Navigating on AWS Cloud

Handbook for novice cloud users to help passing AWS Cloud Practitioner Certification Exam

Version: 1.4

Prepared by:
Stefan Hermanto
Email: skherman@us.ibm.com
Slack: skherman

Date Created:
12/15/2021

Latest Revision:
8/17/2022

Revision History

Date	Version	Author	Revision Notes
12/15/2021	1.0	Stefan Hermanto	*Initial Version*
1/8/2022	1.1	Stefan Hermanto	*Fixing page numbers*
3/23/2022	1.2	Stefan Hermanto	*Removing IBM & AWS Logos*
5/16/2022	1.3	Stefan Hermanto	*Modifying headers & footers*
8/17/2022	1.4	Stefan Hermanto	*Removing all Practiced Exam Questions due to copy right issue*

TABLE OF CONTENTS

1 Introduction

1.1 Purpose

This is a Navigation Document for beginner cloud users that are interested in learning about Amazon Web Services (AWS) a self-journey to the cloud and for the cloud novice users who are trying to pass AWS Cloud Practitioner Certification Exam.

1.2 Who Should be Using this Tutorial?

This tutorial would be helpful for novice users who are trying to pass AWS Cloud Practitioner Certification Exam. It would have been very difficult to envision about AWS Cloud, if you just by reading study materials for AWS Cloud Practitioner Certification Exam and without creating AWS Account and getting your feet wet in AWS account activities such as launching EC2 Instances, creating S3 buckets, verifying domain using Amazon Route 53 or downloading Service Organizational Control (SOC) Report from AWS Artifact.

It is like you are given owner manual on how to drive a car and you try to memorize everything on that owner manual i.e., the difference between engine oil vs. transmission oil; sunroof vs. moonroof; hand brake vs. foot break, etc.

Still using the car's analogy, this document letting you to drive the car and get the valuable experiences that you will never earn it just simply by reading the study materials on AWS Cloud Practitioner Certification Exam.

2 Pre-Requisite Steps

2.1 Complete Six hours AWS Mandatory Training

The first step for you on your AWS Cloud Practitioner Certification Exam is to complete the following mandatory training

https://ibm.ontidwit.com/#/libraries/learn-the-aws-cloud-practitioner-essentials

Once you've completed this mandatory training, it will be counted toward your annual Think40 bucket.

2.2 Creating Free AWS Account

In order for you to be able to participate on this AWS Navigation Journey to the Cloud, you need to create a FREE AWS account first.

Google ***"AWS Account Creation"*** and follow the instruction to create a FREE account. Please note that you will need your active credit card to create an AWS Account and make sure you select a FREE Account upon creating an account on AWS.

You will also need an active email account. Please keep in mind that whatever email account that you use *(your personal email account or IBM email account)* will be the root user account.

2.3 Activate your new FREE AWS Account

Once you have successfully created an active free AWS account, you need to activate it. Make sure you can see AWS Management Console since this would be your Landing Page for AWS login activity

2.4 Understand the Charging Principles of AWS

At this point, you have successfully created your AWS account and activate it. Before you start, please understand the concept of AWS charging: ***COMPUTE, STORAGE & OUTBOUND DATA TRANSFER***. If you perform any of these activities, your credit card will be charged!

In most cases, there is no charge for ***INBOUND DATA TRANSFER*** between other AWS services within the same region.

Please also understand when you have Active EC2 running on your region, you will be charged hourly. Creating VPN is free but once you start using it such as for VPC Peering, NAT Gateway, Interface Gateway, your credit card will be charged.

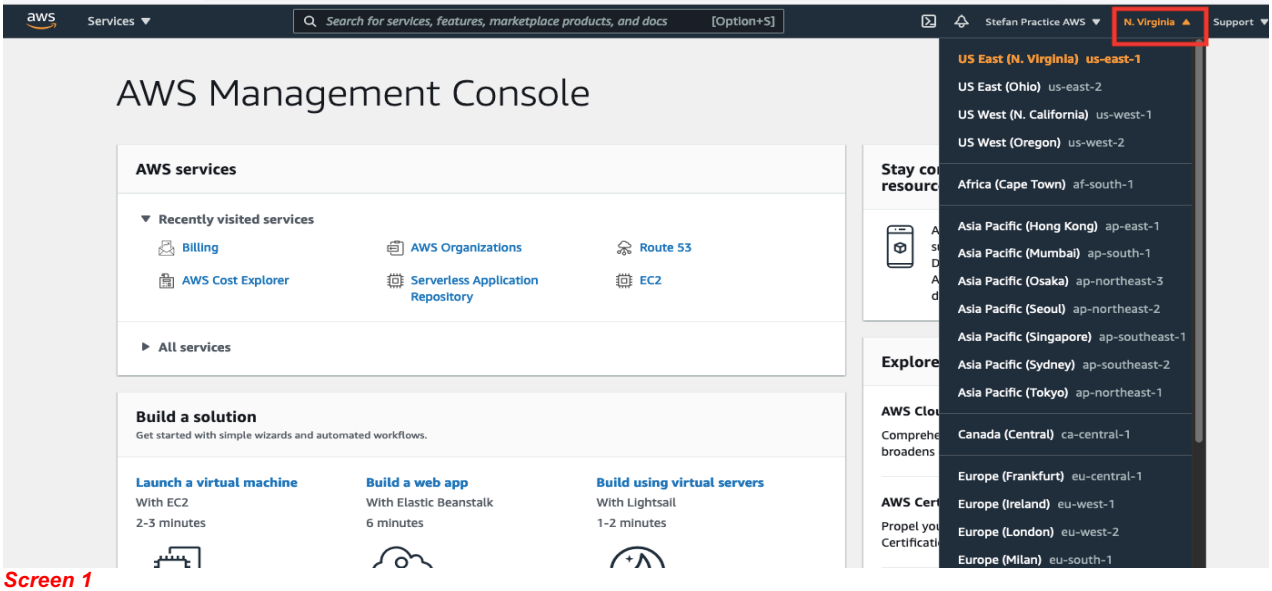
Please note that in every section, you will see a warning should your credit card is charged for the activity that you are about to create.

Please make sure you check your Billing every day or even few times a day!

3 Understanding about AWS Global Structure

3.1 Region

It is a geographical district/physical location. One region consists of at least two Availability Zones (AZs) You can easily change your Region when login into your AWS account



Screen 1

Screen 1 above is showing your current region in Northern Virginia and displaying all other AWS Regions.

3.2 Availability Zone (AZ)

Availability Zone consists of one or more Data Centers owned /operated by AWS. Each AZ consists of one or more discrete Data Centers (Edge Locations). Below are examples of AZs under N. Virginia Region (US-east1).

- US-east1**a**
- US-east1**b**
- US-east1**c**

3.3 Edge Location

Edge Location is data center owned by trusted partner of AWS.

Please note that the maintaining the Global Infrastructure is the responsibility of AWS (Region, Availability Zone & Edge Location) instead of AWS customers.

3.4 AWS Region & Availability Zone Concepts

AWS has the concept of a Region, which is a physical location around the world where we cluster data centers. AWS calls each group of logical data centers an Availability Zone. Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area.

Each AZ has independent power, cooling, and physical security and is connected via redundant, ultra-low-latency networks. AWS customers focused on high availability can design their applications to run in multiple AZ's to achieve even greater fault-tolerance. AWS infrastructure Regions meet the highest levels of security, compliance, and data protection.

- All traffic between Availability Zone is encrypted

- Each AWS Region consists of multiple, isolated, and physically separate AZ's within a geographic area

3.5 Choosing AWS Region

The following points have to be considered when choosing an AWS Region for a service:

- ***Compliance and Data Residency guidelines of the AWS Region should match your business requirements*** - If you have data residency requirements, you can choose the AWS Region that is in close proximity to your desired location.

  You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements.

- ***AWS Region chosen should be geographically closer to the user base that utilizes the hosted AWS services*** - When deploying your applications and workloads to the cloud, you have the flexibility in selecting a technology infrastructure and AWS Region that is closest to your primary target of users.

4 EC2 Instances

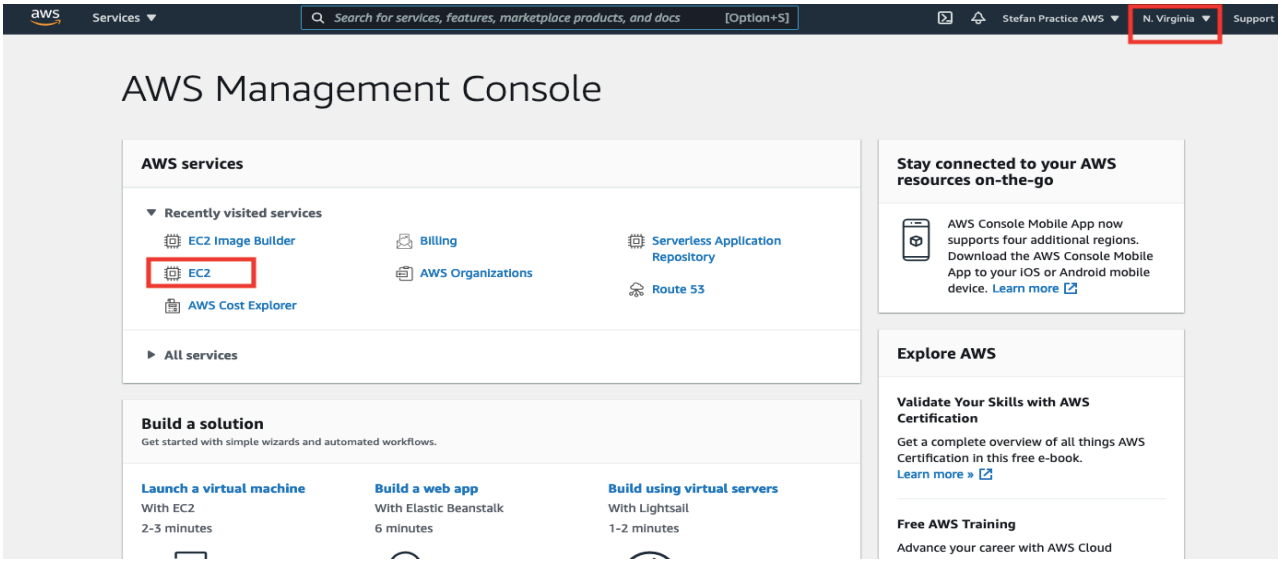
4.1 Creating EC2 Instance

First exercise is to create EC2 Instance. What does it mean by launching EC2 in AWS?
*An instance is a **virtual server in the AWS Cloud**.*

You launch an instance from an Amazon Machine Image (AMI). The AMI provides the operating system, application server, and applications for your instance.

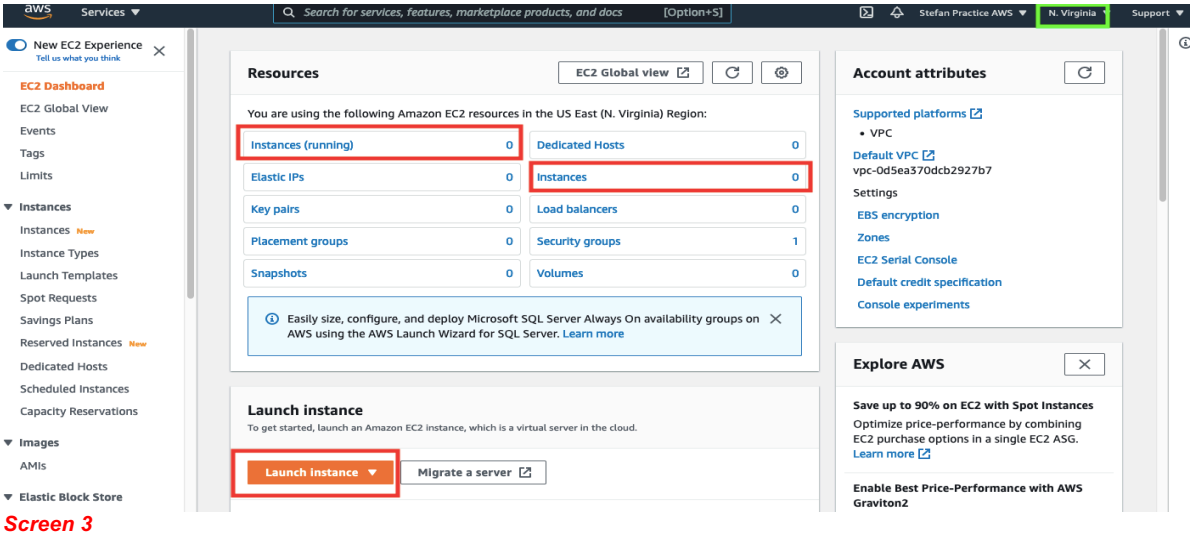
When you sign up for AWS, you can get started with Amazon EC2 for free using the AWS Free Tier.

Login to your AWS Account and you will see screen 2 below. Keep in mind that you are currently in ***Northern Virginia Region***



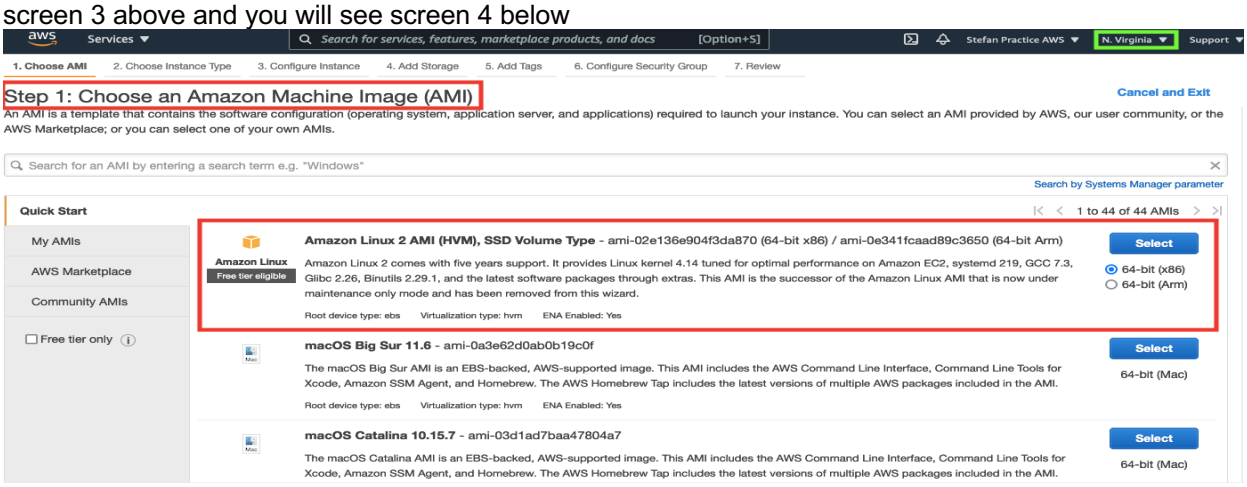
Screen 2

From screen 2 above, click ***"EC2"*** and you will see screen 3 below



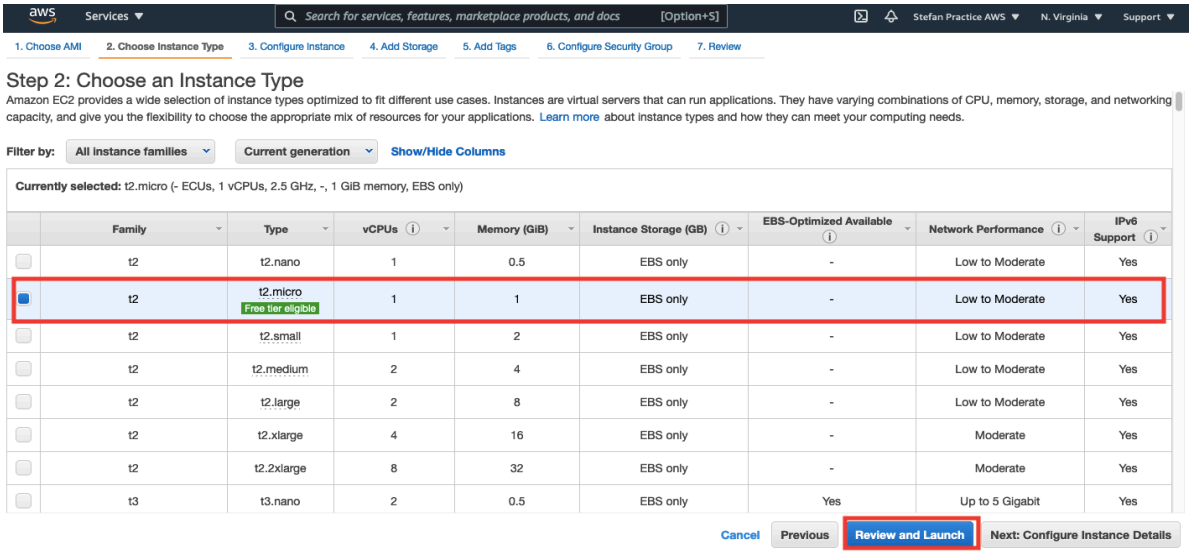
Screen 3

Note in screen 3 above, you do not have any running instances yet. Click ***"Launch Instance"*** from screen 3 above and you will see screen 4 below



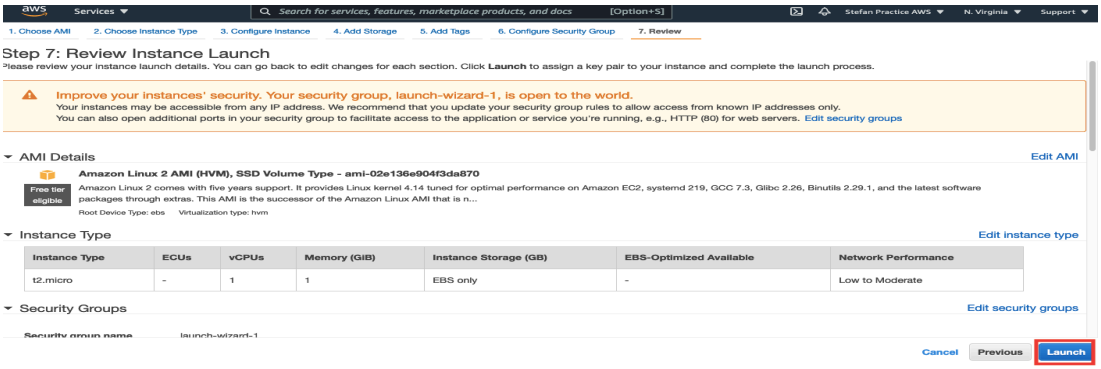
Screen 4

Notice that you are automatically in Amazon Machine Image (AMI), choose an instance, for example, I'm selecting the first one in red box above. Click ***"Select"*** and you will see screen 5 below



