Agreement*

- (•) I agree
- ( ) I do not agree

Submit

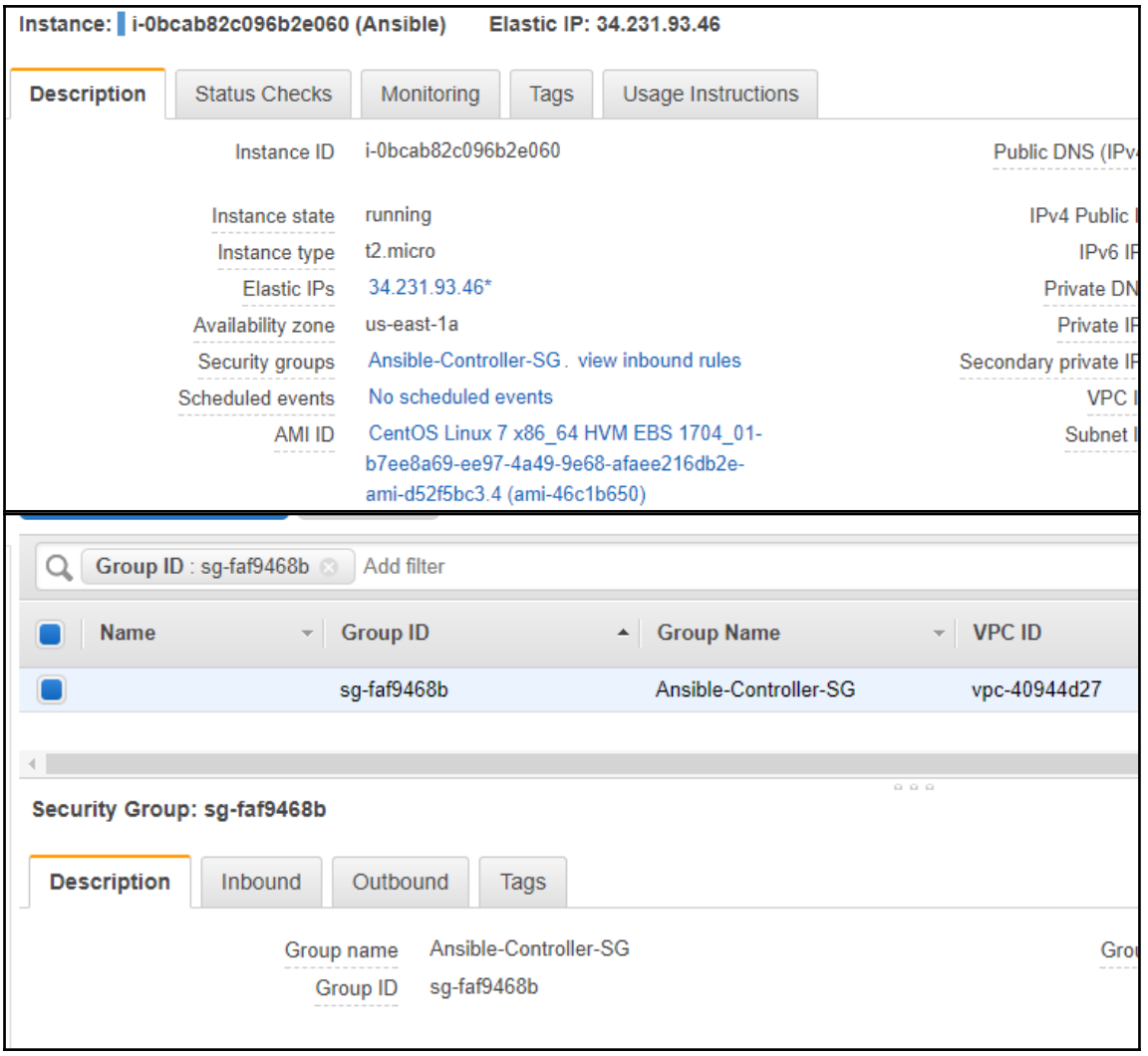
Chapter 8: Troubleshooting and VPC Limits

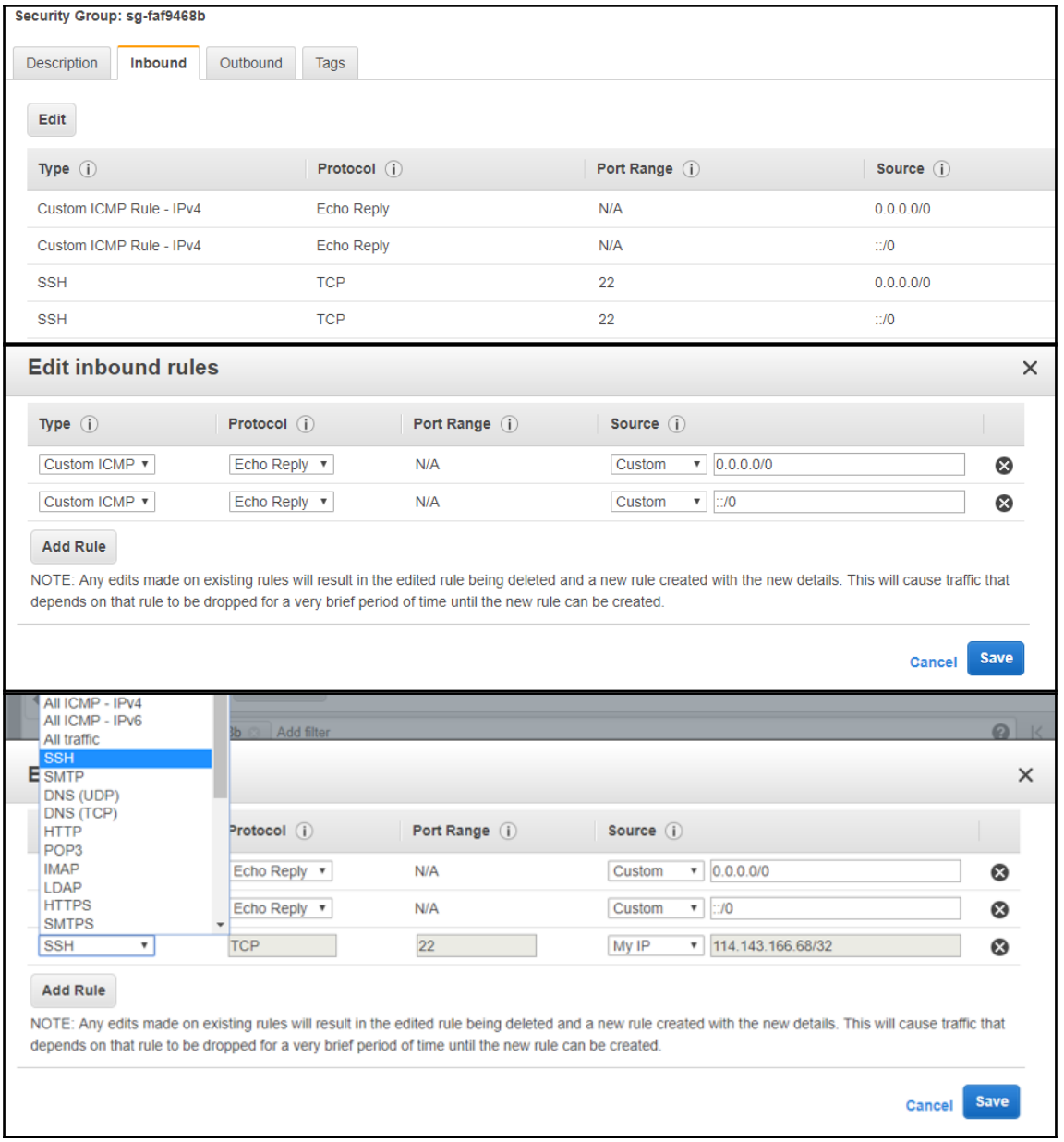


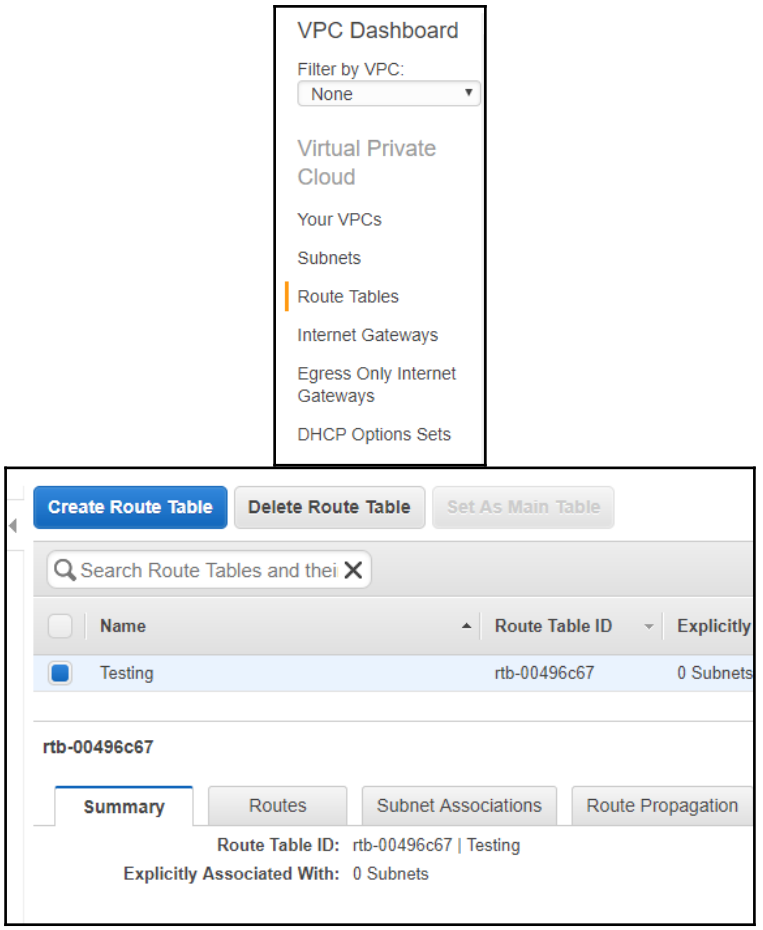

Addresses > Associate address
Associate address
Select the instance OR network interface to which you want to associate this Elastic IP address (34.231.93.46)
Resource type
Instance
Network interface
Instance
i-0bcab82c096b2e060
Private IP
172.31.21.133
Reassociation
Allow Elastic IP to be reassociated if already attached
Warning
If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.
* Required
Cancel
Associate

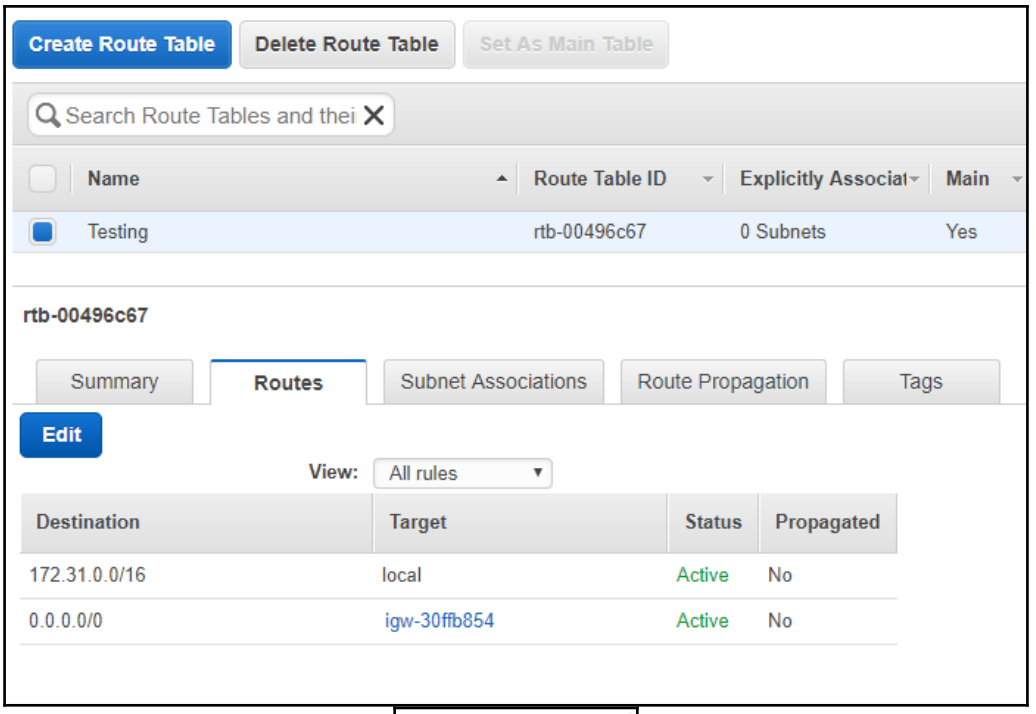
Allocate new address
Actions
Filter by attributes or search by keyword
Elastic IP
Allocation ID
Instance
Private IP address
Scope
34.231.93.46
eipalloc-fe338dcd
i-0bcab82c096b2e0...
172.31.21.133
vpc

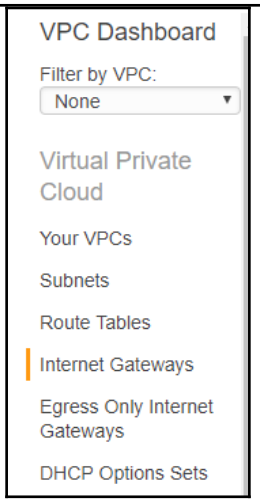
Elastic IP: 34.231.93.46
ring
Tags
Usage Instructions
2c096b2e060
Public DNS (IPv4)
ec2-34-231-93-46.compute-1.amazonaws.com
IPv4 Public IP
34.231.93.46
IPv6 IPs

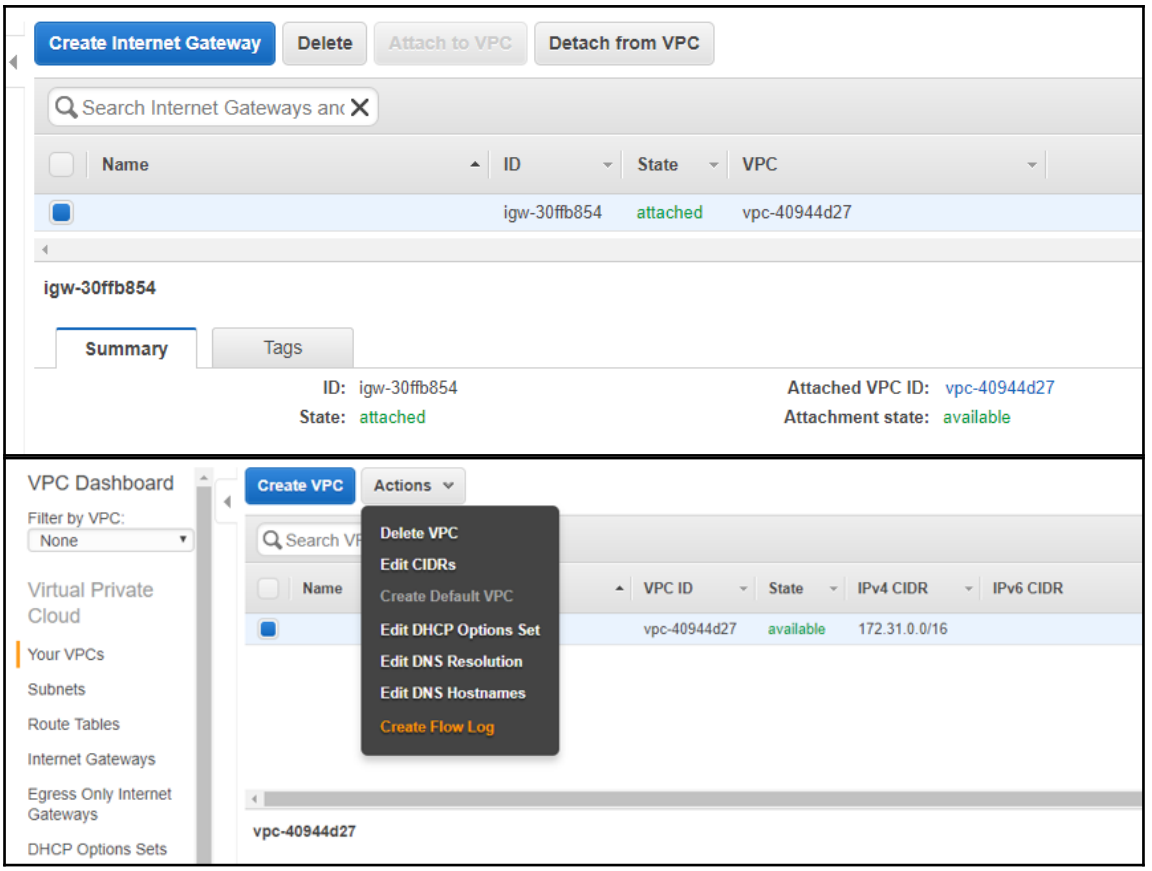

Instance: i-0bcab82c096b2e060 (Ansible) Elastic IP: 34.231.93.46
Description
Status Checks
Monitoring
Tags
Usage Instructions
Instance ID
i-0bcab82c096b2e060
Public DNS (IPv
Instance state
running
IPv4 Public
Instance type
t2.micro
IPv6 IP
Elastic IPs
34.231.93.46*
Private DN
Availability zone
us-east-1a
Private IP
Security groups
Ansible-Controller-SG. view inbound rules
Secondary private IP
Scheduled events
No scheduled events
VPC
AMI ID
CentOS Linux 7 x86_64 HVM EBS 1704_01-b7ee8a69-ee97-4a49-9e68-afaee216db2e-ami-d52f5bc3.4 (ami-46c1b650)
Subnet
Group ID : sg-faf9468b
Add filter
Name
Group ID
Group Name
VPC ID
sg-faf9468b
Ansible-Controller-SG
vpc-40944d27
Security Group: sg-faf9468b
Description
Inbound
Outbound
Tags
Group name
Ansible-Controller-SG
Group ID
sg-faf9468b