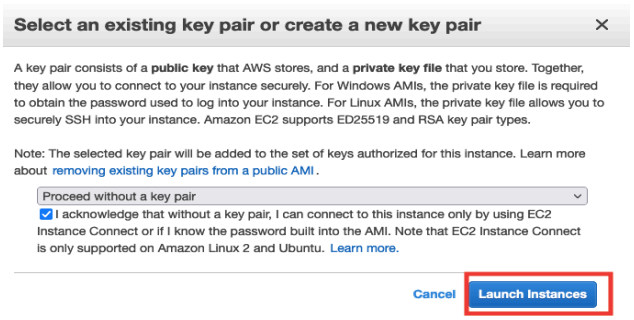
Screen 5

Let's say you select the instance above in screen 5, click ***"Review and Launch"*** and you will see screen 6 below



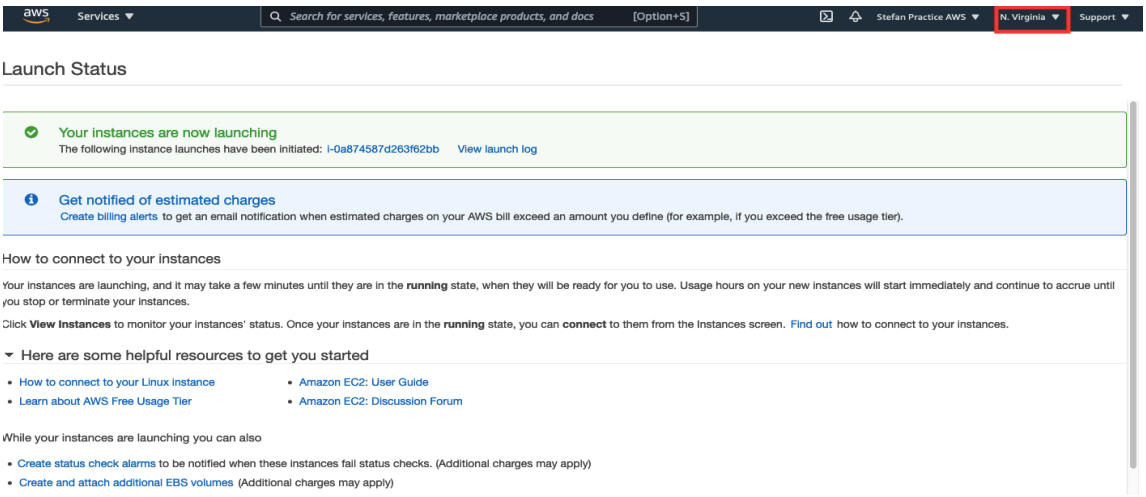
Screen 6

Click ***"Launch"*** on screen 6 above and you will see screen 7 below



Screen 7

Click ***"Launch Instances"*** from screen 7 above and you will see screen 8 below

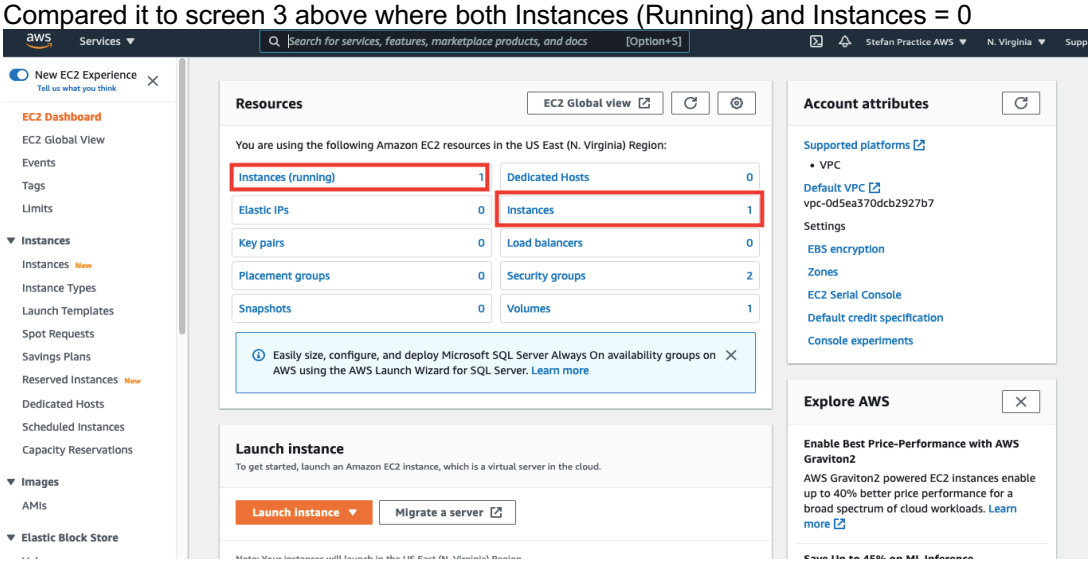


Screen 8

You have successfully launched an instance in Northern Virginia Region
Refresh the screen and go back to AWS Management Console and go to EC2 and you will see screen 9 below

- Instances (running) = 1
- Instances = 1

Compared it to screen 3 above where both Instances (Running) and Instances = 0

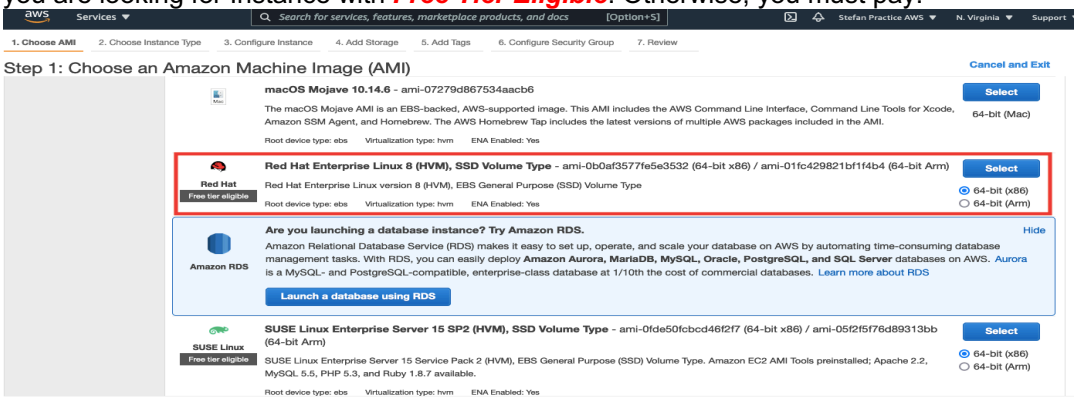


Screen 9

You have successfully launched an instance in Northern Virginia Region

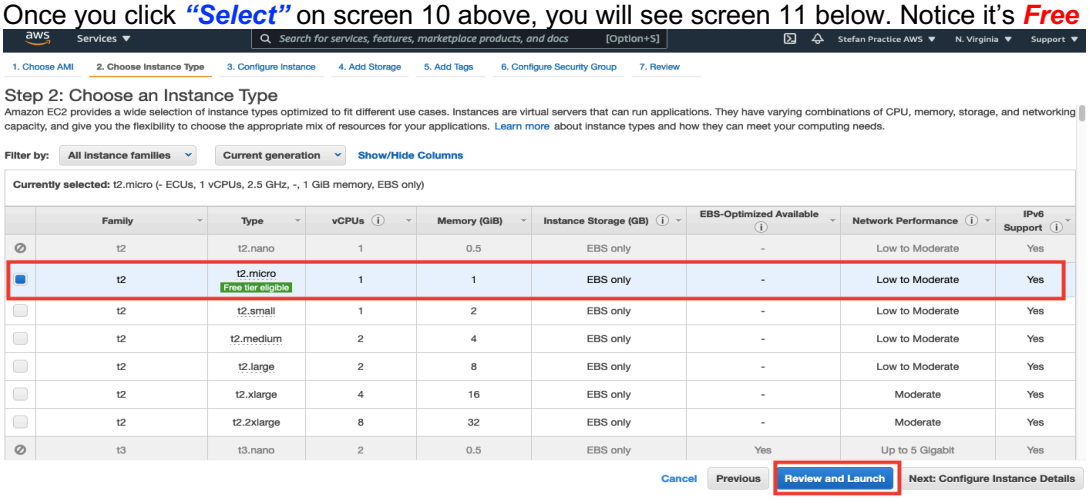
4.2 Adding an EC2 Instance

From screen 9 above, click ***"Launch Instance"*** button again and you will see screen 10 below which is similar to screen 5 above. Keep in mind that once you click ***"Launch Instance"*** button, you are automatically on Amazon Machine Image (AMI) this is because *An Amazon Machine Image (AMI) provides the information required to launch an instance.* When launching an EC2 Instance, please make sure that you are looking for Instance with ***Free Tier Eligible***. Otherwise, you must pay!



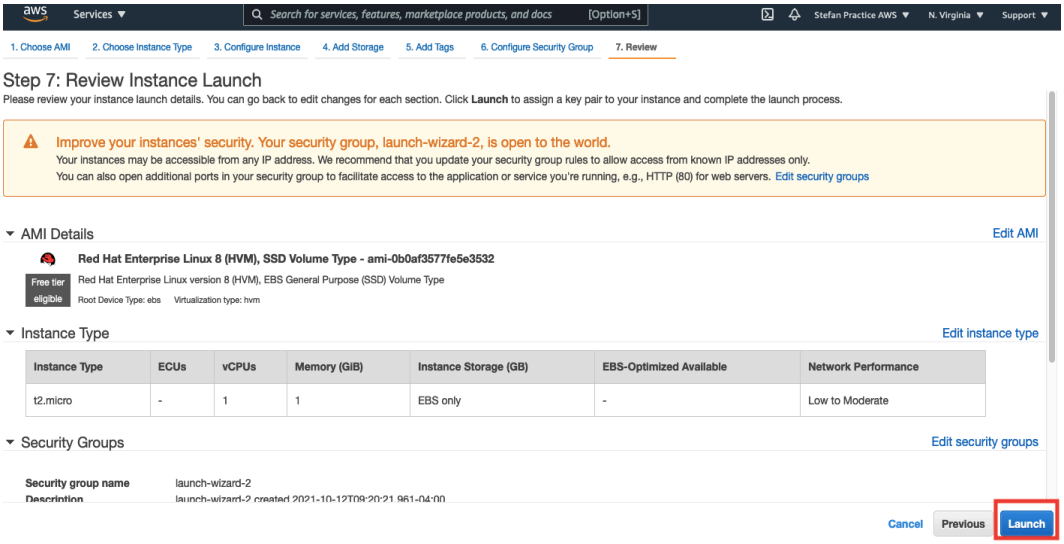
Screen 10

Once you click ***"Select"*** on screen 10 above, you will see screen 11 below. Notice it's ***Free Tier Eligible***



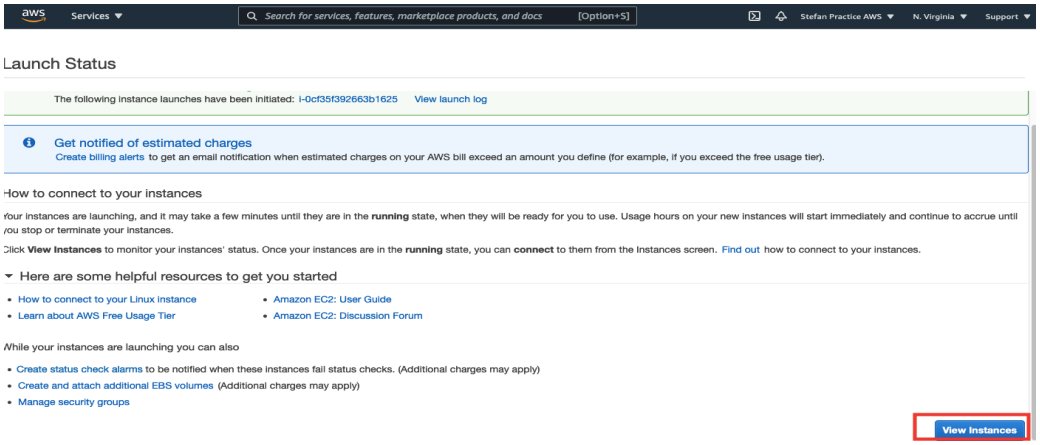
Screen 11

Click ***"Review and Launch"*** on screen 11 above, you will see screen 12 below



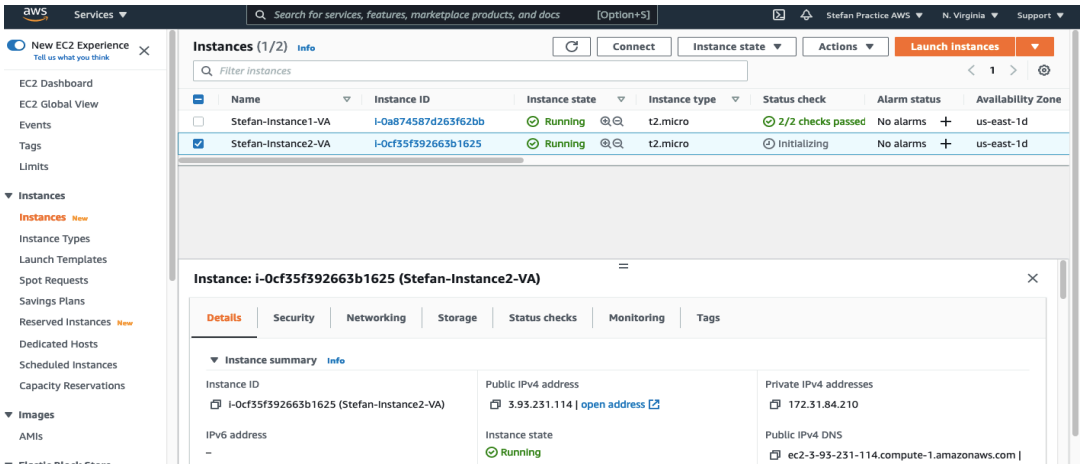
Screen 12

Click ***"Launch"*** on screen 12 above, and after acknowledgement window you will get a confirmation window of your successful launching of your new instance displayed on screen 13 below.

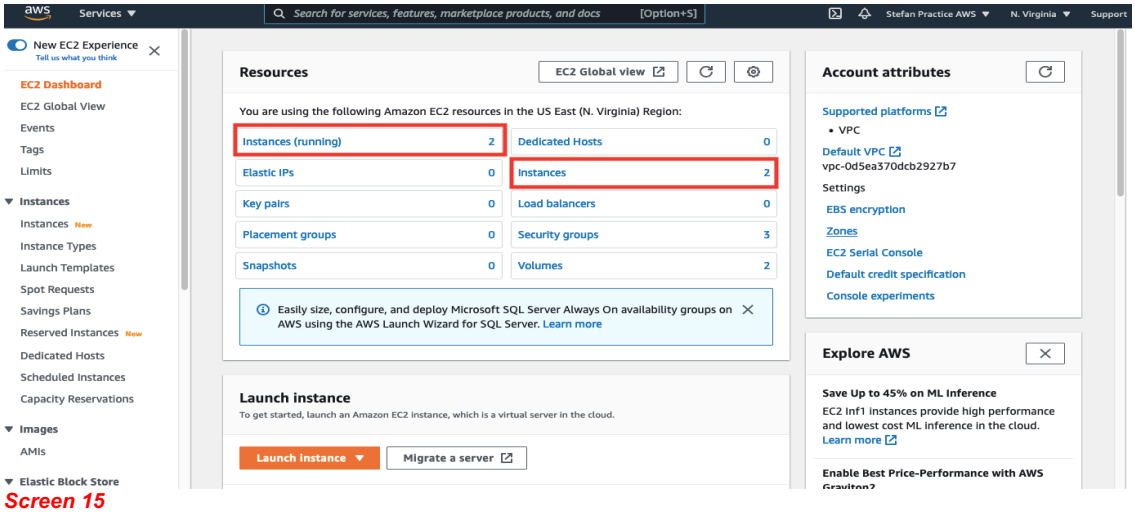


Screen 13

Simply scroll down and click ***"View Instance"*** at the lower left corner on screen 13 above, you will see screen 14 below and you will see that you are now have two instances running in Northern Virginia Region



Screen 14



Screen 15

If you refresh the EC2 Dashboard screen, you will see screen 15 above and notice the following has changed

- Instances (Running) = 2
- Instances = 2

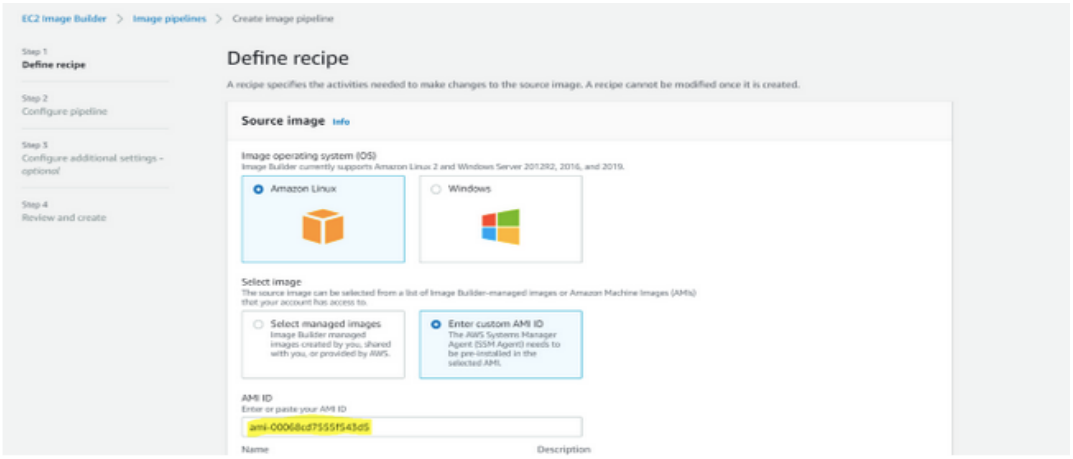
You have successfully added an EC2 Instance in a Region – Please repeat the same process if you want to add additional EC2 instances

4.3 EC2 Image Builder

EC2 Image Builder is **a fully managed AWS service** that makes it easier to automate the creation, management, and deployment of customized, secure, and up-to-date server images that are pre-installed and pre-configured with software and settings to meet specific IT standards.