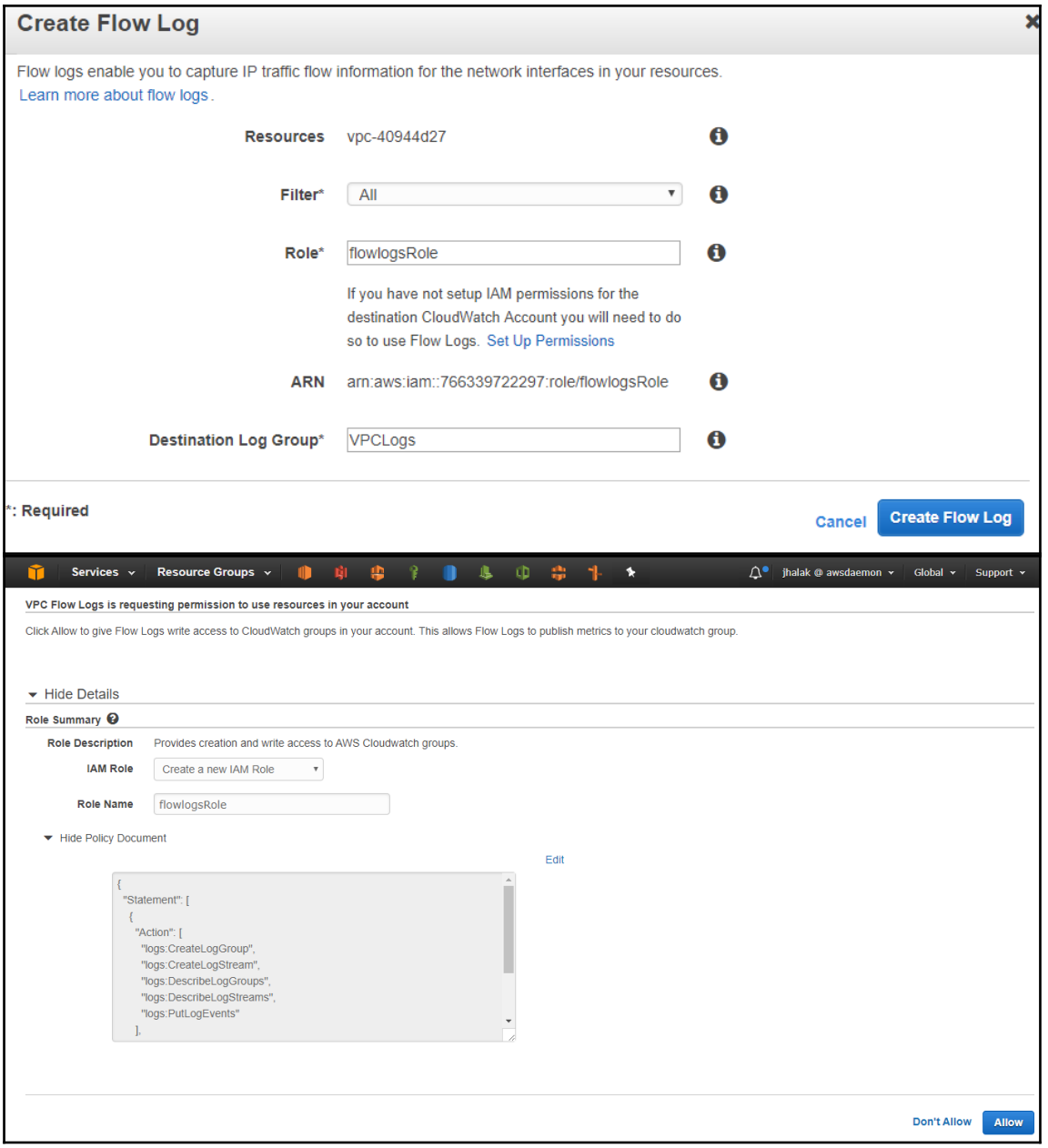

Security Group: sg-faf9468b
Description
Inbound
Outbound
Tags
Edit
Type
Protocol
Port Range
Source
Custom ICMP Rule - IPv4
Echo Reply
N/A
0.0.0.0/0
Custom ICMP Rule - IPv4
Echo Reply
N/A
::/0
SSH
TCP
22
0.0.0.0/0
SSH
TCP
22
::/0
Edit inbound rules
Type
Protocol
Port Range
Source
Custom ICMP
Echo Reply
N/A
Custom
0.0.0.0/0
Custom ICMP
Echo Reply
N/A
Custom
::/0
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
Cancel
Save
All ICMP - IPv4
All ICMP - IPv6
All traffic
SSH
SMTP
DNS (UDP)
DNS (TCP)
HTTP
POP3
IMAP
LDAP
HTTPS
SMTPS
Add filter
Protocol
Port Range
Source
Echo Reply
N/A
Custom
0.0.0.0/0
Echo Reply
N/A
Custom
::/0
SSH
TCP
22
My IP
114.143.166.68/32
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
Cancel
Save


VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and thei
Name
Route Table ID
Explicitly
Testing
rtb-00496c67
0 Subnets
rtb-00496c67
Summary
Routes
Subnet Associations
Route Propagation
Route Table ID: rtb-00496c67 | Testing
Explicitly Associated With: 0 Subnets

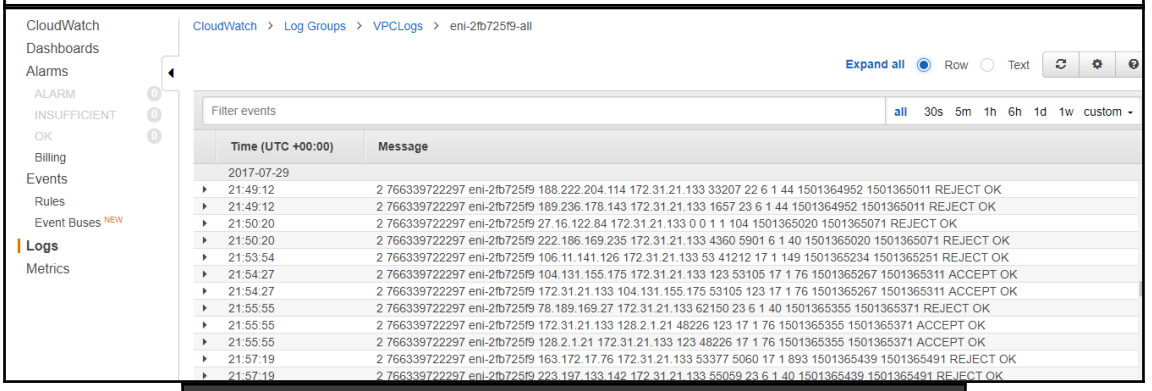

Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and thei
Name
Route Table ID
Explicitly Associat
Main
Testing
rtb-00496c67
0 Subnets
Yes
rtb-00496c67
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
View:
All rules
Destination
Target
Status
Propagated
172.31.0.0/16
local
Active
No
0.0.0.0/0
igw-30ffb854
Active
No

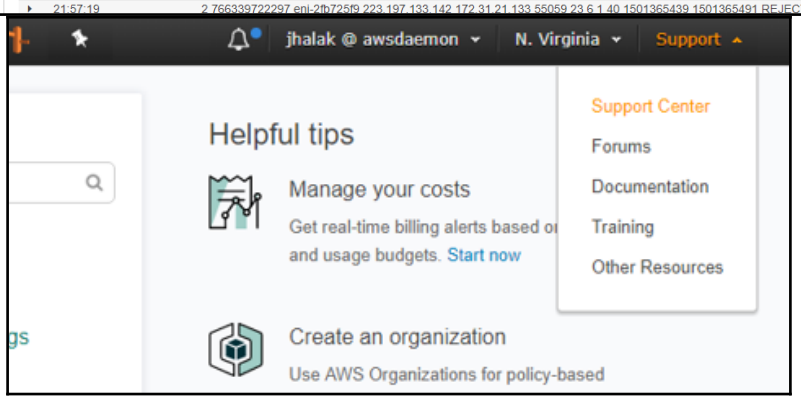

VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets

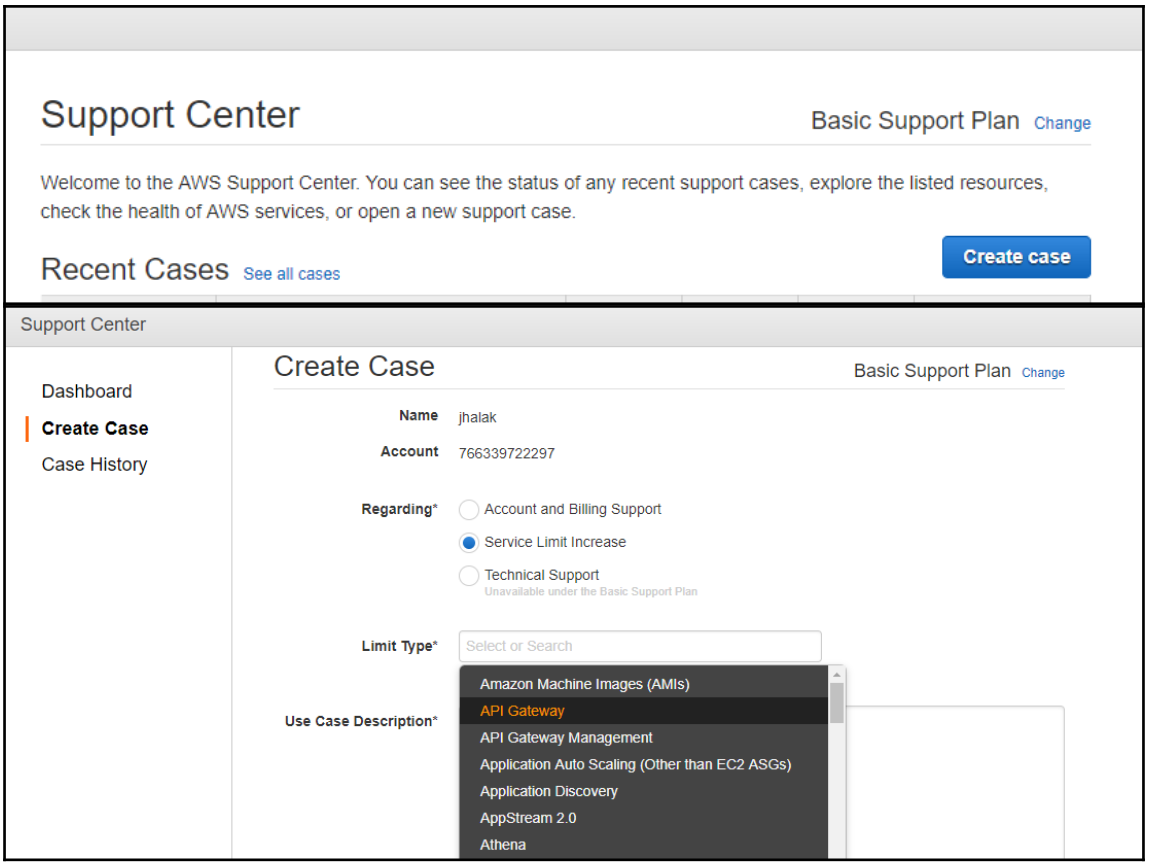

Create Internet Gateway
Delete
Attach to VPC
Detach from VPC
Search Internet Gateways and
Name
ID
State
VPC
igw-30ffb854
attached
vpc-40944d27
igw-30ffb854
Summary
Tags
ID: igw-30ffb854
State: attached
Attached VPC ID: vpc-40944d27
Attachment state: available
VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Create VPC
Actions
Delete VPC
Edit CIDRs
Create Default VPC
Edit DHCP Options Set
Edit DNS Resolution
Edit DNS Hostnames
Create Flow Log
Search VP
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
vpc-40944d27
available
172.31.0.0/16
vpc-40944d27

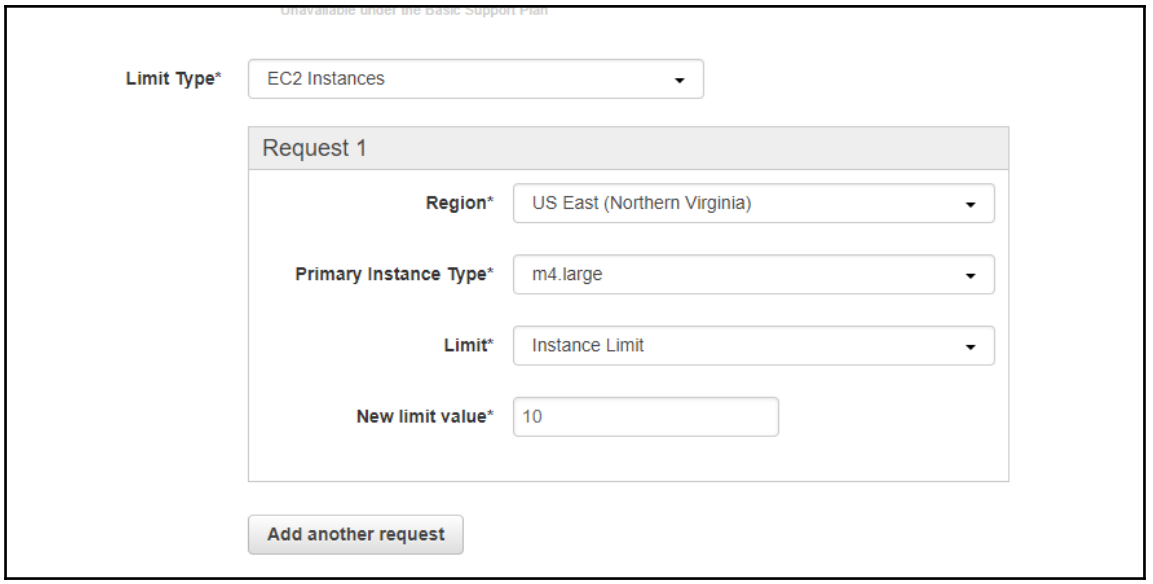

Create Flow Log
Flow logs enable you to capture IP traffic flow information for the network interfaces in your resources.
Learn more about flow logs.
Resources
vpc-40944d27
Filter*
All
Role*
flowlogsRole
If you have not setup IAM permissions for the destination CloudWatch Account you will need to do so to use Flow Logs. Set Up Permissions
ARN
arn:aws:iam::766339722297:role/flowlogsRole
Destination Log Group*
VPCLogs
*: Required
Cancel
Create Flow Log
Services
Resource Groups
jhalak @ awsdaemon
Global
Support
VPC Flow Logs is requesting permission to use resources in your account
Click Allow to give Flow Logs write access to CloudWatch groups in your account. This allows Flow Logs to publish metrics to your cloudwatch group.
Hide Details
Role Summary
Role Description
Provides creation and write access to AWS Cloudwatch groups.
IAM Role
Create a new IAM Role
Role Name
flowlogsRole
Hide Policy Document
Edit
{
"Statement": [
{
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:DescribeLogGroups",
"logs:DescribeLogStreams",
"logs:PutLogEvents"
],
Don't Allow
Allow

Create VPC
Actions
Search VPCs and their proper
1 to 1 of 1 VPC
Name
VPC ID
State
IPv4 CIDR
IPv6 CIDR
DHCP options set
Route table
vpc-40944d27
available
172.31.0.0/16
dopt-e07f8184
rtb-00496c67 | ...
vpc-40944d27
Summary
Flow Logs
Tags
You can create flow logs on your resources to capture IP traffic flow information for the network interfaces for your resources. Learn more about flow logs.
Create Flow Log
Flow Log ID
Filter
CloudWatch Logs Group
IAM Role ARN
Creation Time
Status
Inherited From
fl-716d9d18
ALL
VPCLogs
arn:aws:iam::766339722297:role/flowlogsRole
July 30, 2017 at 1:14:33 AM UTC+5:30
Active
-

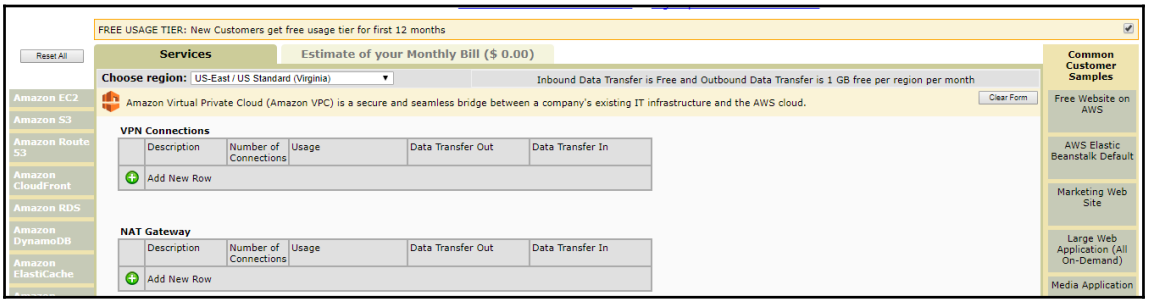

CloudWatch
Dashboards
Alarms
ALARM
INSUFFICIENT
OK
Billing
Events
Rules
Event Buses NEW
Logs
Metrics
CloudWatch > Log Groups > VPCLogs > eni-2fb725f9-all
Expand all
Row
Text
Filter events
all
30s
5m
1h
6h
1d
1w
custom
Time (UTC +00:00)
Message
2017-07-29
21:49:12 2 766339722297 eni-2fb725f9 188.222.204.114 172.31.21.133 33207 22 6 1 44 1501364952 1501365011 REJECT OK
21:49:12 2 766339722297 eni-2fb725f9 189.236.178.143 172.31.21.133 1657 23 6 1 44 1501364952 1501365011 REJECT OK
21:50:20 2 766339722297 eni-2fb725f9 27.16.122.84 172.31.21.133 0 0 1 1 104 1501365020 1501365071 REJECT OK
21:50:20 2 766339722297 eni-2fb725f9 222.186.169.235 172.31.21.133 4360 5901 6 1 40 1501365020 1501365071 REJECT OK
21:53:54 2 766339722297 eni-2fb725f9 106.11.141.126 172.31.21.133 53 41212 17 1 149 1501365234 1501365251 REJECT OK
21:54:27 2 766339722297 eni-2fb725f9 104.131.155.175 172.31.21.133 123 53105 17 1 76 1501365267 1501365311 ACCEPT OK
21:54:27 2 766339722297 eni-2fb725f9 172.31.21.133 104.131.155.175 53105 123 17 1 76 1501365267 1501365311 ACCEPT OK
21:55:55 2 766339722297 eni-2fb725f9 78.189.169.27 172.31.21.133 62150 23 6 1 40 1501365355 1501365371 REJECT OK
21:55:55 2 766339722297 eni-2fb725f9 172.31.21.133 128.2.1.21 48226 123 17 1 76 1501365355 1501365371 ACCEPT OK
21:55:55 2 766339722297 eni-2fb725f9 128.2.1.21 172.31.21.133 123 48226 17 1 76 1501365355 1501365371 ACCEPT OK
21:57:19 2 766339722297 eni-2fb725f9 163.172.17.76 172.31.21.133 53377 5060 17 1 893 1501365439 1501365491 REJECT OK
21:57:19 2 766339722297 eni-2fb725f9 223.197.133.142 172.31.21.133 55059 23 6 1 40 1501365439 1501365491 REJECT OK

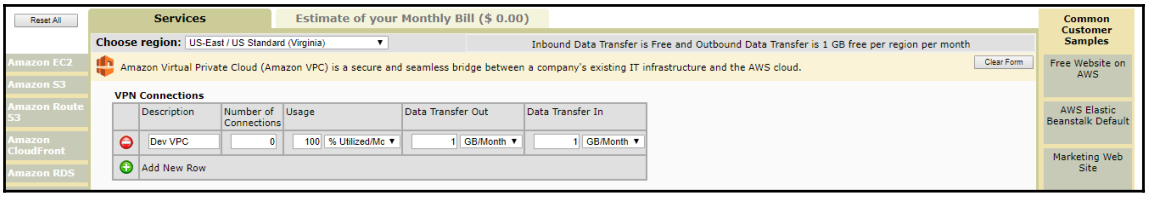

jhalak @ awsdaemon
N. Virginia
Support
Support Center
Forums
Documentation
Training
Other Resources
Helpful tips
Manage your costs
Get real-time billing alerts based o
and usage budgets. Start now
Create an organization
Use AWS Organizations for policy-based

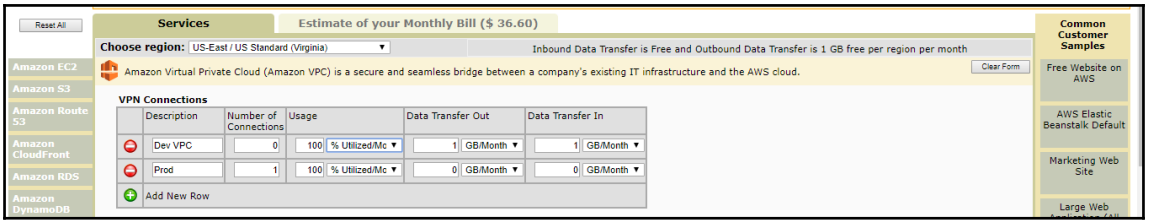

Support Center
Basic Support Plan Change
Welcome to the AWS Support Center. You can see the status of any recent support cases, explore the listed resources, check the health of AWS services, or open a new support case.
Recent Cases See all cases
Create case
Support Center
Dashboard
Create Case
Case History
Create Case
Basic Support Plan Change
Name jhalak
Account 766339722297
Regarding* Account and Billing Support
Service Limit Increase
Technical Support
Unavailable under the Basic Support Plan
Limit Type* Select or Search
Use Case Description*
Amazon Machine Images (AMIs)
API Gateway
API Gateway Management
Application Auto Scaling (Other than EC2 ASGs)
Application Discovery
AppStream 2.0
Athena

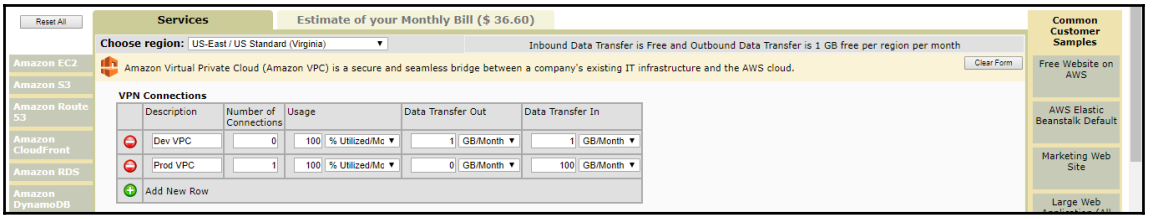

Unavailable under the Basic Support Plan
Limit Type*
EC2 Instances
Request 1
Region*
US East (Northern Virginia)
Primary Instance Type*
m4.large
Limit*
Instance Limit
New limit value*
10
Add another request

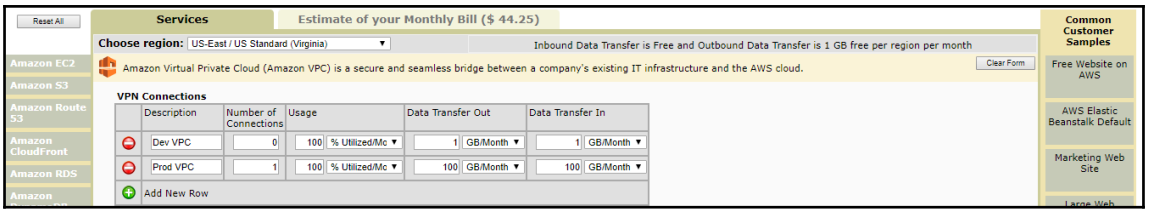
Chapter 9: Pricing of VPC and Related Components