EC2 Image Builder simplifies the building, testing, and deployment of Virtual Machine and container images for use on AWS or on-premises.

Keeping Virtual Machine and container images up to date can be time-consuming, resource-intensive, and error-prone. Currently, customers either manually update and snapshot VMs or have teams that build automation scripts to maintain images. Image Builder significantly reduces the effort of keeping images up-to-date and secure by providing a simple graphical interface, built-in automation, and AWS-provided security settings. With Image Builder, there are no manual steps for updating an image nor do you have to build your own automation pipeline.



Screen 16

4.4 EC2 Instance Types

AWS offers a range of EC2 instance types optimized for various purposes. Please understand the five EC2 Instance Types available out there.

4.4.1 General Purpose

General Purpose is good to use when you are not sure what to choose for your EC2 Instance Types.

4.4.2 Compute Optimized

Compute Optimized is best used for any applications that benefit from high computer power and high-performance web server activities.

4.4.3 Memory Optimized

Memory Optimized is the perfect solution for running custom workload and it delivers fast performance for your workloads that process large data sets in memory.

4.4.4 Accelerated Optimized

Accelerated Optimized is used for software running on CPU, graphic processing and other GPU uses.

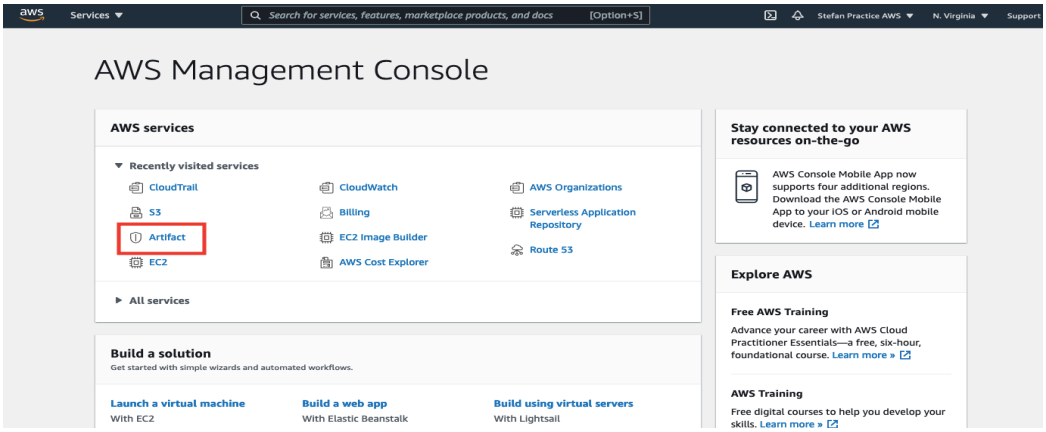
4.4.5 Storage Optimized

Storage Optimized can be used when you require high sequential read/write access to a very large dataset such as Hadoop.

5 AWS Security

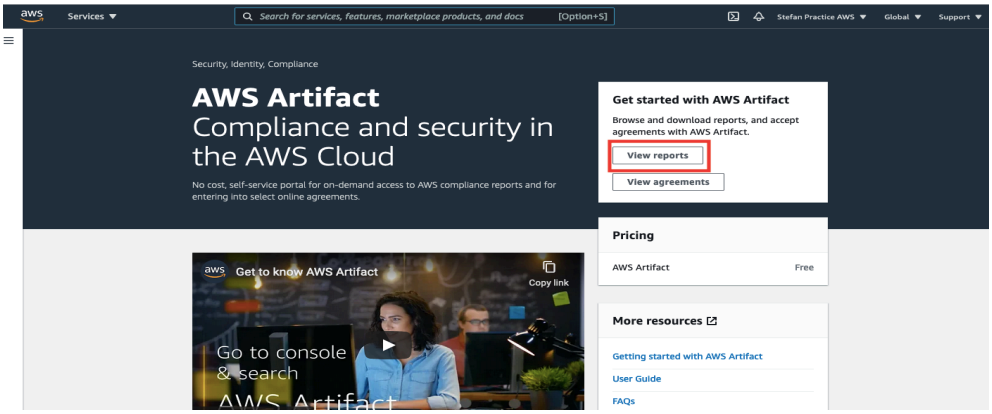
5.1 AWS Artifact

AWS Artifact provides on-demand access to AWS Security & Compliance reports & online agreement. *AWS Artifact is FREE.* Go to AWS Management Console displayed on screen below



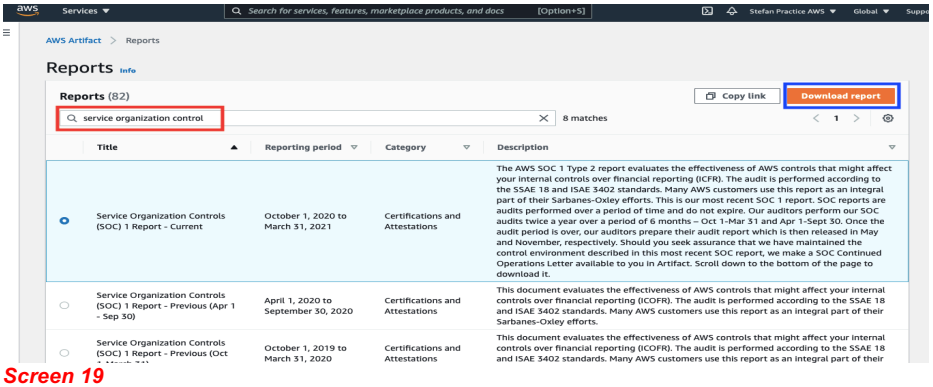
Screen 17

Click ***"Artifact"*** from screen above and you will see screen below



Screen 18

Click ***"View Reports"*** from screen above and you will see screen below

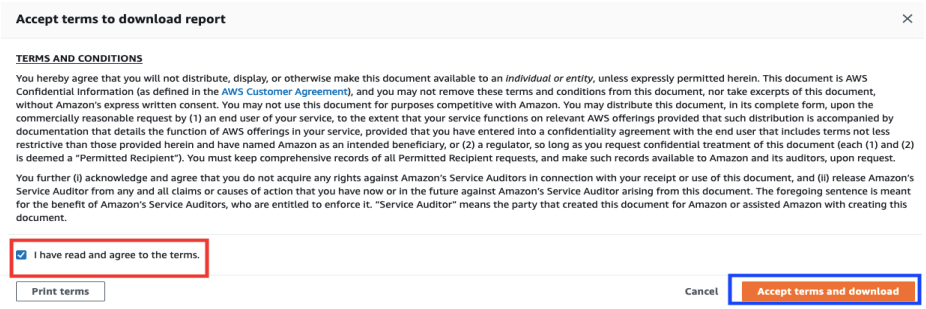


Screen 19

Here, you can see all the reports available in AWS Artifact. We all know that AWS Artifact stores the following reports

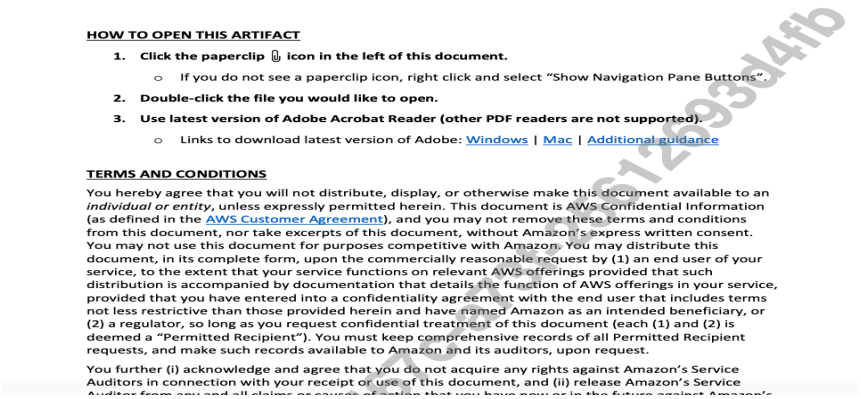
- Service Organization Control (SOC) Report
- Payment Card Industry (PCI) Report

OK, let's search for Service Organization Control (SOC) Report. I typed ***"Service Organization Control"*** on screen above and I can see various SOC Reports being displayed on screen above.
Select the SOC report that you want and click ***"Download Report"*** showed on screen above. You will see screen below



Screen 20

Click the agreement's radio button on screen 20 and click ***"Accept terms and download"*** and you will see screen below, the actual SOC report downloaded



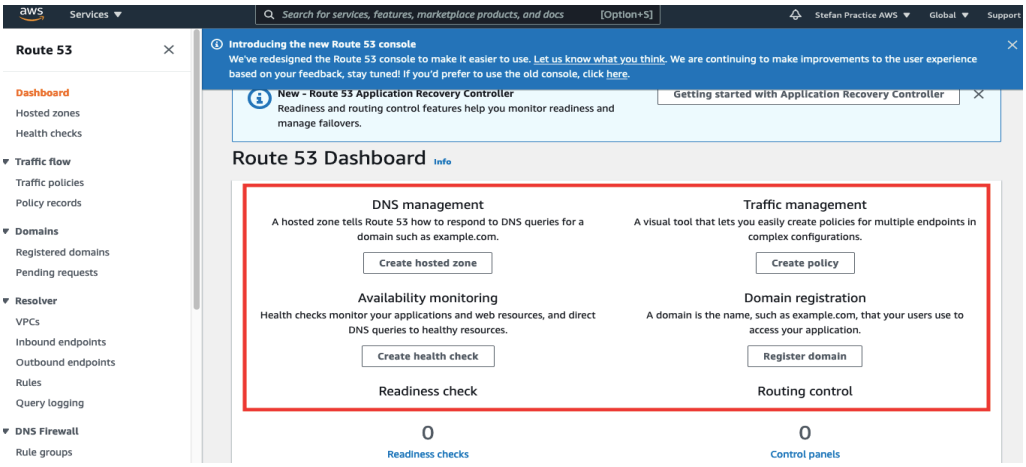
Screen 21

You have successfully downloaded ***Service Organization Control (SOC) Report*** from AWS Artifact

5.2 Amazon Route 53

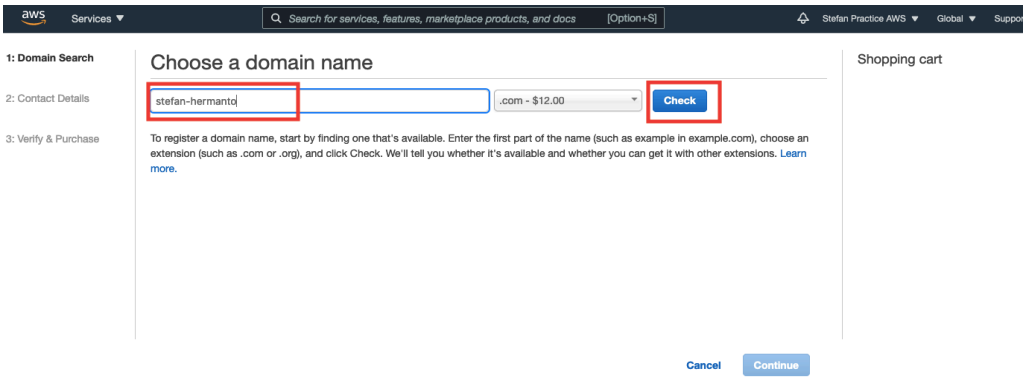
Type ***"Amazon Route 53"*** from AWS Management Console and you will see screen below.
As you can see, Route 53 can be used for the following activities:

- DNS Management
- Health Check Monitoring Tool
- Traffic Management
- Domain Registration



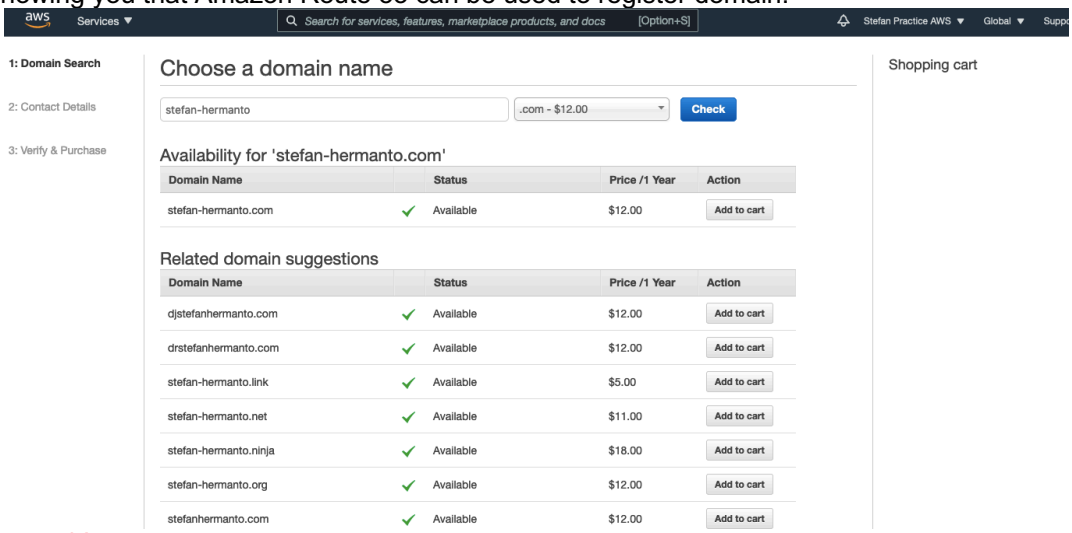
Screen 22

Let's say for example you click ***"Register Domain"*** from screen 21 above, you will be able to see screen below



Screen 23

Let's say, you type your name ***"Stefan-Hermanto"*** as it displayed on screen above and click ***"Check"*** button on screen above, you will be able to see screen below. As you can see from Screen below that domain is available for sale. If you click ***"Add to Cart"*** your credit card will be charged. This exercise is showing you that Amazon Route 53 can be used to register domain.



Screen 24

Please also note that Route 53 also can be used for various routing:

1. ***Simple Routing*** – Route traffic to single resource
2. ***Weighted Routing*** – Route traffic to multiple resources with a single domain name
3. ***Latency Routing*** – Route traffic to region that provides the BEST latency – Fast experience, cost effective, reliable
4. ***Failover Routing*** – Active/Passive failover
5. ***Geolocation Routing*** – localize your content – route traffic based on the location of our users
6. ***Geoproximity Routing*** – route traffic based on the location of your resources – shift traffic from resources in 1 location to resources in another location
7. ***Mutivalue Answer Routing*** – Respond to DNS queries with up to 8 healthy records selected random

5.4 AWS Trusted Advisor

It provides recommendations that help you follow AWS best practices.
It checks identify ways to optimize your AWS infrastructure, improve security and performance, reduce costs, and monitor service quotas
It also provides most common security misconfigurations such as:

1. Allowing public access to S3 bucket

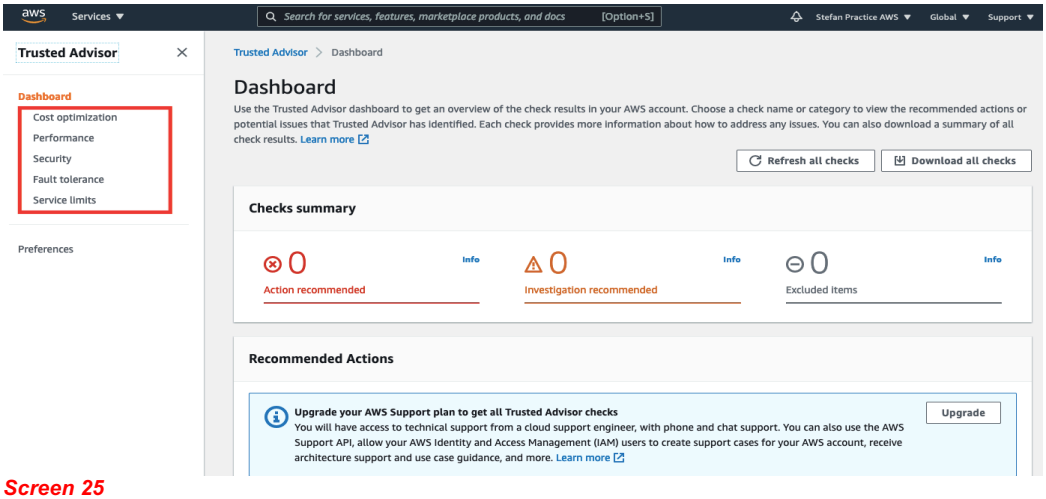
2. Not turning on user activity logging (AWS CloudTrail)
3. Not using MFA on your root account

Furthermore, the following can be used to identify ALL EC2 instances that are **UNDER UTILIZED**:

- AWS Cost Explorer
- AWS Trusted Advisor

From AWS Management Console Type “AWS Trusted Advisor” and you will see screen 25 below. Please note on the left side of the screen 25, it is stating the 5 pillars best practices of AWS Trusted Advisor:

- Cost Optimization
- Performance
- Security
- Fault-Tolerant
- Service Limits

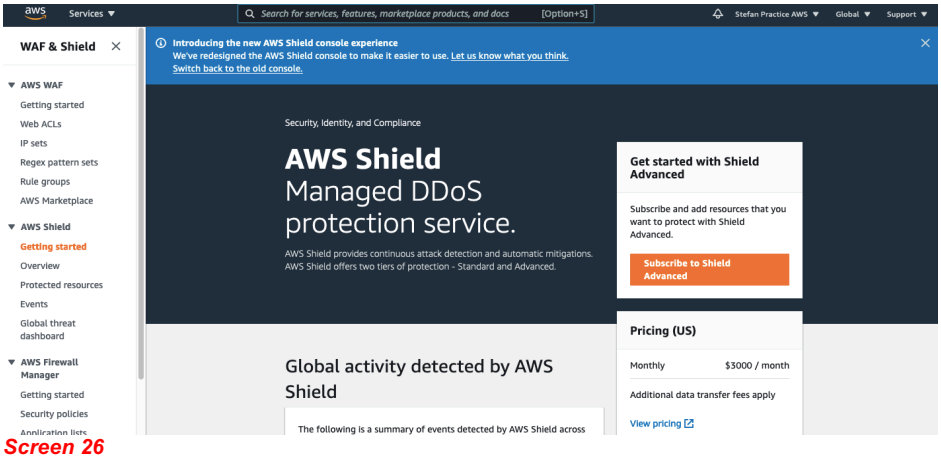


Screen 25

5.5 AWS Shield Standard

Please be very careful, when you are at AWS Shield Standard screen, you are being asked to upgrade to AWS Shield Advanced which is not free

WARNING: Please DO NOT accidently click Upgrade to AWS Shield Advanced. Your Credit Card will be charged for $3,000 monthly



Screen 26

The main purpose of AWS Shield Standard as well as AWS Shield Advanced is to mitigate Distributed Denial of Service (DD0S) Attack

Please understand the differences between standard vs. advanced

AWS Shield Standard (AWS)	*AWS Shield Advanced (Cust.)*
Free – no extra cost *Protects your APP from Layer 3 (Network) & Layer 4 (Transport)*	*Additional Cost $3,000 monthly* *Protects your APP from Layer 3 (Network), Layer 4 (Transport) & Layer 7 (Application)* *Minimum 1 year commitment*
Works very well with: *1. AWS CloudFront* *2. AWS Route 53*	*Provides expanded DDoS attack protection from web APP running on* *1. EC2* *2. ELB* *3. Amazon CloudFront* *4. Amazon Route 53* *5. AWS Global Accelerator*

Screen 27

5.6 AWS Inspector

AWS Inspector automates security assessments and inspects running OS against known vulnerabilities. It also analyses against unintended network accessibility.