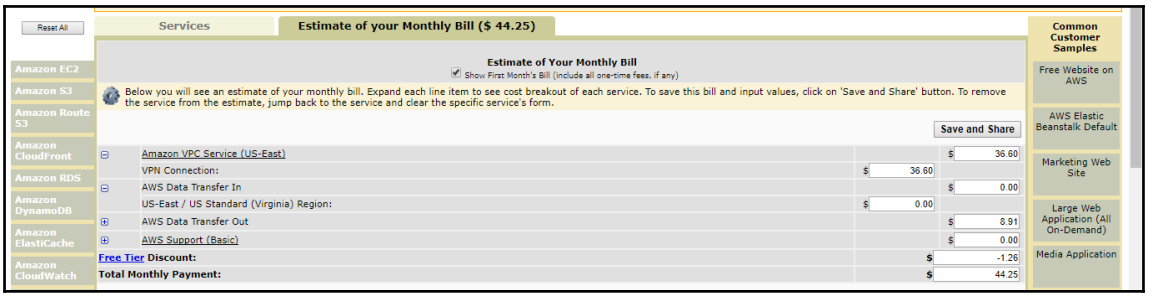


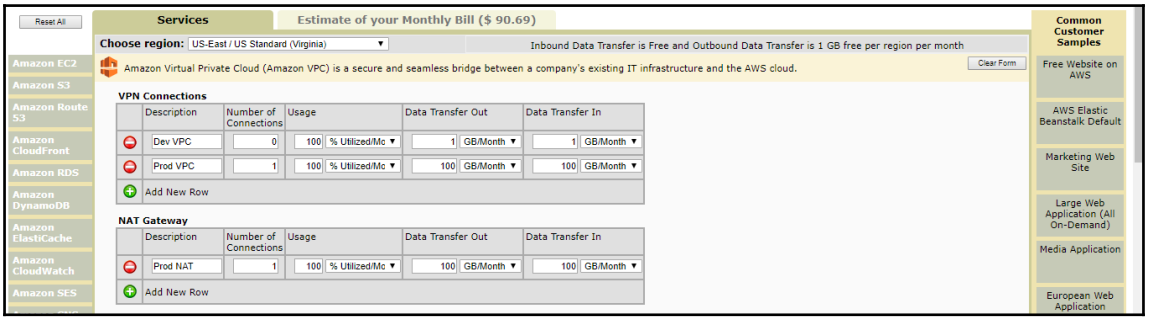


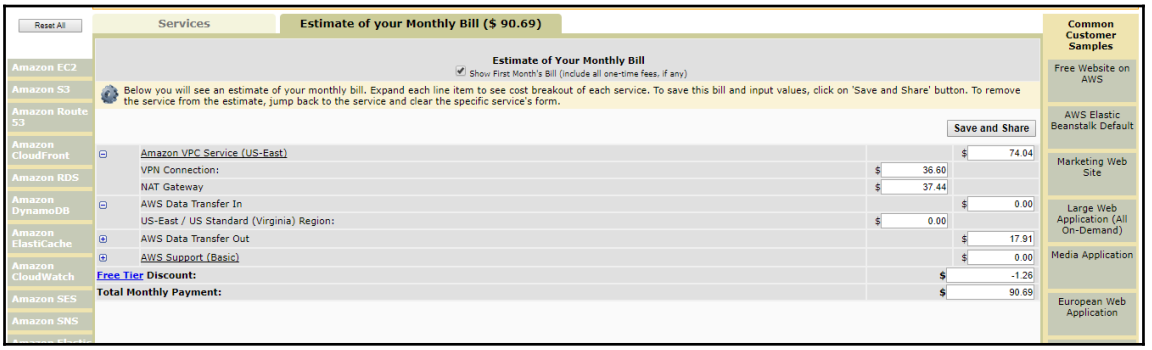


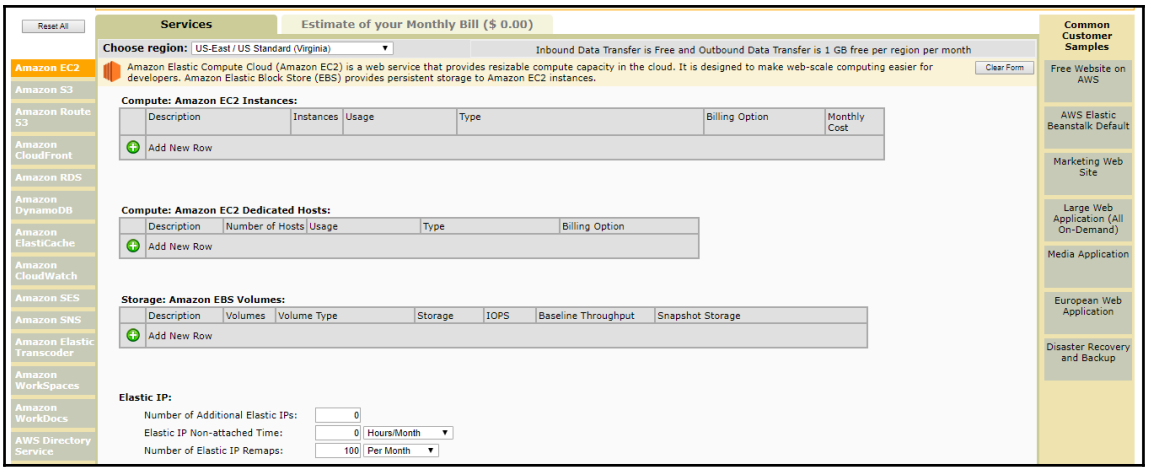


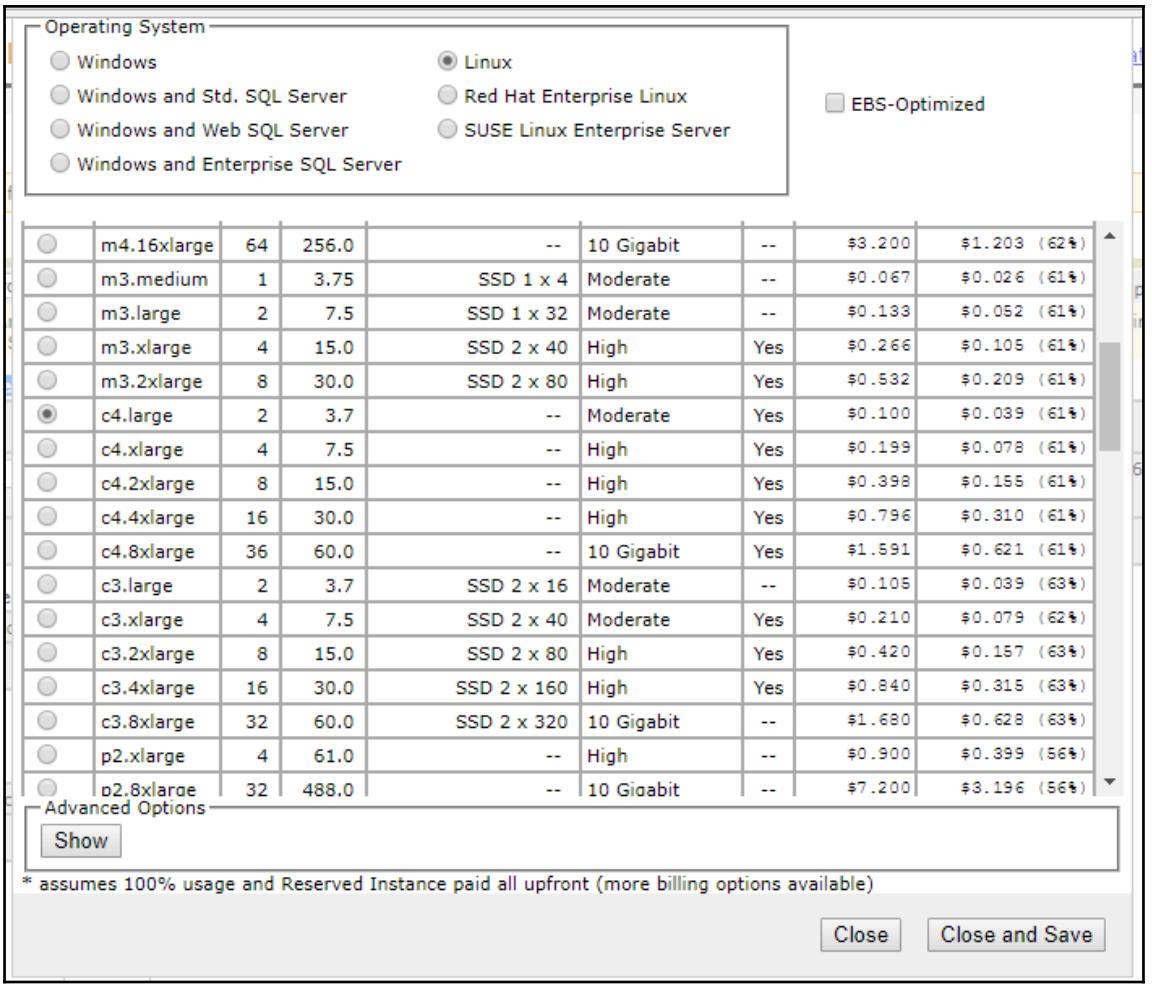

Reset All
Services
Estimate of your Monthly Bill ($ 44.25)
Choose region: US-East / US Standard (Virginia)
Inbound Data Transfer is Free and Outbound Data Transfer is 1 GB free per region per month
Amazon Virtual Private Cloud (Amazon VPC) is a secure and seamless bridge between a company's existing IT infrastructure and the AWS cloud.
Clear Form
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
VPN Connections
Description
Number of Connections
Usage
Data Transfer Out
Data Transfer In
Dev VPC
Prod VPC
% Utilized/Mo
GB/Month
Add New Row
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site