Amazon Inspector helps you to identify *security vulnerabilities as well as deviations from security best practices* in applications, both before they are deployed, and while they are running in a production environment. This helps improve the overall security posture of your applications deployed on AWS.

5.7 AWS Key Management Services (KMS)

AWS Key Management Service (KMS) makes it easy for you to create and manage cryptographic keys and control their use across a wide range of AWS services and in your applications. AWS KMS is a secure and resilient service that uses hardware security modules that have been validated under FIPS 140-2, or are in the process of being validated, to protect your keys. AWS KMS is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

5.8 AWS Cloud Hardware Security Model (HSM)

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs. CloudHSM offers you the flexibility to integrate with your applications using industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.

5.8.1 AWS KMS vs. AWS Cloud HSM

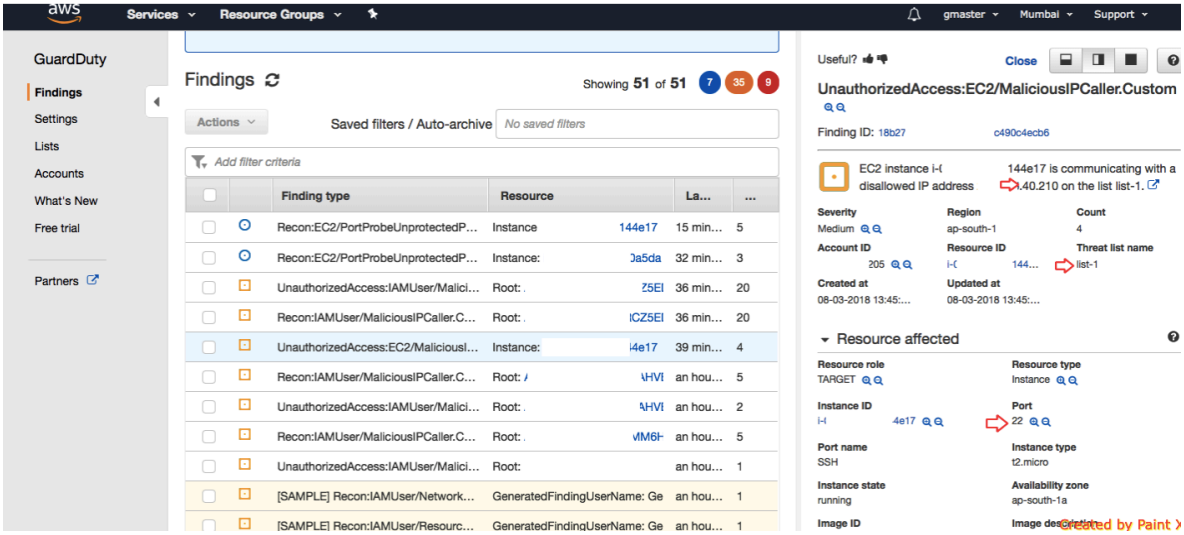
AWS Key Management Services (KMS)	*AWS Cloud Hardware Security Model (HSM)*
Create keys and control encryption multi-tenant	*Dedicated hardware*
Cost efficient	*It gives you your own hardware module*
Encryption module – shared with other AWS customers	*Ensure your keys were isolated on their own encryption module*

Screen 28

5.9 Amazon GuardDuty

Amazon GuardDuty is a threat detection service that continuously monitors your AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

It is a threat detection service that *continuously monitor malicious activities* behavior to protect AWS accounts, workloads, and data storage in Amazon S3



Screen 29

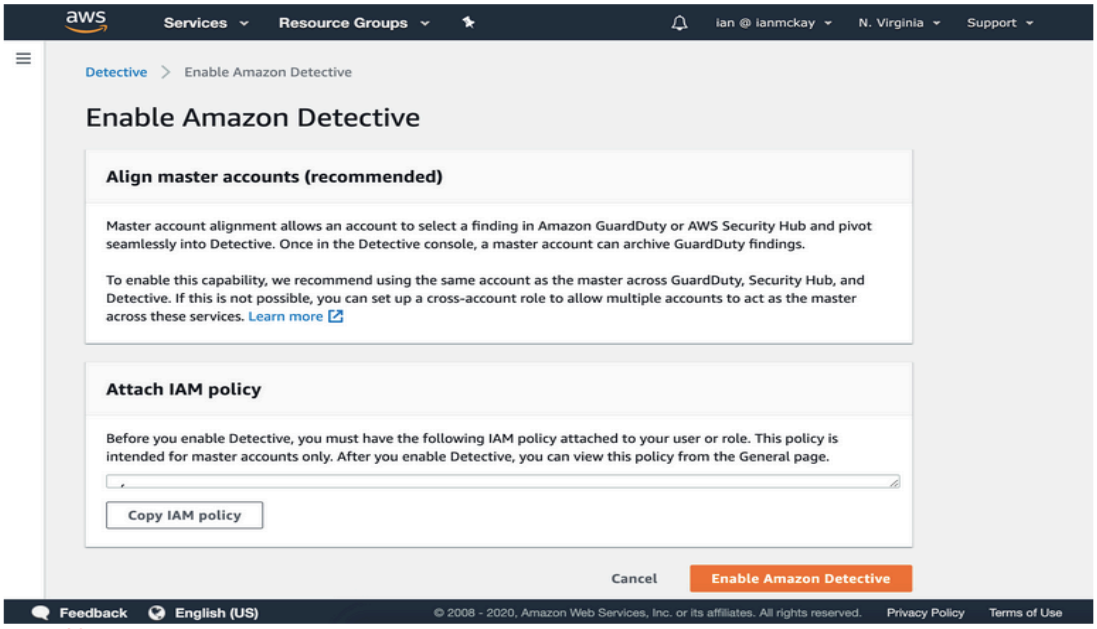
5.10 Amazon Detective

Amazon Detective analyzes, investigates, and quickly identifies the root cause of potential security issues or suspicious activity.

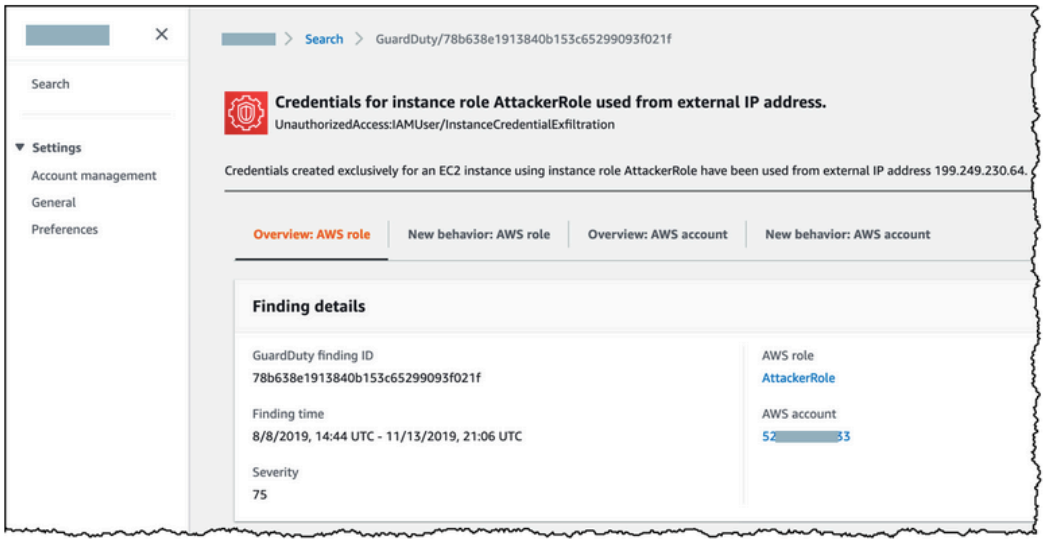
You need to have Amazon GuardDuty before using Amazon Detective.

The following data sources are used by Amazon Detective to analyze event and identify potential security issue:

- AWS CloudTrails Logs
- Amazon VPC Flow Logs
- Amazon GuardDuty Findings



Screen 30



Screen 31

5.11 AWS Web Application Firewall (WAF)

AWS WAF is **a web application firewall** that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.

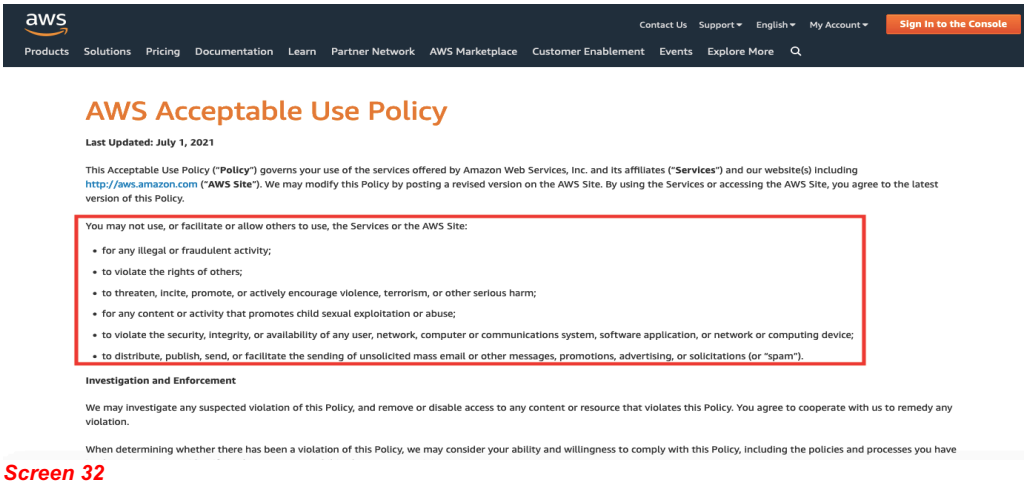
AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to CloudFront, and lets you control access to your content.

AWS WAF is used to perform the following:

- Helps protect a company's web applications by inspecting and filtering traffic between each web application and the internet.
- It can help defend web APP from attacks such as cross-site request forgery (CSRF), cross-site-scripting (XSS), file inclusion & SQL injection.
- Layer 7 (Application) protection

5.12 AWS Acceptable User Policy

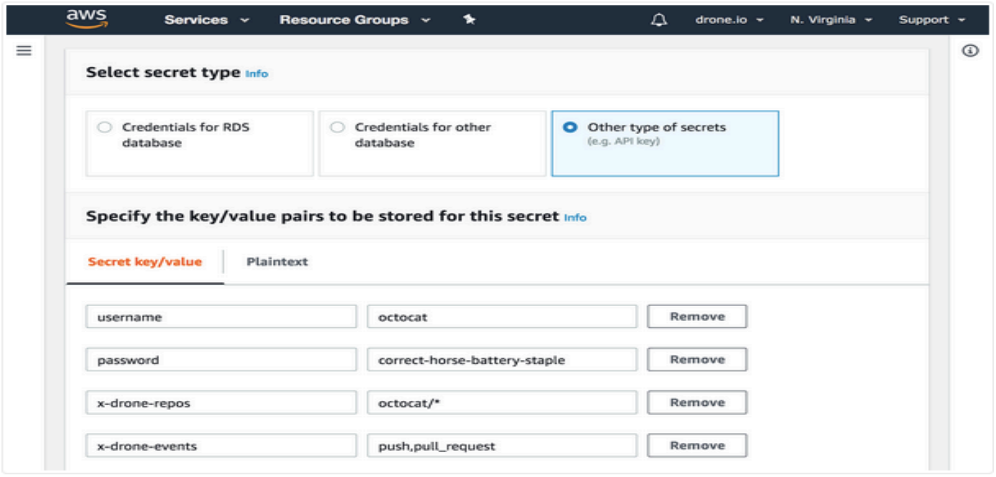
AWS Acceptable User Policy describes prohibited uses of web services offered by AWS. You will see something like this below:



Screen 32

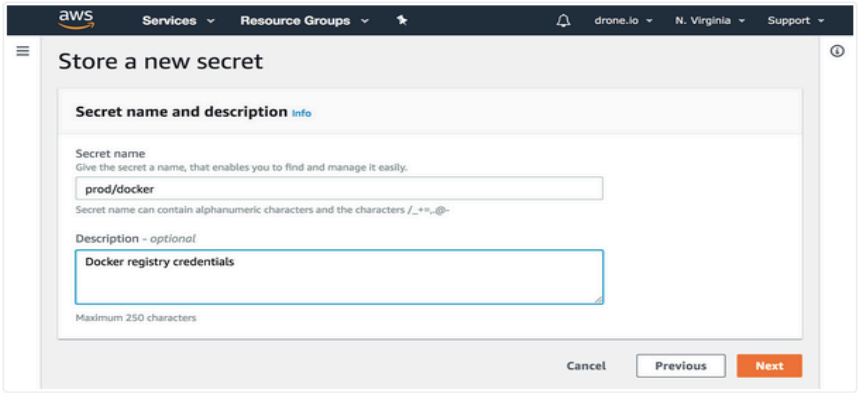
5.13 AWS Secret Manager

AWS Secret Manager retrieves database credential, API keys and other secrets. It protects secrets needed to access your applications, service, and IT resources.



Screen 33

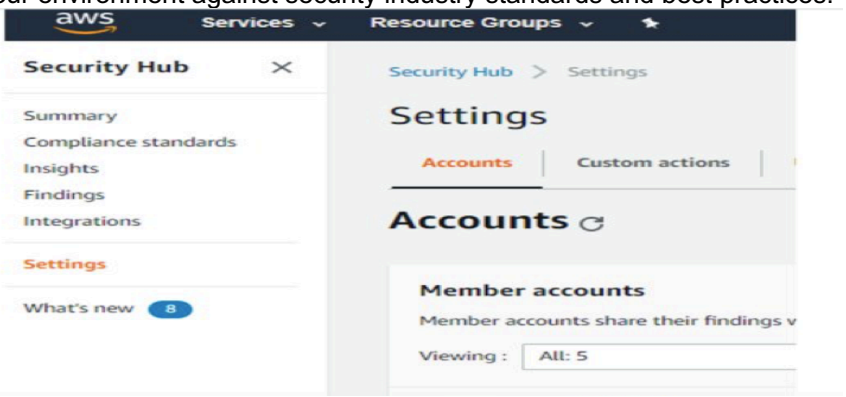
Using AWS Secrets Manager, you can help secure secrets by encrypting them with encryption keys that you manage using AWS Key Management Service (KMS).



Screen 34

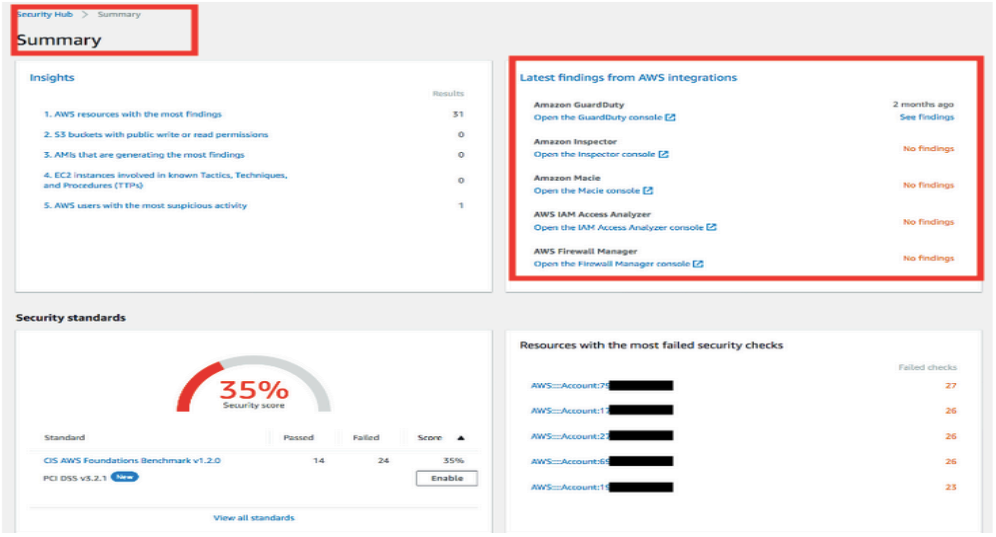
5.14 AWS Security Hub

AWS Security Hub provides you with a *comprehensive view of your security state in AWS* and helps you to check your environment against security industry standards and best practices.



Screen 35

AWS Security Hub collects data from Guard Duty, Inspector, Config, Macie, & other connected partner services to provide a single view of the resources in your account and their associated compliance with the configured rules.



Screen 36

In other words, AWS Security Hub collects security data from across AWS accounts, services, and supported third-party partner products and helps you to analyze your security trends and identify the highest priority security issues.