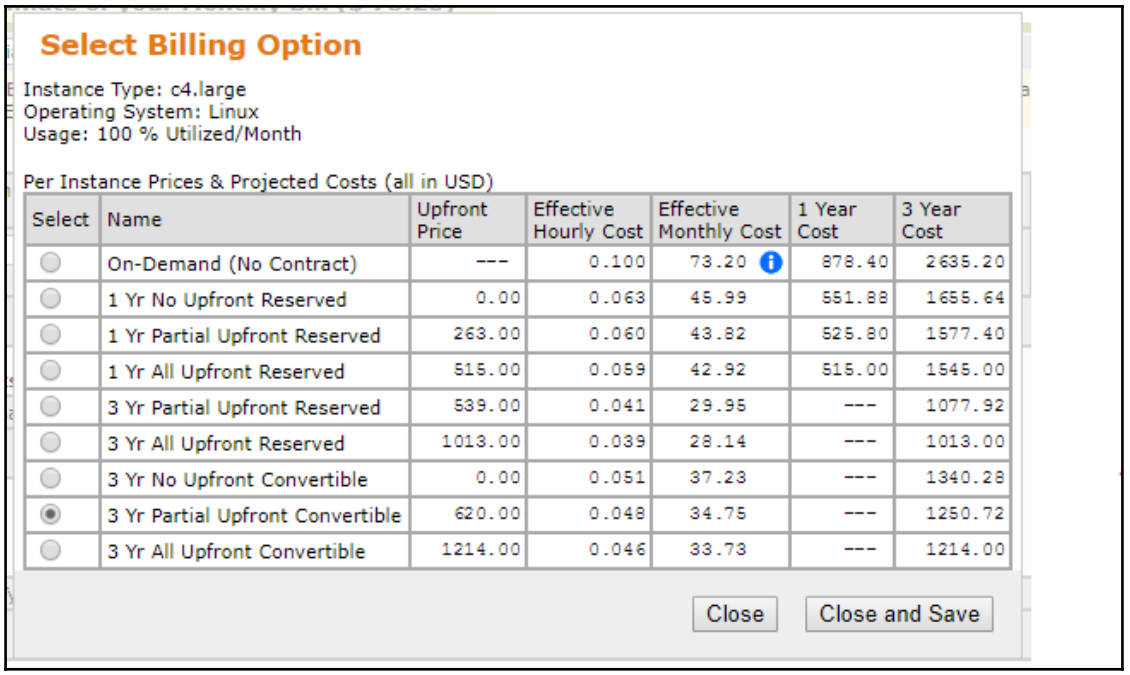

Reset All
Services
Estimate of your Monthly Bill ($ 44.25)
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
Amazon VPC Service (US-East)
VPN Connection:
AWS Data Transfer In
US-East / US Standard (Virginia) Region:
AWS Data Transfer Out
AWS Support (Basic)
Free Tier Discount:
Total Monthly Payment:
36.60
0.00
8.91
0.00
-1.26
44.25
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application


Reset All
Services
Estimate of your Monthly Bill ($ 90.69)
Choose region: US-East / US Standard (Virginia)
Inbound Data Transfer is Free and Outbound Data Transfer is 1 GB free per region per month
Amazon Virtual Private Cloud (Amazon VPC) is a secure and seamless bridge between a company's existing IT infrastructure and the AWS cloud.
Clear Form
VPN Connections
Description
Number of Connections
Usage
Data Transfer Out
Data Transfer In
Dev VPC
Prod VPC
% Utilized/Mo
GB/Month
Add New Row
NAT Gateway
Prod NAT
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Amazon SES
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application
European Web Application


Reset All
Services
Estimate of your Monthly Bill ($ 90.69)
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
Amazon VPC Service (US-East)
VPN Connection:
NAT Gateway
AWS Data Transfer In
US-East / US Standard (Virginia) Region:
AWS Data Transfer Out
AWS Support (Basic)
Free Tier Discount:
Total Monthly Payment:
74.04
36.60
37.44
0.00
0.00
17.91
0.00
-1.26
90.69
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Amazon SES
Amazon SNS
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application
European Web Application


Reset All
Services
Estimate of your Monthly Bill ($ 0.00)
Choose region: US-East / US Standard (Virginia)
Inbound Data Transfer is Free and Outbound Data Transfer is 1 GB free per region per month
Clear Form
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed to make web-scale computing easier for developers. Amazon Elastic Block Store (EBS) provides persistent storage to Amazon EC2 instances.
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Amazon SES
Amazon SNS
Amazon Elastic Transcoder
Amazon WorkSpaces
Amazon WorkDocs
AWS Directory Service
Compute: Amazon EC2 Instances:
Description
Instances
Usage
Type
Billing Option
Monthly Cost
Add New Row
Compute: Amazon EC2 Dedicated Hosts:
Description
Number of Hosts
Usage
Type
Billing Option
Add New Row
Storage: Amazon EBS Volumes:
Description
Volumes
Volume Type
Storage
IOPS
Baseline Throughput
Snapshot Storage
Add New Row
Elastic IP:
Number of Additional Elastic IPs: 0
Elastic IP Non-attached Time: 0 Hours/Month
Number of Elastic IP Remaps: 100 Per Month
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application
European Web Application
Disaster Recovery and Backup


Operating System
Windows
Windows and Std. SQL Server
Windows and Web SQL Server
Windows and Enterprise SQL Server
Linux
Red Hat Enterprise Linux
SUSE Linux Enterprise Server
EBS-Optimized
m4.16xlarge 64 256.0 -- 10 Gigabit -- $3.200 $1.203 (62%)
m3.medium 1 3.75 SSD 1 x 4 Moderate -- $0.067 $0.026 (61%)
m3.large 2 7.5 SSD 1 x 32 Moderate -- $0.133 $0.052 (61%)
m3.xlarge 4 15.0 SSD 2 x 40 High Yes $0.266 $0.105 (61%)
m3.2xlarge 8 30.0 SSD 2 x 80 High Yes $0.532 $0.209 (61%)
c4.large 2 3.7 -- Moderate Yes $0.100 $0.039 (61%)
c4.xlarge 4 7.5 -- High Yes $0.199 $0.078 (61%)
c4.2xlarge 8 15.0 -- High Yes $0.398 $0.155 (61%)
c4.4xlarge 16 30.0 -- High Yes $0.796 $0.310 (61%)
c4.8xlarge 36 60.0 -- 10 Gigabit Yes $1.591 $0.621 (61%)
c3.large 2 3.7 SSD 2 x 16 Moderate -- $0.105 $0.039 (63%)
c3.xlarge 4 7.5 SSD 2 x 40 Moderate Yes $0.210 $0.079 (62%)
c3.2xlarge 8 15.0 SSD 2 x 80 High Yes $0.420 $0.157 (63%)
c3.4xlarge 16 30.0 SSD 2 x 160 High Yes $0.840 $0.315 (63%)
c3.8xlarge 32 60.0 SSD 2 x 320 10 Gigabit -- $1.680 $0.628 (63%)
p2.xlarge 4 61.0 -- High -- $0.900 $0.399 (56%)
p2.8xlarge 32 488.0 -- 10 Gigabit -- $7.200 $3.196 (56%)
Advanced Options
Show
* assumes 100% usage and Reserved Instance paid all upfront (more billing options available)
Close
Close and Save



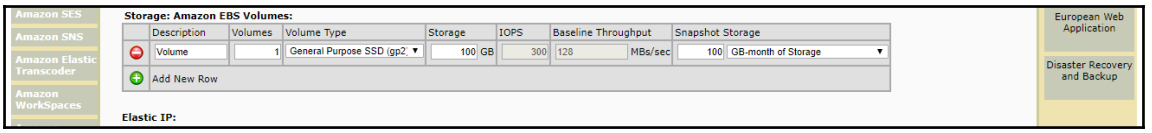
Select Billing Option

Instance Type: c4.large
Operating System: Linux
Usage: 100 % Utilized/Month

Per Instance Prices & Projected Costs (all in USD)

Select	Name	Upfront Price	Effective Hourly Cost	Effective Monthly Cost	1 Year Cost	3 Year Cost
○	On-Demand (No Contract)	---	0.100	73.20	878.40	2635.20
○	1 Yr No Upfront Reserved	0.00	0.063	45.99	551.88	1655.64
○	1 Yr Partial Upfront Reserved	263.00	0.060	43.82	525.80	1577.40
○	1 Yr All Upfront Reserved	515.00	0.059	42.92	515.00	1545.00
○	3 Yr Partial Upfront Reserved	539.00	0.041	29.95	---	1077.92
○	3 Yr All Upfront Reserved	1013.00	0.039	28.14	---	1013.00
○	3 Yr No Upfront Convertible	0.00	0.051	37.23	---	1340.28
◉	3 Yr Partial Upfront Convertible	620.00	0.048	34.75	---	1250.72
○	3 Yr All Upfront Convertible	1214.00	0.046	33.73	---	1214.00

Close | Close and Save



Amazon SES
Amazon SNS
Amazon Elastic Transcoder
Amazon WorkSpaces

Storage: Amazon EBS Volumes:

Description	Volumes	Volume Type	Storage	IOPS	Baseline Throughput	Snapshot Storage
Volume	1	General Purpose SSD (gp2)	100 GB	300	128 MBs/sec	100 GB-month of Storage

Add New Row

Elastic IP:

European Web Application
Disaster Recovery and Backup

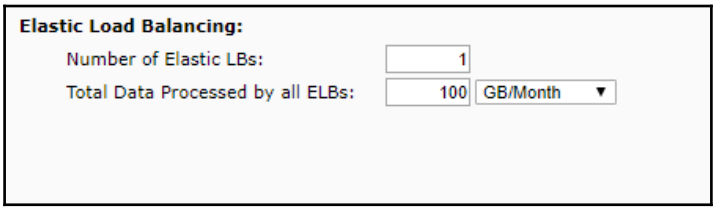
Amazon WorkSpaces
Amazon WorkDocs
AWS Directory Service
Amazon Redshift
Amazon Glacier
Amazon SQS
Amazon SWF
Amazon Elastic MapReduce

Elastic IP:

Number of Additional Elastic IPs:	1	
Elastic IP Non-attached Time:	0	Hours/Month
Number of Elastic IP Remaps:	2	Per Month

Data Transfer:

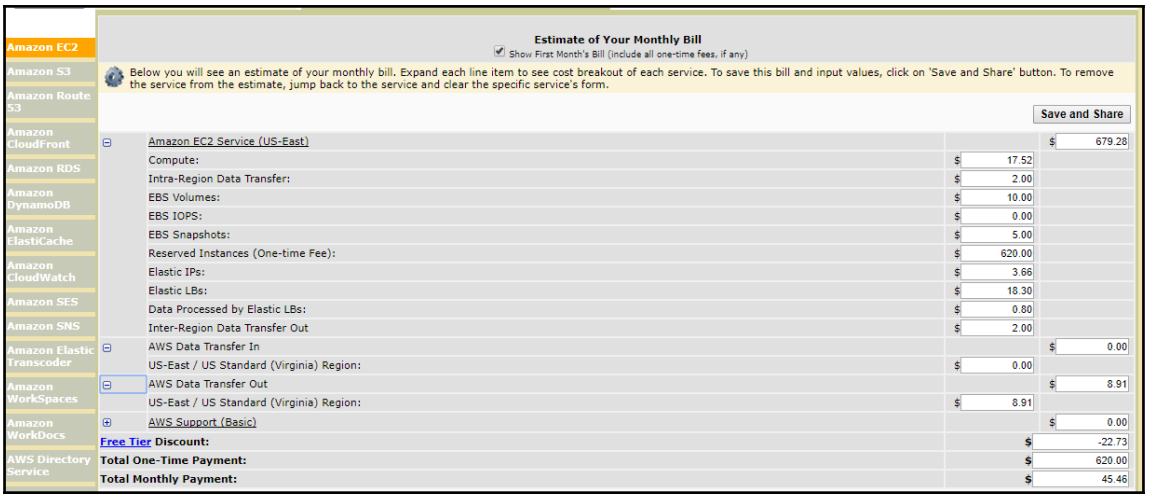
Inter-Region Data Transfer Out:	100	GB/Month
Data Transfer Out:	100	GB/Month
Data Transfer In:	100	GB/Month
VPC Peering Data Transfer:	0	GB/Month
Intra-Region Data Transfer:	100	GB/Month
Public IP/Elastic IP Data Transfer:	100	GB/Month



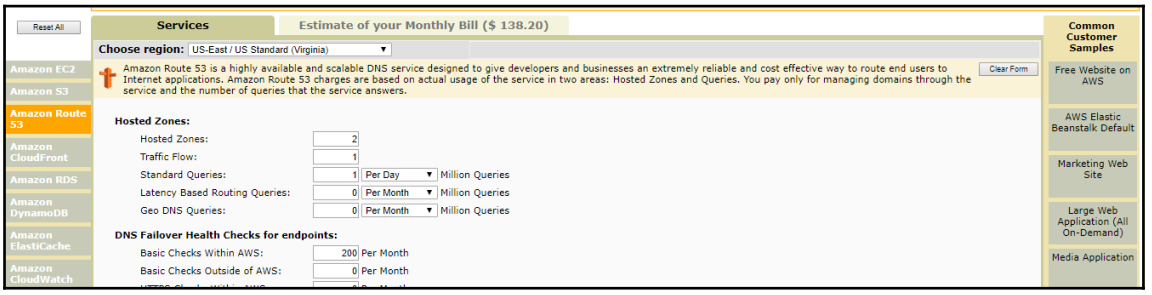
Elastic Load Balancing:

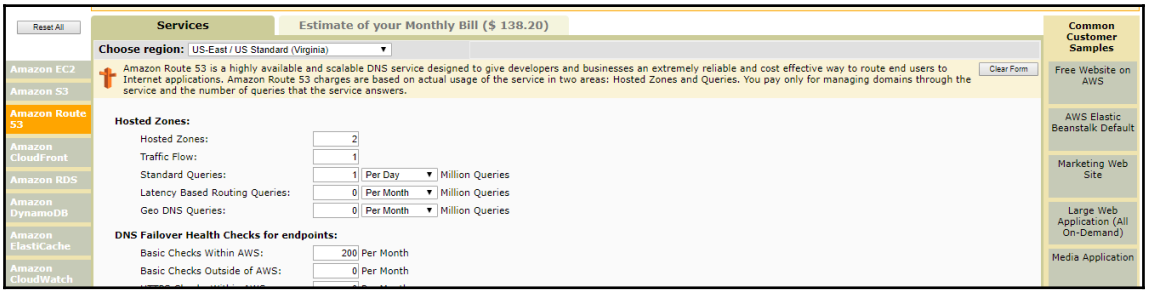
Number of Elastic LBs: 1

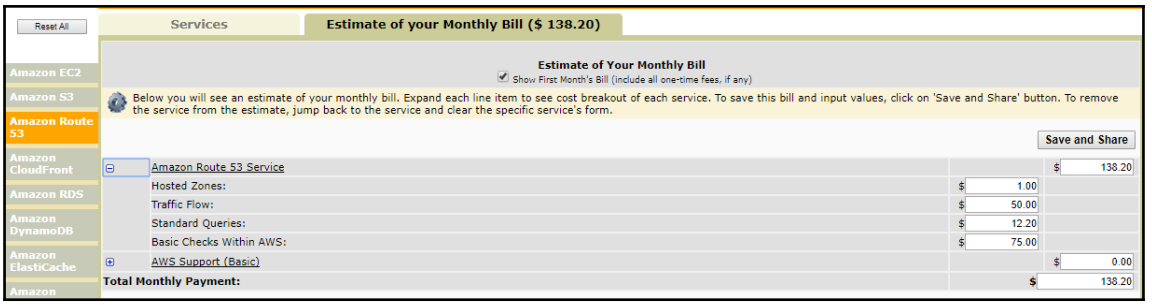
Total Data Processed by all ELBs: 100 GB/Month

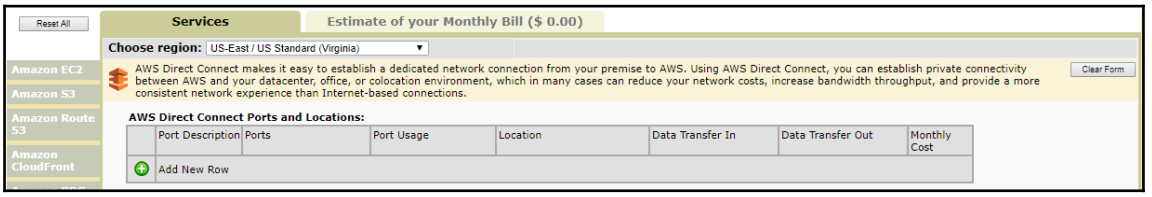

Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Amazon SES
Amazon SNS
Amazon Elastic Transcoder
Amazon WorkSpaces
Amazon WorkDocs
AWS Directory Service
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
Amazon EC2 Service (US-East) $ 679.28
Compute: $ 17.52
Intra-Region Data Transfer: $ 2.00
EBS Volumes: $ 10.00
EBS IOPS: $ 0.00
EBS Snapshots: $ 5.00
Reserved Instances (One-time Fee): $ 620.00
Elastic IPs: $ 3.66
Elastic LBs: $ 18.30
Data Processed by Elastic LBs: $ 0.80
Inter-Region Data Transfer Out $ 2.00
AWS Data Transfer In $ 0.00
US-East / US Standard (Virginia) Region: $ 0.00
AWS Data Transfer Out $ 8.91
US-East / US Standard (Virginia) Region: $ 8.91
AWS Support (Basic) $ 0.00
Free Tier Discount: $ -22.73
Total One-Time Payment: $ 620.00
Total Monthly Payment: $ 45.46

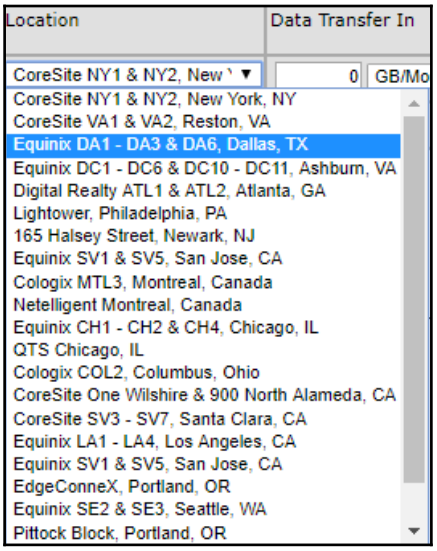
Reset All
Services
Estimate of your Monthly Bill ($ 0.00)
Choose region: US-East / US Standard (Virginia)
Amazon Route 53 is a highly available and scalable DNS service designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications. Amazon Route 53 charges are based on actual usage of the service in two areas: Hosted Zones and Queries. You pay only for managing domains through the service and the number of queries that the service answers.
Clear Form
Hosted Zones:
Hosted Zones: 0
Traffic Flow: 0
Standard Queries: 0 Per Month Million Queries
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site

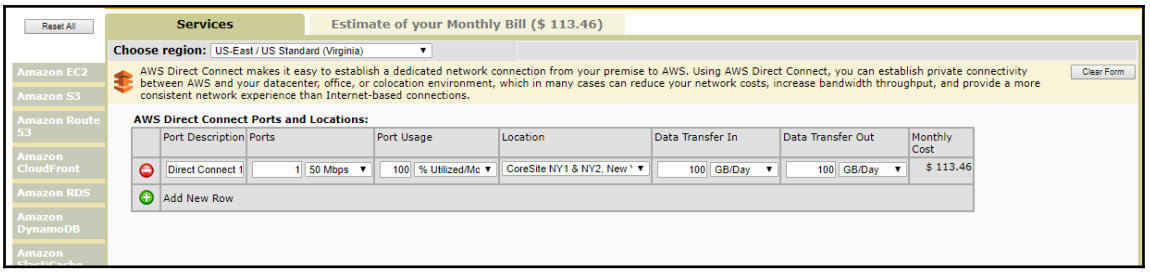

Reset All
Services
Estimate of your Monthly Bill ($ 138.20)
Choose region: US-East / US Standard (Virginia)
Amazon Route 53 is a highly available and scalable DNS service designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications. Amazon Route 53 charges are based on actual usage of the service in two areas: Hosted Zones and Queries. You pay only for managing domains through the service and the number of queries that the service answers.
Clear Form
Hosted Zones:
Hosted Zones: 2
Traffic Flow: 1
Standard Queries: 1 Per Day Million Queries
Latency Based Routing Queries: 0 Per Month Million Queries
Geo DNS Queries: 0 Per Month Million Queries
DNS Failover Health Checks for endpoints:
Basic Checks Within AWS: 200 Per Month
Basic Checks Outside of AWS: 0 Per Month
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application