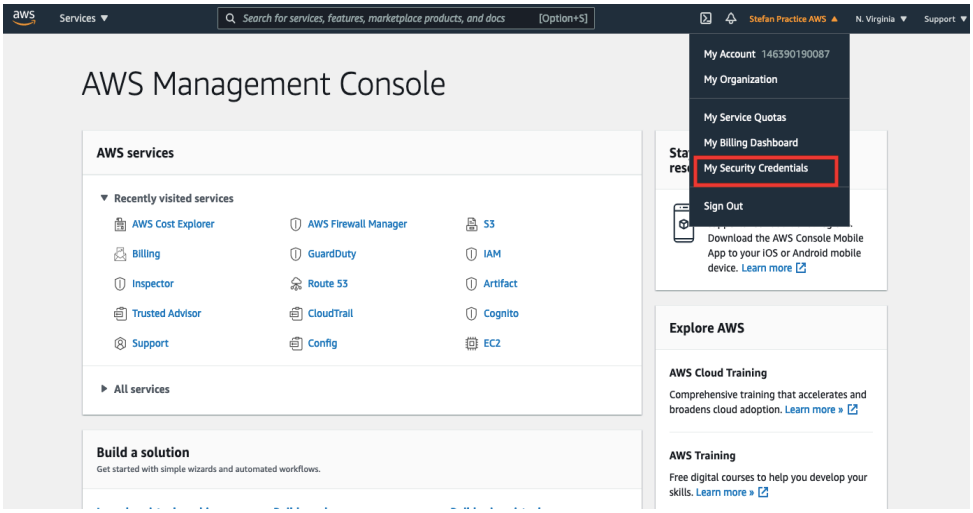
Please refer to screen 32 below, the security hub collects information from the following resources

- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- AWS IAM Access Analyzer
- AWS Firewall Manager

6 MFA and IAM

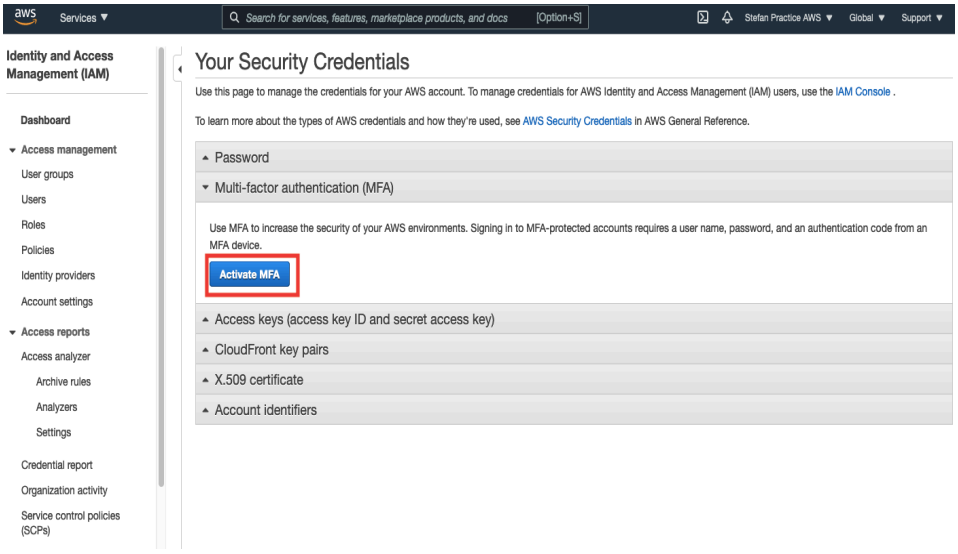
6.1 Multi Factor Authentication (MFA)

For increased security, you should use multi-factor authentication (MFA) to help protect your AWS resources. You can enable MFA for IAM users or the AWS account root user. When you enable MFA for the root user, it affects only the root user credentials. IAM users in the account are distinct identities with their own credentials, and each identity has its own MFA configuration. Go to AWS Management Console and go to ***My Security Credentials*** displayed on screen below



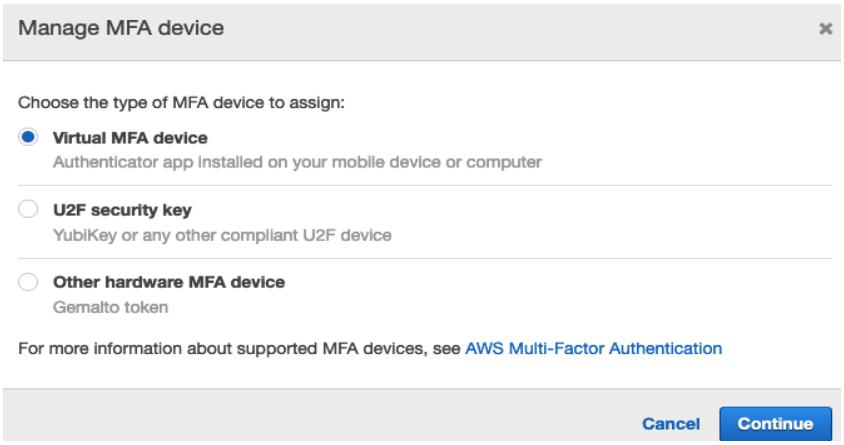
Screen 37

Once you click ***My Security Credentials*** displayed on screen 37 above, you will see screen 38 below



Screen 38

Click ***Activate MFA*** and you will see screen below



Screen 39

Keep in mind there are several MFA types;

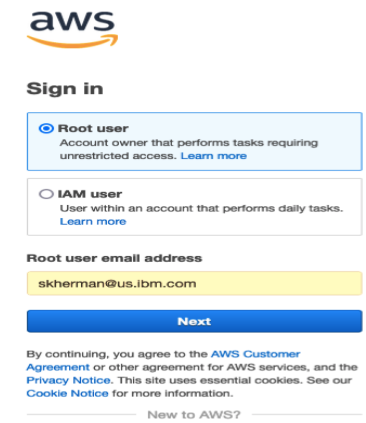
- ***Virtual MFA Device*** – software application runs on a phone emulates a physical device generates six digits numeric code
- ***U2F Security Key*** – device you plug into USB
- ***Hardware MFA device*** – RSA Token
- ***SMS Text Based MFA*** – AWS send six digits code by SMS text
- ***Soft Token MFA Device*** – software basd security token that generates single use login PIN

Once, you have entered your MFA code and you are to login into AWS successfully

Do not use the AWS account root user for any task where it's not required. *Instead, create a new IAM user for each person that requires administrator access.*

Then make those users administrators by placing the users into an "Administrators" group to which you attach the AdministratorAccess managed policy.

Please refer to screen 36 below.



Screen 40

If you don't already have an access key for your AWS account root user, don't create one unless you need to. If you do have an access key for your AWS account root user, delete it.

Never share your AWS account root user password or access keys with anyone. Use a strong password to help protect account-level access to the AWS Management Console.

Enable AWS multi-factor authentication (MFA) on your AWS account root user account.

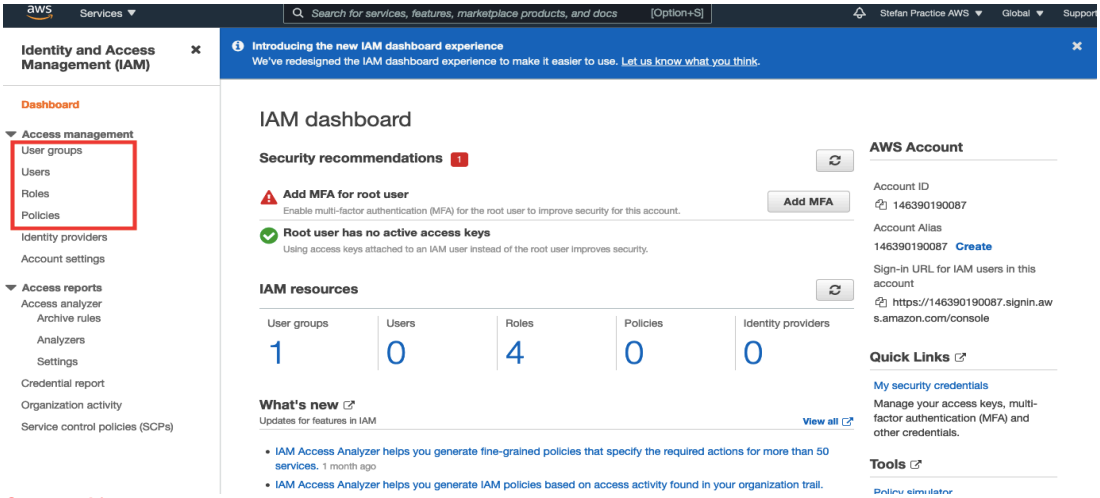
6.2 Identity and Access Management (IAM)

It's to manage account privileges and it is essential for implementing security of resources in AWS Cloud.

Best Practices IAM Service

- Enable MFA for **ALL** Users
- Rotate credentials regularly

From AWS Management Console type ***"IAM"*** and you will see screen below which is the landing screen for Identity and Access Management



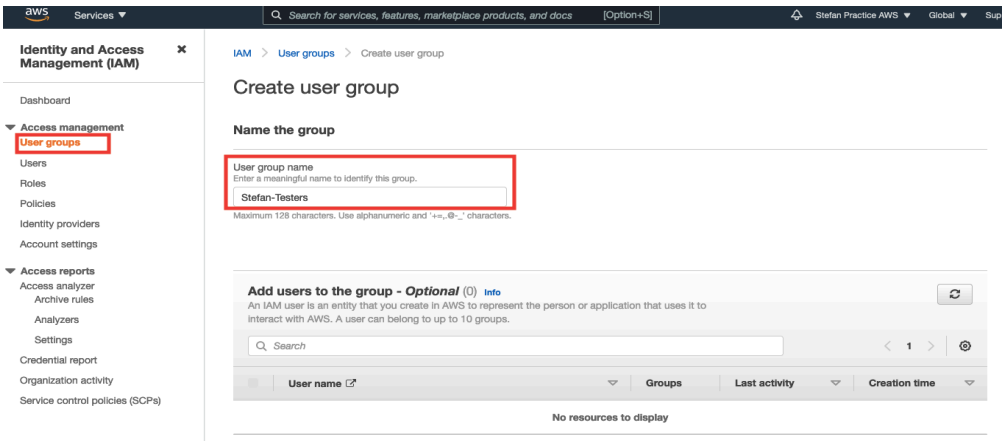
Screen 41

As you can see from screen above you can see the 4 concepts of IAM mentioned here

- **Groups:** *Collection of users with common theme i.e, Developers, Testers, Intern Students, etc.*
- **Users:** *Specific individuals, can receive personal login. It gives people the ability to login into AWS. It has name, password, access key id, secret access key*
- **Roles:** *Collections of policies, NOT typically tie to individual user. DOES NOT have any credentials (password or access key) associated with it*
- **Policies:** *Policy can be attached to users, groups or roles. Allow or Deny*

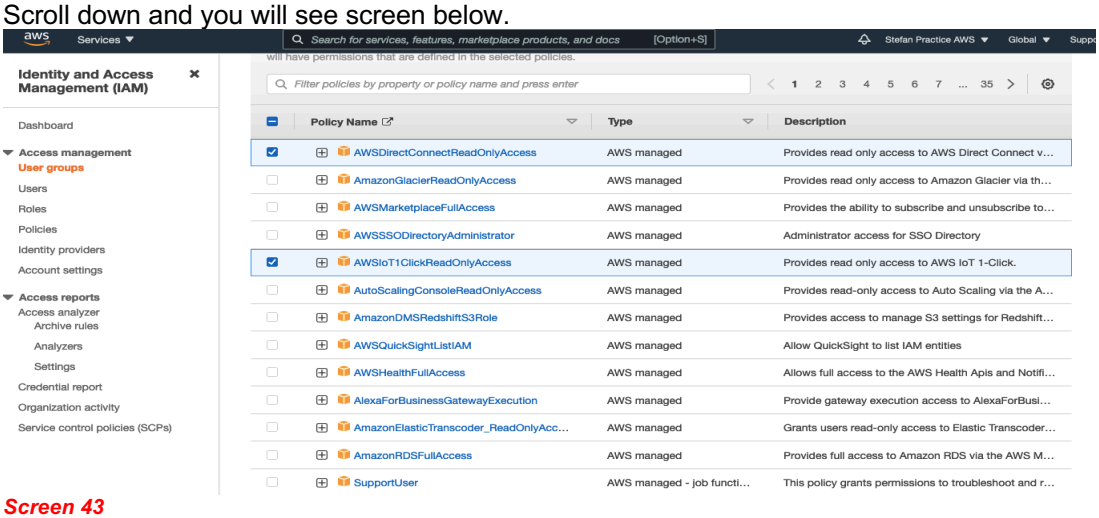
6.2.1 IAM Groups

Collection of users with common themes i.e., Developers, Testers, Student Interns, etc. From IAM Dashboard click User Groups and you will see screen below



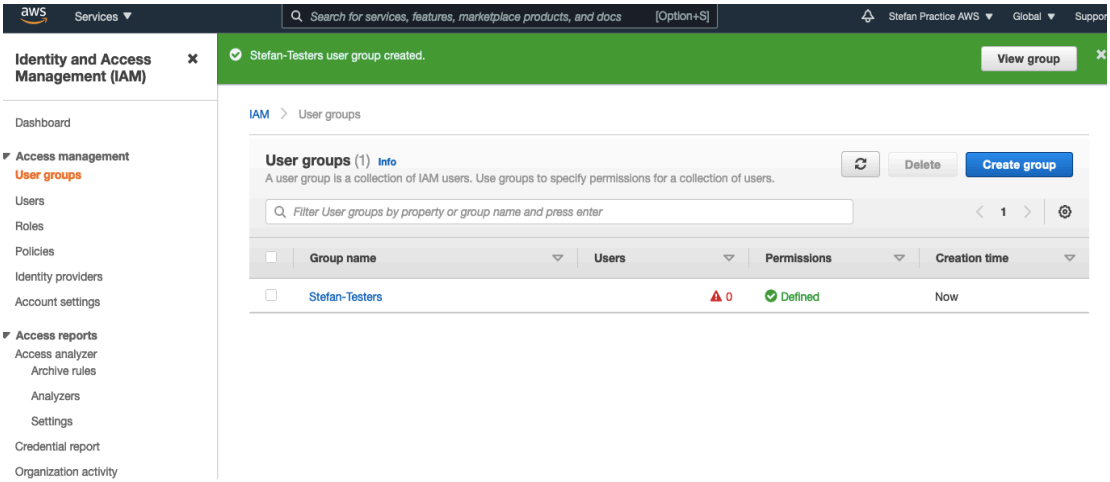
Screen 42

Give a name for your IAM Group for example ***"Stefan-Testers"*** displayed on screen 38 above Scroll down and you will see screen below.



Screen 43

On screen above, select whatever policies you would like to attach to your IAM Group called ***Stefan-Testers***. Let's say you selected two policies for your IAM Group – ***Stefan-Testers*** as it displayed on screen above. Scroll down and click ***"Create Group"*** and after that you will be able to see screen below



Screen 44

On screen above, click ***Stefan-Testers*** and you will be able to see screen below. Notice under ***Permissions*** tab you will see two policies attached here. This is basically what you've selected above when creating this IAM Group – when you selected the policies for IAM Group.

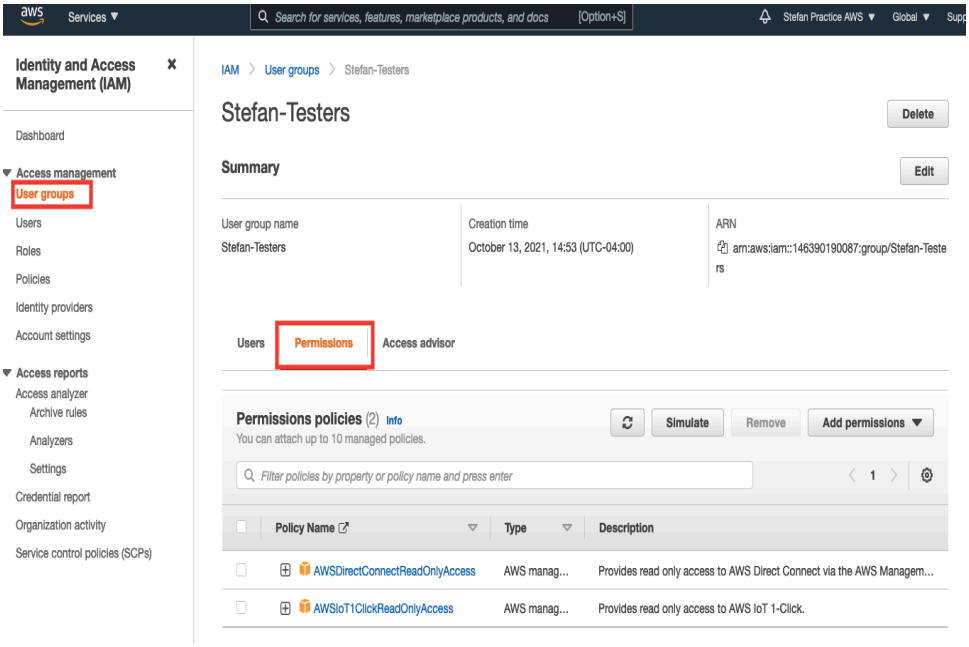
IAM Group ***Stefan-Testers*** has been created successfully. Please repeat this step if you want to create another IAM Group.

6.2.2 IAM Access Advisor

IAM Access Advisor is to review permission granted. You can also use IAM Access Advisor to identify unnecessary permissions so that you can revise your IAM Policy Accordingly.

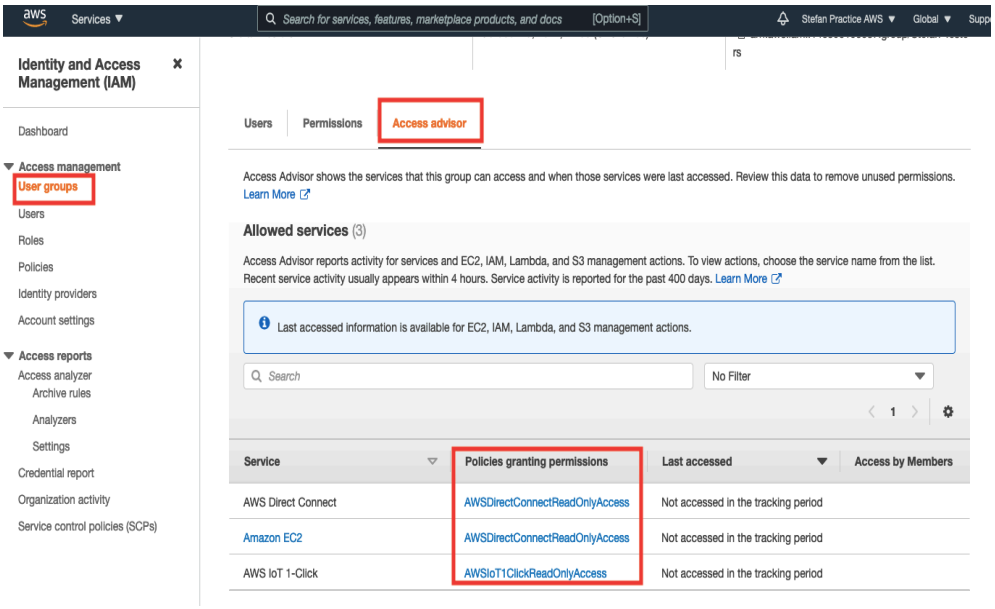
You can easily review the permissions granted to users and if necessary, remove permissions on IAM Policy accordingly.

On screen above, click ***Stefan-Testers*** and you will be able to see screen below. Notice under ***Permissions*** tab you will see two policies attached here. This is basically what you've selected above when creating this IAM Group – when you selected the policies for IAM Group.



Screen 45

Click the next tab which is ***Access Advisor*** to review permission granted and you will see screen 46 below



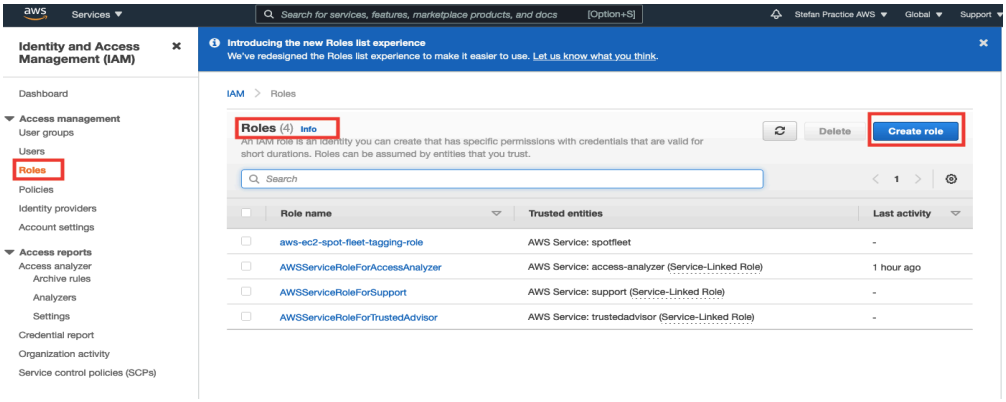
Screen 46

Here on screen 46, you can easily review permission granted and identify unnecessary permissions so that you can revise your IAM Policy accordingly.

6.2.3 IAM Roles

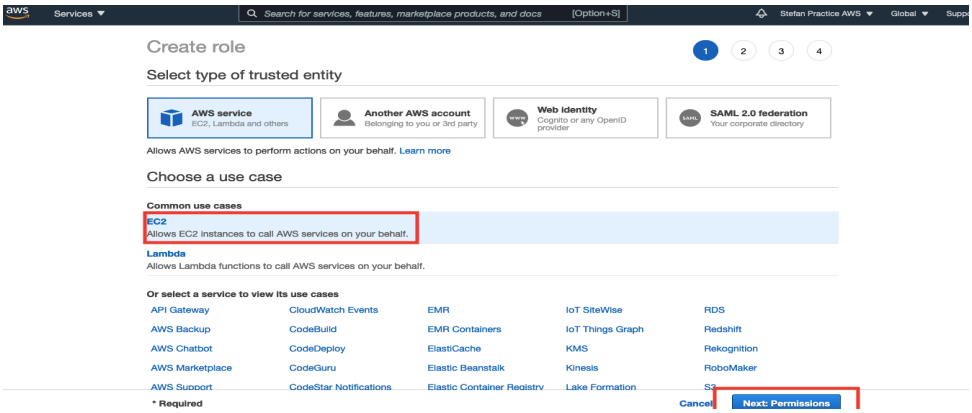
IAM Roles – collection of policies and it's not typically tie to individual user, and it does not have any credentials (password or access key) associated with it.

From IAM Dashboard click ***Roles*** and you will see screen 47 below.



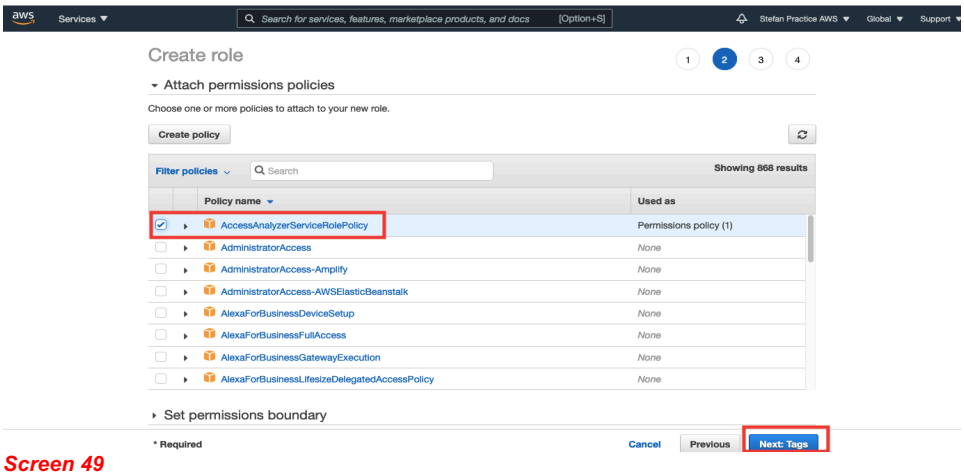
Screen 47

Here you see that currently there are 4 Roles available. You can create your own roles if you want to. Click ***Create Role*** and you will see screen below.



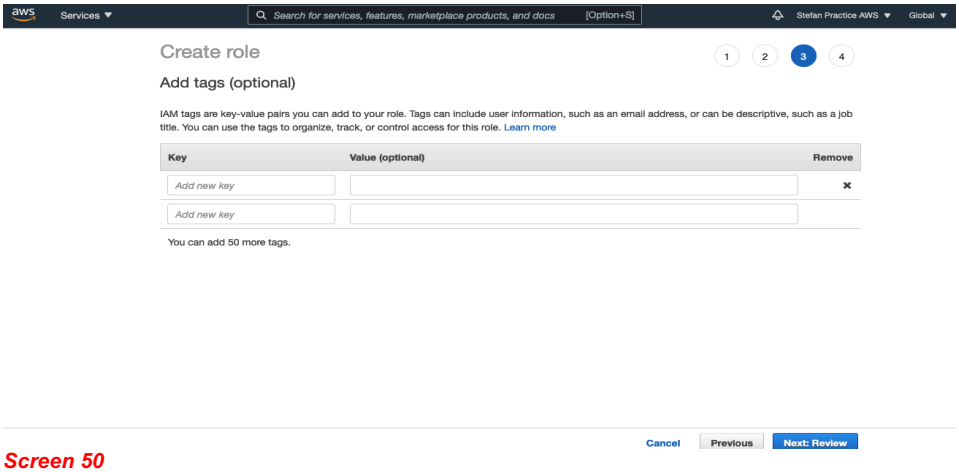
Screen 48

Select use cases, in this case – select EC2 and click ***Next Permissions*** on the lower right side of screen above and you will see screen 49 below



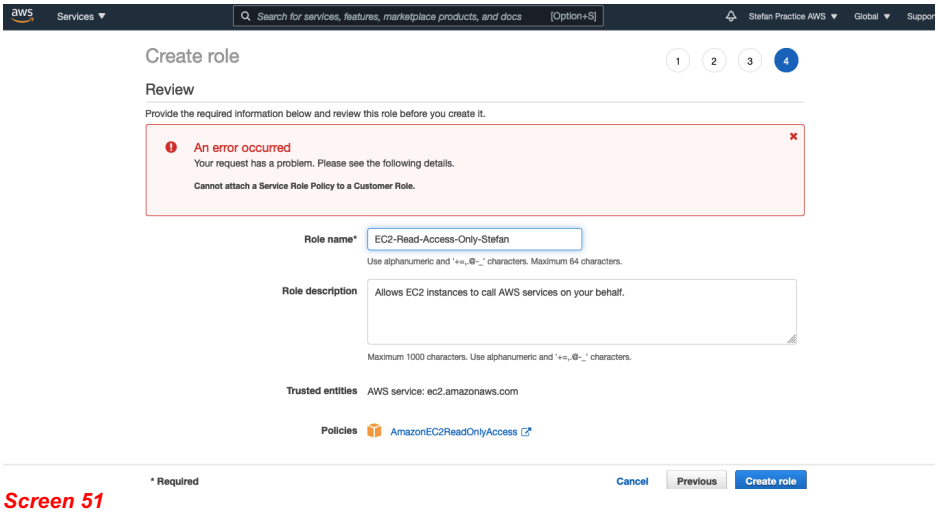
Screen 49

Select whatever policy/policies you want to attach to your role and when you're done click ***Next Tag*** and you will see screen below



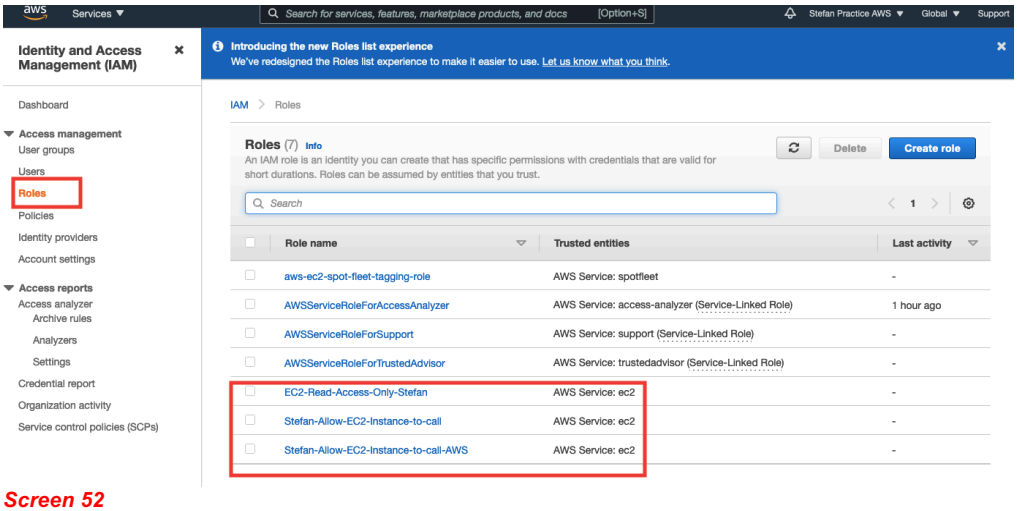
Screen 50

Tag is optional, you can just click ***Next: Review*** button and you will see screen below



Screen 51

Click ***Create Role*** button and you will see screen below

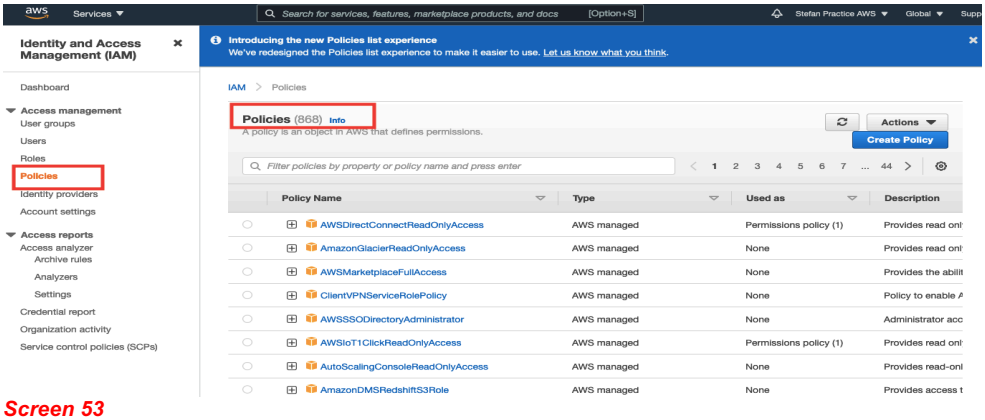


Screen 52

You can create multiple roles like shown on screen 52 above. Three additional roles have been successfully created in IAM Role.

6.2.4 IAM Policies

Allow or Deny. Policy can be attached to users, groups or roles.
From IAM Dashboard click ***Policies*** and you will see screen below. As you can see, currently there are 868 policies available to use. You can create additional policy/policies simply by clicking ***Create Policy*** button below and follow instruction.



Screen 53

You can easily review the permissions granted to users and if necessary, remove permissions on IAM Policy accordingly.

6.2.5 IAM Users

It's s specific individuals, it can receive personal login. IAM USERS give people the ability to sign into AWS. IAM USERS – Name, password, access key ID – secret access key. In other words, Access Key ID & Secret Access Key are tied to IAM USERS.

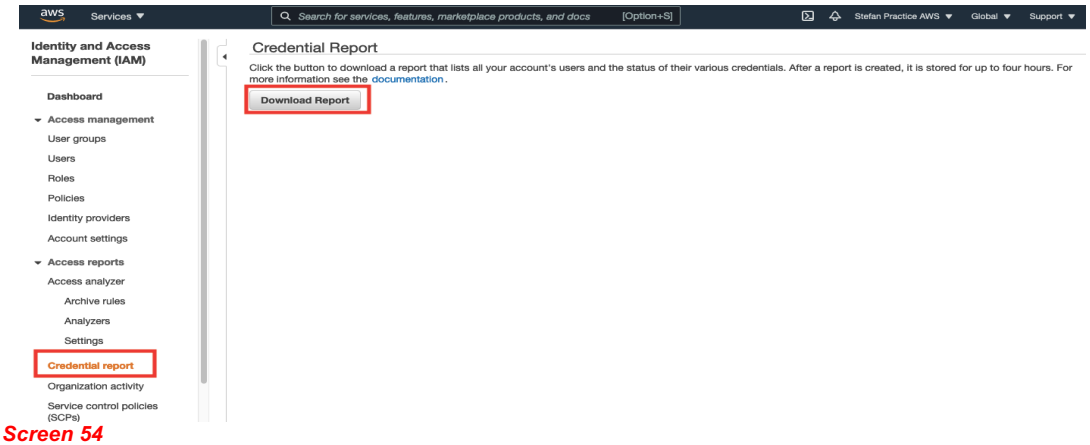
6.3 IAM Credential Report

You can use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation.

It provides lists in your account and the status of their various account aspects such as password, access keys, and MFA devices.

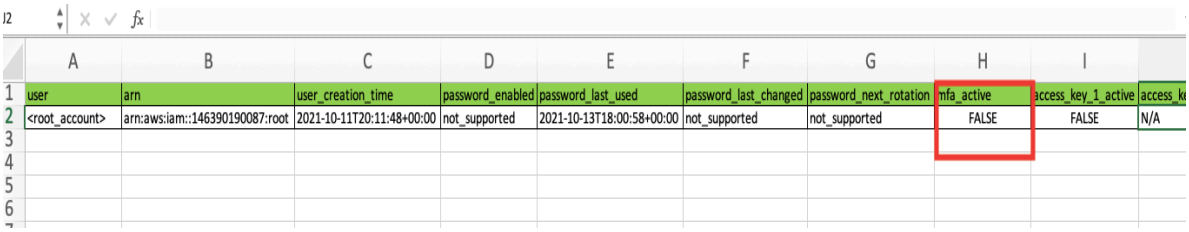
To view the status of all user *credentials*, including passwords, access keys, and multi-factor authentication (MFA) devices.

Go to AWS Management Console and type ***"IAM"*** and you will see screen below



Screen 54

Click ***"Download Report"*** from screen 50 above, you can have this excel downloaded for you which is an example of Credential Report



	A	B	C	D	E	F	G	H	I	
1	user	arn	user_creation_time	password_enabled	password_last_used	password_last_changed	password_next_rotation	mfa_active	access_key_1_active	access_k
2	<root_account>	arn:aws:iam::146390190087:root	2021-10-11T20:11:48+00:00	not_supported	2021-10-13T18:00:58+00:00	not_supported	not_supported	FALSE	FALSE	N/A
3										
4										
5										
6										

Screen 55

You can see that this is the information about your root account. Notice in column H that ***MFA_Active = FALSE*** which means that you have not activated your MFA yet. You can also write your own SQL to generate IAM Credential Reports if you need to find information such as.