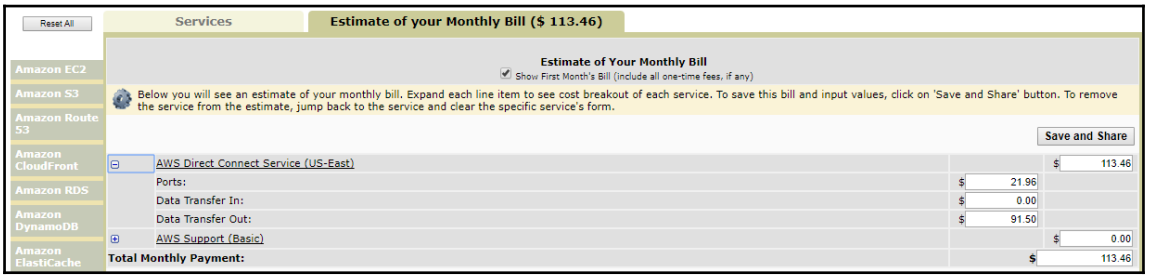

Reset All
Services
Estimate of your Monthly Bill ($ 138.20)
Choose region: US-East / US Standard (Virginia)
Amazon Route 53 is a highly available and scalable DNS service designed to give developers and businesses an extremely reliable and cost effective way to route end users to Internet applications. Amazon Route 53 charges are based on actual usage of the service in two areas: Hosted Zones and Queries. You pay only for managing domains through the service and the number of queries that the service answers.
Clear Form
Hosted Zones:
Hosted Zones: 2
Traffic Flow: 1
Standard Queries: 1 Per Day Million Queries
Latency Based Routing Queries: 0 Per Month Million Queries
Geo DNS Queries: 0 Per Month Million Queries
DNS Failover Health Checks for endpoints:
Basic Checks Within AWS: 200 Per Month
Basic Checks Outside of AWS: 0 Per Month
Common Customer Samples
Free Website on AWS
AWS Elastic Beanstalk Default
Marketing Web Site
Large Web Application (All On-Demand)
Media Application

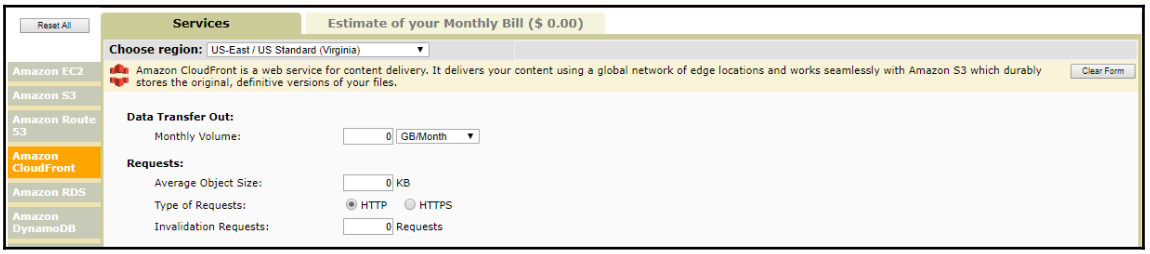

Reset All
Services
Estimate of your Monthly Bill ($ 138.20)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
Amazon Route 53 Service $ 138.20
Hosted Zones: $ 1.00
Traffic Flow: $ 50.00
Standard Queries: $ 12.20
Basic Checks Within AWS: $ 75.00
AWS Support (Basic) $ 0.00
Total Monthly Payment: $ 138.20

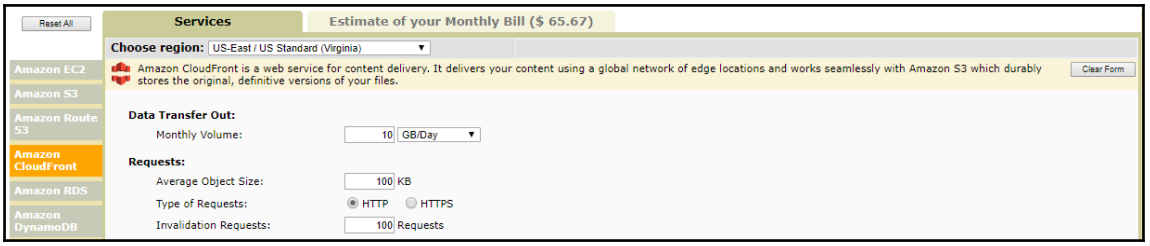

Reset All
Services
Estimate of your Monthly Bill ($ 0.00)
Choose region: US-East / US Standard (Virginia)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
AWS Direct Connect makes it easy to establish a dedicated network connection from your premise to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
Clear Form
AWS Direct Connect Ports and Locations:
Port Description
Ports
Port Usage
Location
Data Transfer In
Data Transfer Out
Monthly Cost
Add New Row

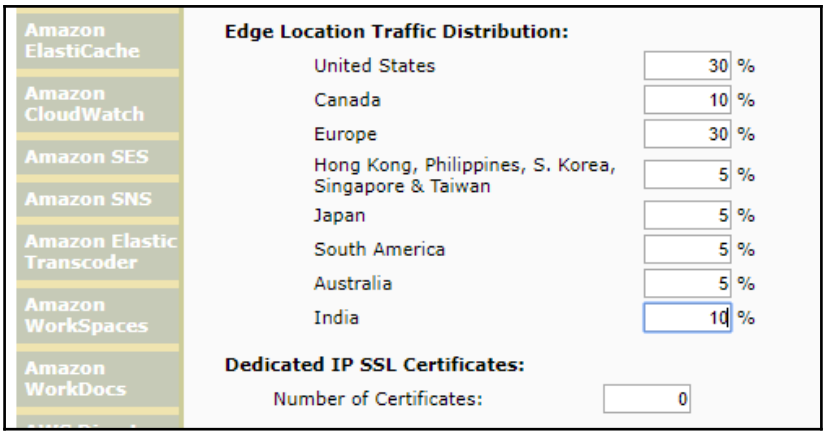

Location
Data Transfer In
CoreSite NY1 & NY2, New
0
GB/Mo
CoreSite NY1 & NY2, New York, NY
CoreSite VA1 & VA2, Reston, VA
Equinix DA1 - DA3 & DA6, Dallas, TX
Equinix DC1 - DC6 & DC10 - DC11, Ashburn, VA
Digital Realty ATL1 & ATL2, Atlanta, GA
Lightower, Philadelphia, PA
165 Halsey Street, Newark, NJ
Equinix SV1 & SV5, San Jose, CA
Cologix MTL3, Montreal, Canada
Netelligent Montreal, Canada
Equinix CH1 - CH2 & CH4, Chicago, IL
QTS Chicago, IL
Cologix COL2, Columbus, Ohio
CoreSite One Wilshire & 900 North Alameda, CA
CoreSite SV3 - SV7, Santa Clara, CA
Equinix LA1 - LA4, Los Angeles, CA
Equinix SV1 & SV5, San Jose, CA
EdgeConneX, Portland, OR
Equinix SE2 & SE3, Seattle, WA
Pittock Block, Portland, OR

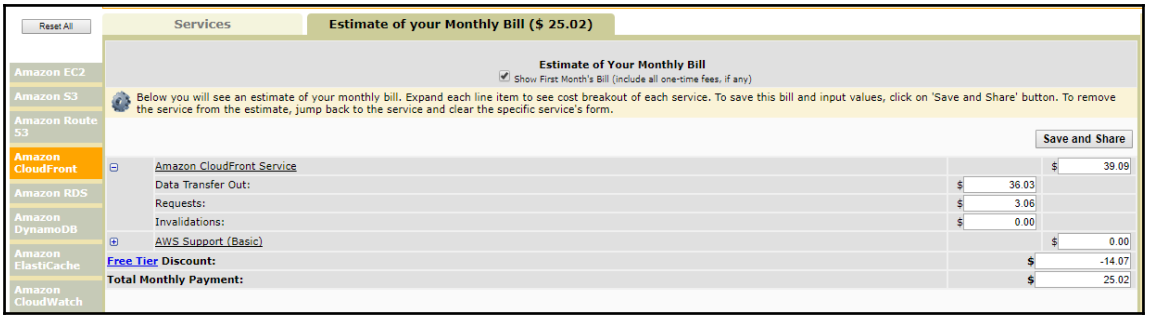

Reset All
Services
Estimate of your Monthly Bill ($ 113.46)
Choose region: US-East / US Standard (Virginia)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
AWS Direct Connect makes it easy to establish a dedicated network connection from your premise to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your datacenter, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.
Clear Form
AWS Direct Connect Ports and Locations:
Port Description
Ports
Port Usage
Location
Data Transfer In
Data Transfer Out
Monthly Cost
Direct Connect 1
1
50 Mbps
100
% Utilized/Mc
CoreSite NY1 & NY2, New
100
GB/Day
100
GB/Day
$ 113.46
Add New Row


Reset All
Services
Estimate of your Monthly Bill ($ 113.46)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
AWS Direct Connect Service (US-East)
$ 113.46
Ports:
$ 21.96
Data Transfer In:
$ 0.00
Data Transfer Out:
$ 91.50
AWS Support (Basic)
$ 0.00
Total Monthly Payment:
$ 113.46


Reset All
Services
Estimate of your Monthly Bill ($ 0.00)
Choose region: US-East / US Standard (Virginia)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon CloudFront is a web service for content delivery. It delivers your content using a global network of edge locations and works seamlessly with Amazon S3 which durably stores the original, definitive versions of your files.
Clear Form
Data Transfer Out:
Monthly Volume: 0 GB/Month
Requests:
Average Object Size: 0 KB
Type of Requests: HTTP HTTPS
Invalidation Requests: 0 Requests


Reset All
Services
Estimate of your Monthly Bill ($ 65.67)
Choose region: US-East / US Standard (Virginia)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon CloudFront is a web service for content delivery. It delivers your content using a global network of edge locations and works seamlessly with Amazon S3 which durably stores the original, definitive versions of your files.
Clear Form
Data Transfer Out:
Monthly Volume: 10 GB/Day
Requests:
Average Object Size: 100 KB
Type of Requests: HTTP HTTPS
Invalidation Requests: 100 Requests


Amazon ElastiCache
Amazon CloudWatch
Amazon SES
Amazon SNS
Amazon Elastic Transcoder
Amazon WorkSpaces
Amazon WorkDocs
Edge Location Traffic Distribution:
United States 30 %
Canada 10 %
Europe 30 %
Hong Kong, Philippines, S. Korea, Singapore & Taiwan 5 %
Japan 5 %
South America 5 %
Australia 5 %
India 10 %
Dedicated IP SSL Certificates:
Number of Certificates: 0


Reset All
Services
Estimate of your Monthly Bill ($ 25.02)
Amazon EC2
Amazon S3
Amazon Route 53
Amazon CloudFront
Amazon RDS
Amazon DynamoDB
Amazon ElastiCache
Amazon CloudWatch
Estimate of Your Monthly Bill
Show First Month's Bill (include all one-time fees, if any)
Below you will see an estimate of your monthly bill. Expand each line item to see cost breakout of each service. To save this bill and input values, click on 'Save and Share' button. To remove the service from the estimate, jump back to the service and clear the specific service's form.
Save and Share
Amazon CloudFront Service $ 39.09
Data Transfer Out: $ 36.03
Requests: $ 3.06
Invalidations: $ 0.00
AWS Support (Basic) $ 0.00
Free Tier Discount: $ -14.07
Total Monthly Payment: $ 25.02