6.3.1 Has the root user been access recently?

```
> select
   user_name,
   password_last_used,
   age(date(current timestamp), date(password last used)) as pw last used
   from
   aws_iam_credential_report
   where
   user_name = '<root_account>';

   +----------------+---------------------+-----------------------+
   | user_name      | password_last_used  | pw_last_used          |
   +----------------+---------------------+-----------------------+
   | <root_account> | 2019-07-17 04:49:39 | 1 year 6 mons 23 days |
   +----------------+---------------------+-----------------------+
```

6.3.2 Does the root account have MFA enabled?

```
> select
   user_name,
   mfa active
   from
   aws_iam_credential_report
   where
   user_name = '<root_account>';

   +----------------+------------+
   | user_name      | mfa_active |
   +----------------+------------+
   | <root_account> | true       |
   +----------------+------------+
```

6.3.3 Does the root account have access keys enabled?

```
> select
   user_name,
    access_key_1_active,
    access_key_2_active
   from
   aws_iam_credential_report
   where
   user_name = '<root_account>';

   +----------------+---------------------+---------------------+
   | user_name      | access_key_1_active | access_key_2_active |
   +----------------+---------------------+---------------------+
   | <root_account> | false               | false               |
   +----------------+---------------------+---------------------+
```

6.3.4 Inactive users – never logged in for over 90 days

```
> select
   user_name,
   password_enabled,
   password_last_used,
   age(date(current_timestamp), date(password_last_used)) as last_used_age
   from
   aws_iam_credential_report
   where
   user_name != '<root_account>'
   and password_enabled
   and (
   password_last_used is null
   or (date(current_timestamp) - date(password_last_used)) > 90
   );
```

```
+----------------+------------------+---------------------+-----------------------+
| user_name      | password_enabled | password_last_used  | pw_last_used          |
+----------------+------------------+---------------------+-----------------------+
| dwight_schrute | true             |                     |                       |
| kelly_kapoor   | true             |                     |                       |
| ryan_howard    | true             |                     |                       |
| pam_beesly     | true             | 2019-07-17 04:49:39 | 1 year 6 mons 23 days |
+----------------+------------------+---------------------+-----------------------+
```

6.3.5 Is MFA enabled for all Users? Users that are not using MFA

```
> select
  user_name,
  mfa_active
  from
  aws_iam_credential_report
  where
  not mfa_active;

  +----------------+------------+
  | user_name      | mfa_active |
  +----------------+------------+
  | darryl_philbin | false      |
  | ryan_howard    | false      |
  | dwight_schrute | false      |
  | kelly_kapoor   | false      |
  +----------------+------------+
```

7 Network Infrastructure & Connectivity

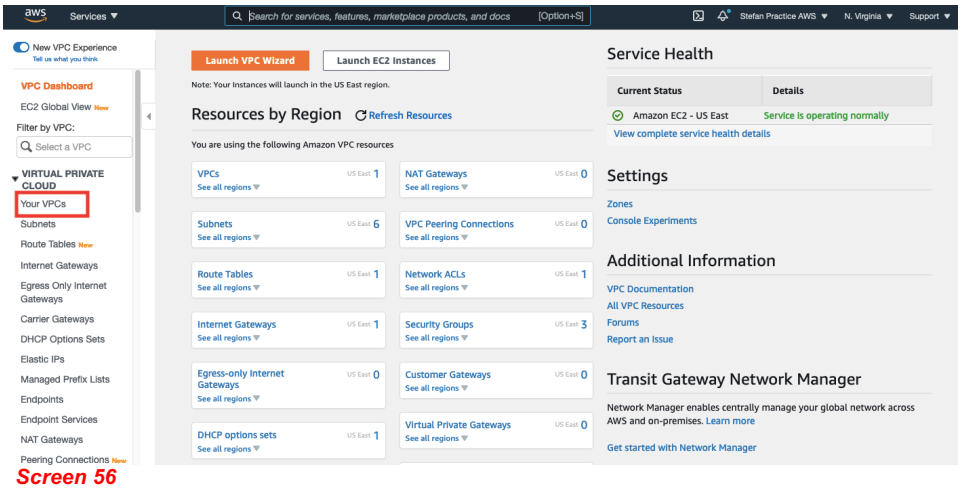
7.1 VPC Components

Virtual Private Cloud (VPC) is a Virtual Network in your own logically isolated area in AWS Cloud. It is your own network in the Cloud. VPC spans all Availability Zones within a region.

VPC consists of:

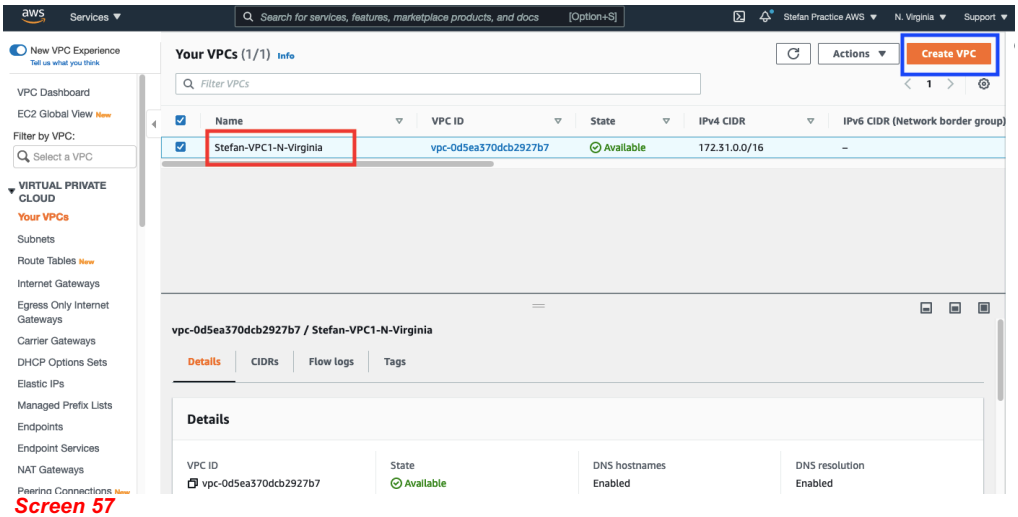
- Subnet – *Range of IP address in VPC*
- Internet Gateway – *Gateway that you attach to your VPC to enable communication between resources in your VPC and the internet.*
- VPC Endpoint – *Enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection*
- Route Table – *Where network traffic is directed*

From AWS Management Console, click ***VPC*** & you will be on ***VPC Dashboard*** displayed on screen 56



Screen 56

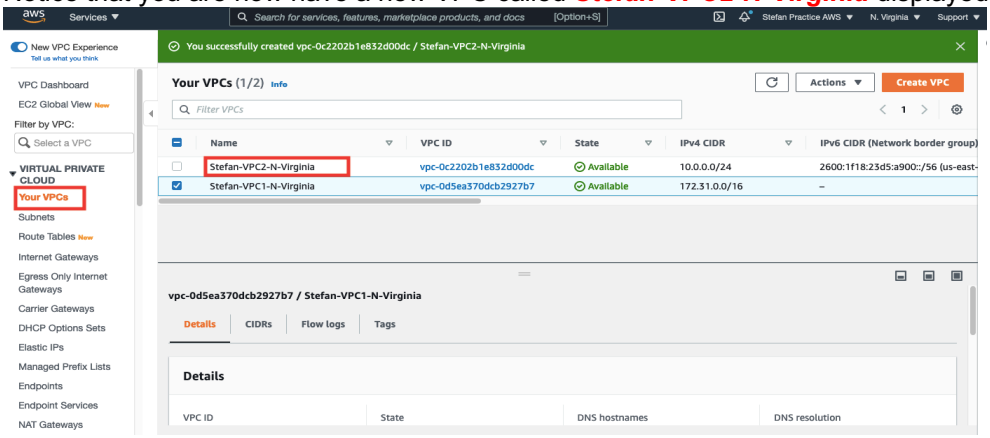
Click Your VPC on screen above and you will see screen below



Screen 57

You are currently only having 1 VPC called ***Stefan-VPC1-N-Virginia***, Click ***Create VPC*** on screen above to create another VPC and follow the instruction. When you've successfully created another VPC, refresh your VPC Dashboard and click ***Your VPCs*** again and you will see screen below.

Notice that you are now have a new VPC called ***Stefan-VPC2-N-Virginia*** displayed on screen 58



Screen 58

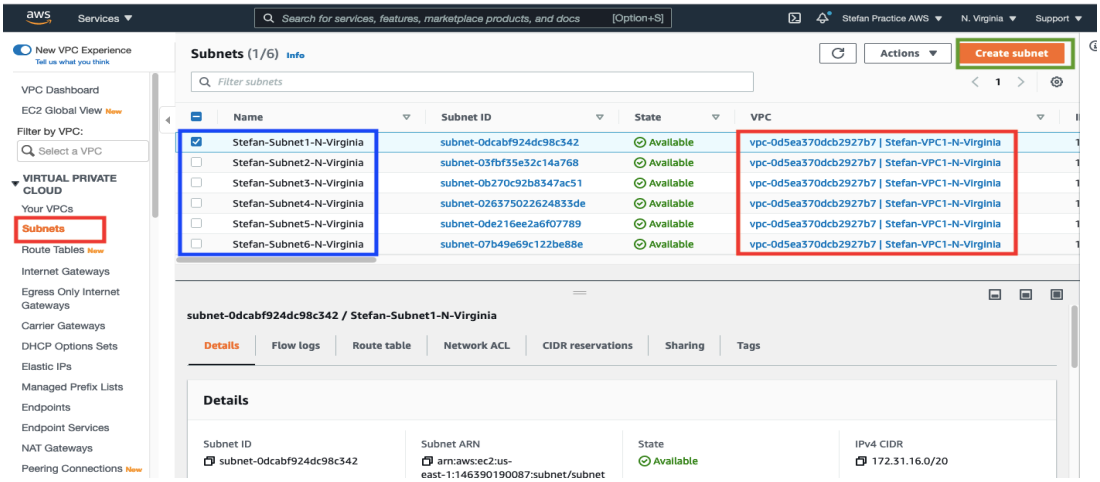
You have successfully created another VPC.

7.1.1 VPC Component: Subnet

VPC is like an apartment and subnet is like a room on your apartment. You can have up to 200 subnets on each VPC. Subnet is associated 1 to 1 with AZ. Subnet can only be in 1 Availability Zone.

Subnet is a key component in VPC. A VPC can contain **all public subnets** (or) public/private subnet combination. Private Subnet is a subnet which doesn't have a route to the internet gateway. A subnet can be configured as a VPN-only subnet by routing traffic via virtual private gateway.

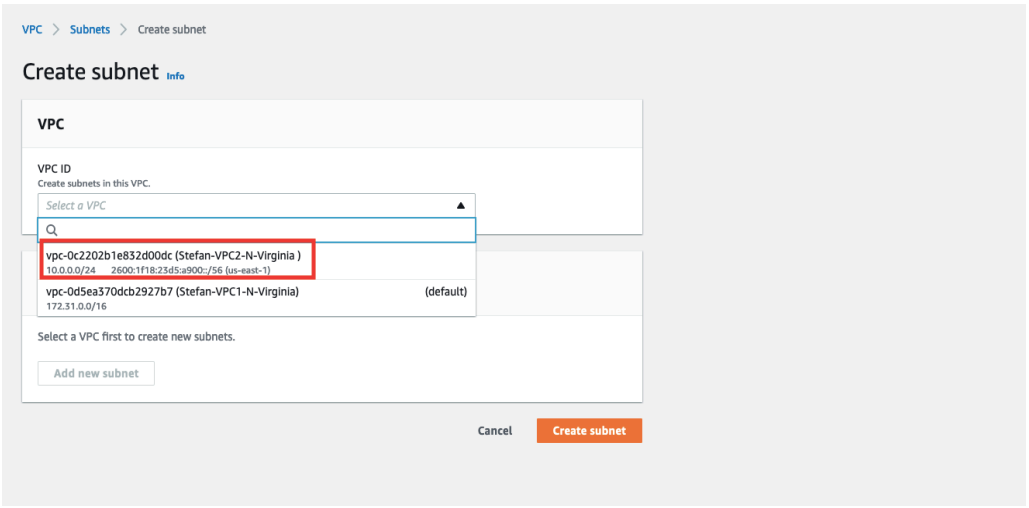
Click ***Subnets*** on the left side of your screen and you will see screen below



Screen 59

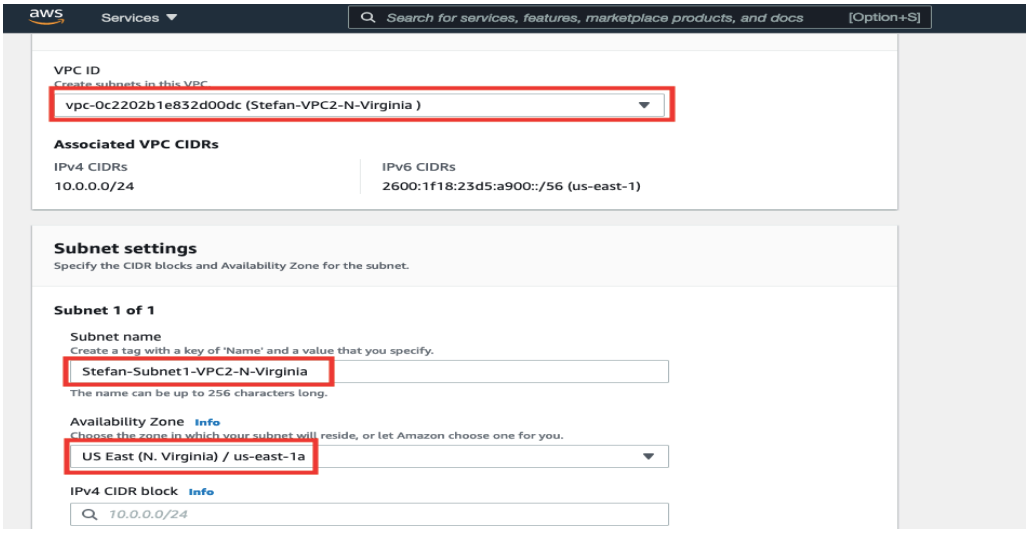
Please note that you have currently six subnets and all of them are in a single VPC called ***Stefan-VPC1-N-Virginia***. Again, one VPC can have up to 200 subnets.

You can create additional subnets by clicking ***Create Subnet*** on screen 55 above and you will see screen below. You must first select VPC when creating a subnet since subnet is a component of VPC *(a room/Subnet inside an apartment/VPC)*.



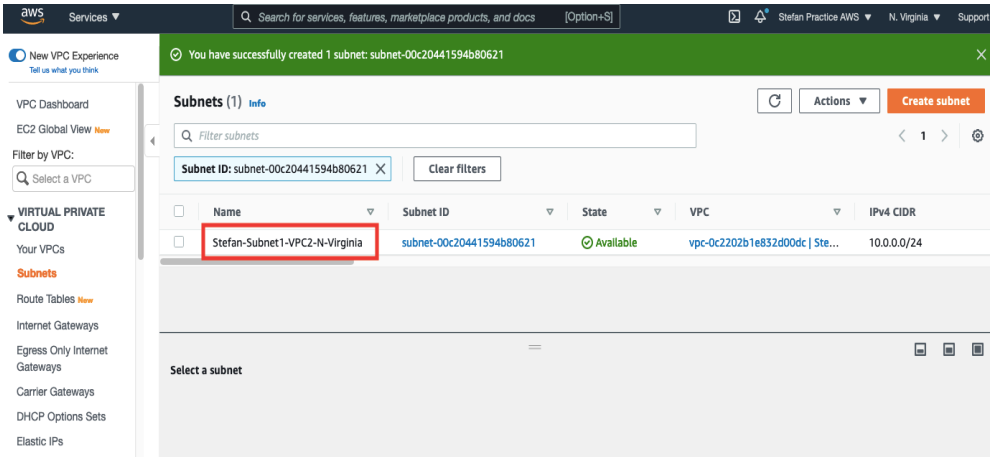
Screen 60

Scroll down on screen below and populate Subnet Name & specify the Availability Zone. Remember a subnet is identic to an Availability Zone and both are inside VPC.



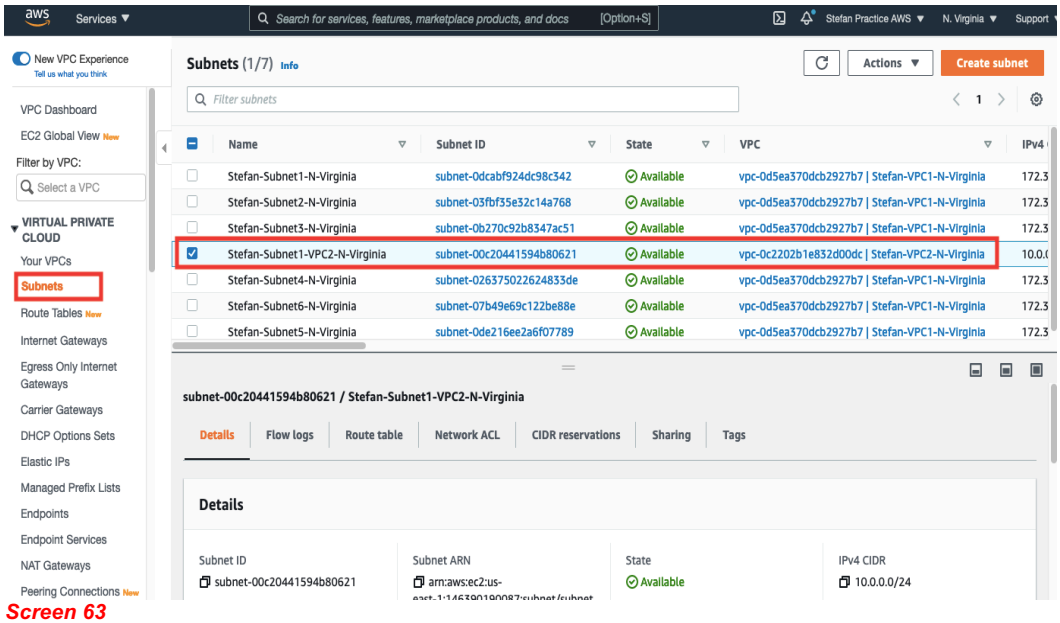
Screen 61

Scroll all the way down and click ***Create Subnet*** and you will see screen below



Screen 62

You have successfully created another Subnet in VPC 2. Click the subnet id and you will see screen 63



Screen 63

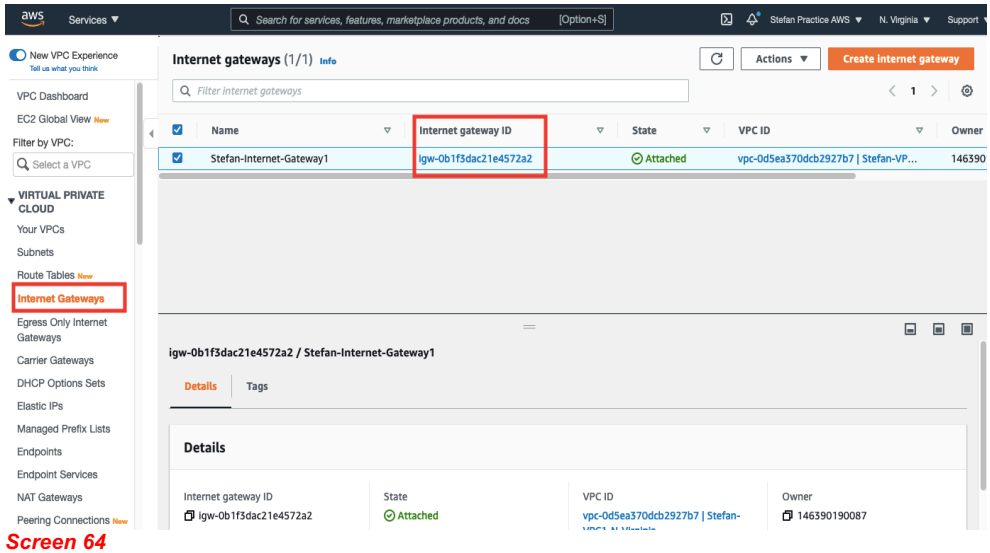
7.1.2 VPC Component: Internet Gateway

It's a VPC component that allows communication between the VPC and the internet. They are horizontally scaled, redundant, and highly available.

You cannot use an internet gateway to interconnect your ON-PREM network with AWS Cloud.

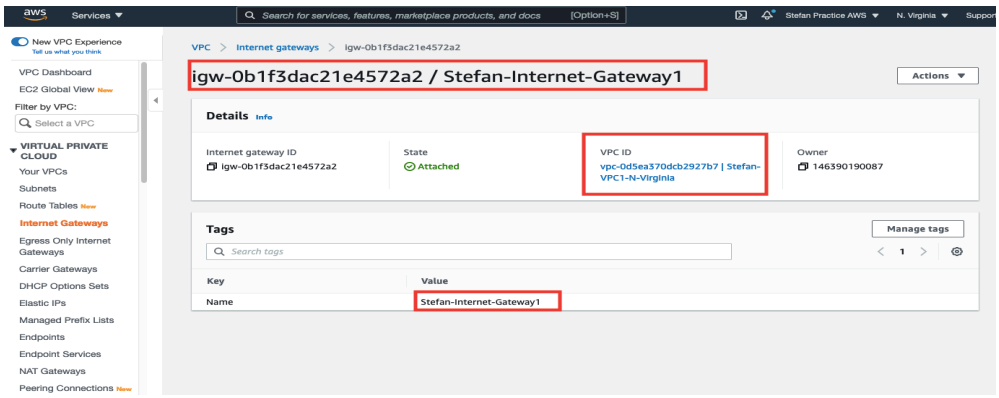
It's a VPC with PUBLIC Subnet to Internet

On your left side of the screen click ***Internet Gateways*** and you will see screen below



Screen 64

On screen above, click internet gateway id link and you will see screen below



Screen 65

This is an Internet Gateway called ***Stefan-Internet-Gateway1*** running inside VPC called ***Stefan-VPC1-N-Virginia***

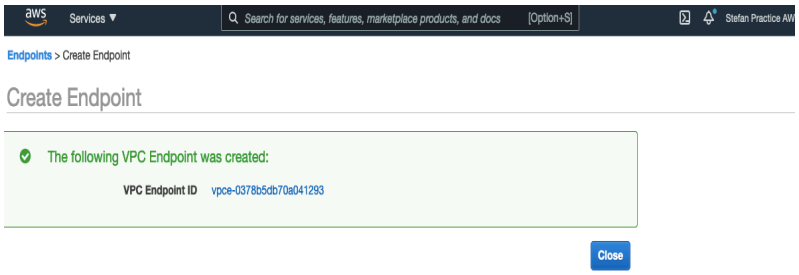
7.1.3 VPC Component: VPC Endpoint (Gateway & Interface)

A VPC Endpoint is a private connection between your VPC and another AWS service that doesn't require internet access.

There are two types of VPC Endpoints

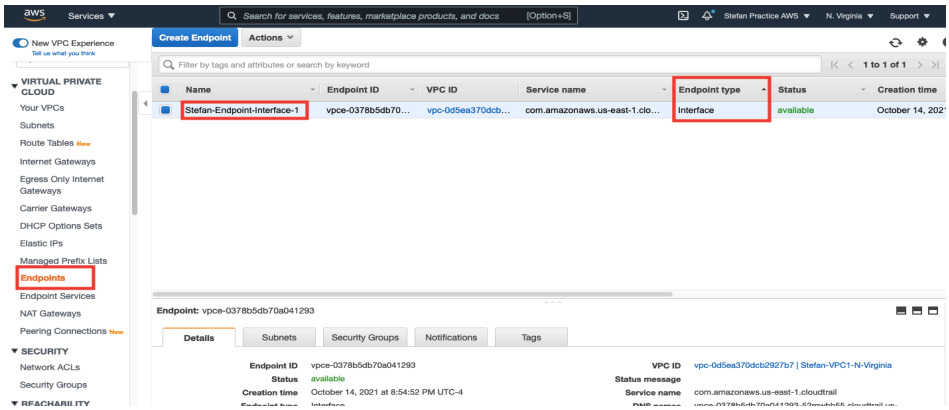
1. VPC Endpoint Gateway
2. VPC Endpoint Interface

From VPC Dashboard, on the left side click ***Endpoints*** and follow instructions to create Endpoint. Once you've successfully created an Endpoint, you will see screen below



Screen 66

Refresh Endpoint and you will see screen below



Screen 67

Here you can see VPC Endpoint Interface has been created successfully. Keep in mind again, there are two types of VPC Endpoint: VPC Endpoint Gateway & VPC Endpoint Interface

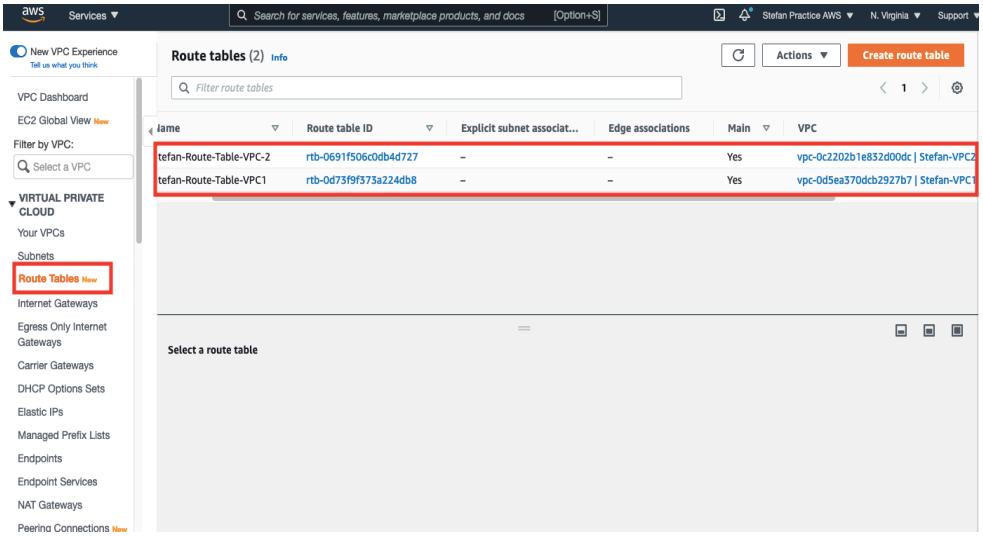
VPC Endpoint Gateway	*VPC Endpoint Interface*
• Sit inside VPC • Must be inside VPC to be used • Support ONLY; Amazon S3 & Dynamo DB	• Sit inside subnet • Available to be used outside of VPC with VPN, Direct Connect or VPC Peering • Support must of AWS services i.e., Amazon SQS, Amazon SNS & AWS Cloud Formation

Screen 68

7.1.4 VPC Component: Route Table

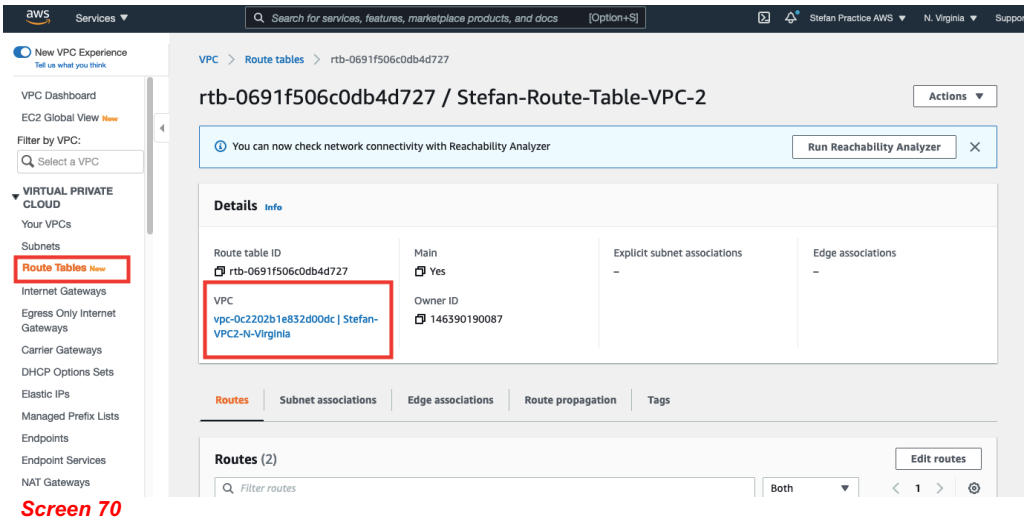
A route table contains a set of rules, called routes, that are used to determine where network traffic from your subnet or gateway is directed. To put it simply, a route table **tells network packets which way they need to go to get to their destination**

From VPC Dashboard, on your left side of your menu, click Route Tables and you will see screen below



Screen 69

You are currently having two Route Table records on screen above. Click the Route Table Id of the first record and you will see screen below.



Screen 70

Screen above is telling you that it will route the traffic to ***Stefan-VPC2-N-Virginia***

You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
A VPC spans all Availability Zones (AZs) within a region.

Virtual Private Network (VPC) – Your Isolated Network – on ***Stefan-VPC1-N-Virginia***
Region: Northern Virginia (US-East1)

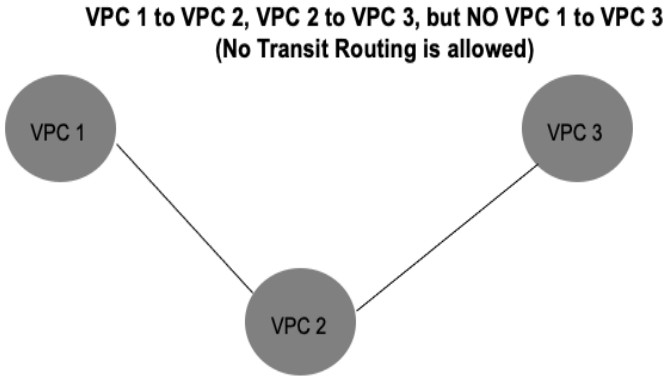
- Subnet – Availability Zone 1 (US-East1**a**)
- Subnet – Availability Zone 2 (US-East1**b**)
- Subnet – Availability Zone 3 (US-East1**c**)
- Subnet – Availability Zone 3 (US-East1**d**)
- Subnet – Availability Zone 3 (US-East1**e**)
- Subnet – Availability Zone 3 (US-East1**f**)

Screen 71

7.2 VPC Peering Vs. Transit Gateway

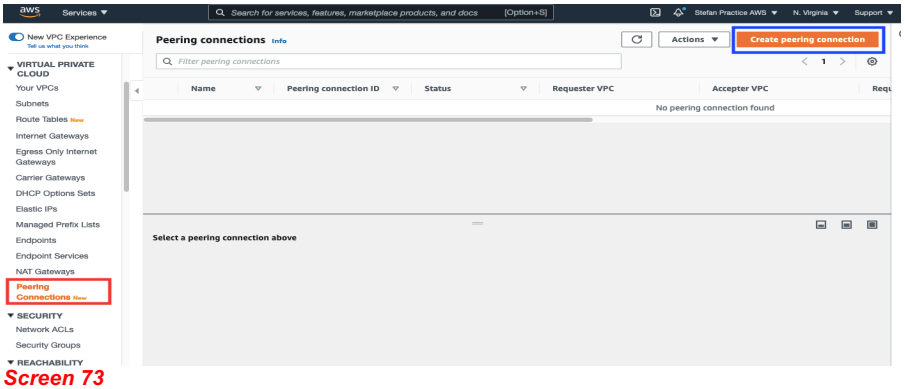
7.2.1. VPC Peering

VPC Peering is network connection between two VPCs. It can connect two VPCs in different AWS accounts. No transit routing is allowed with VPC Peering



Screen 72

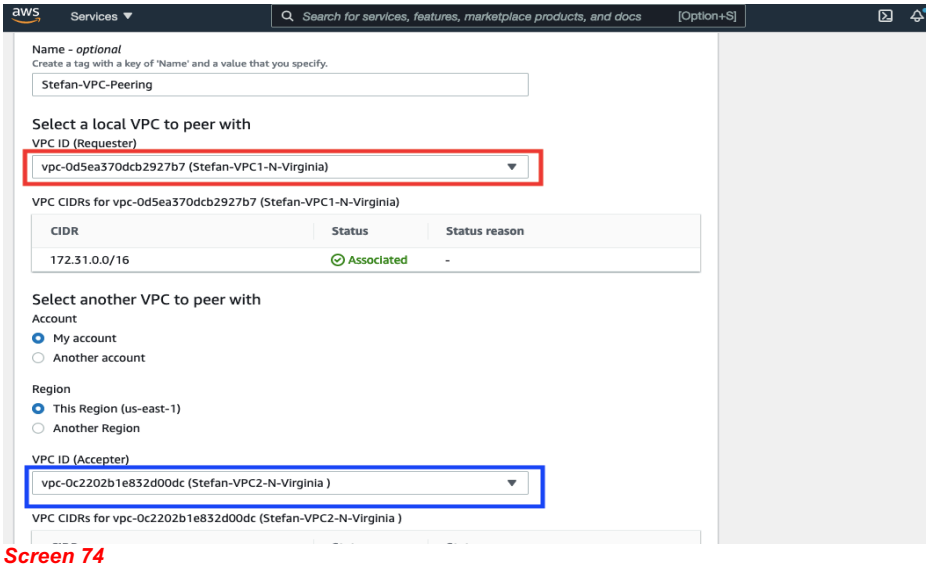
Now that you have two VPCs, you can do VPC Peering. On the left side of your screen 68 above, scroll down and click ***Peering Connection*** and you will see screen 69 below



Screen 73

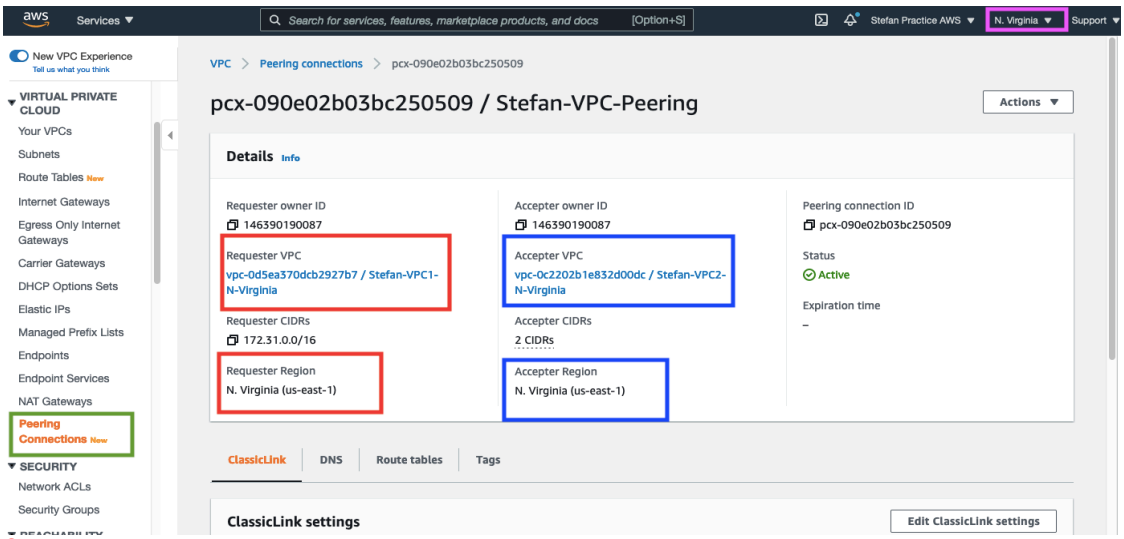
On screen above, click ***Create Peering Connection*** and you will see screen below.

Basically, I'd like to connect between my two VPCs; VPC # 1: ***Stefan-VPC1-N-Virginia*** & VPC # 2: ***Stefan-VPC2-N-Virginia***



Screen 74

Notice on screen above, I specified my VPC **Requester** which is ***Stefan-VPC1-N-Virginia*** & my VPC **Accepter** which is ***Stefan-VPC2-N-Virginia***. Scroll down and click ***Create Peering Connection*** and you need to accept this peering request. Once you've done it, refresh ***Peering Connection*** screen and you will see screen below



Screen 75

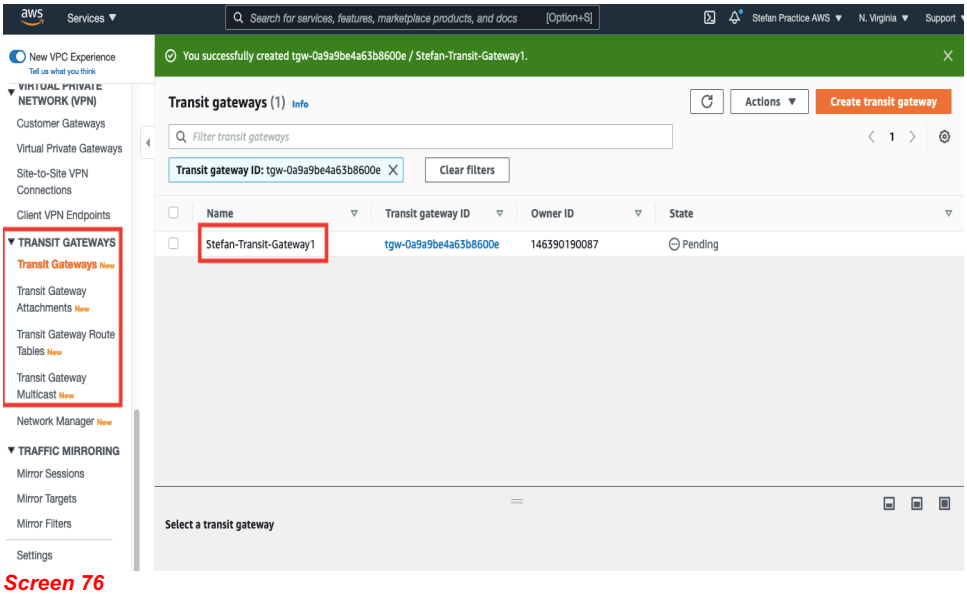
You have successfully connected between VPC 1 (***Requester VPC: Stefan-VPC1-N-Virginia***) to VPC 2 (***Accepter VPC: Stefan-VPC2-N-Virginia***) using VPC Peering, as you can see on screen above.

Please note that you can have these two VPCs at different regions and/or different AWS accounts if you want to but both of my VPCs are in Northern Virginia region.

7.2.2. AWS Transit Gateway

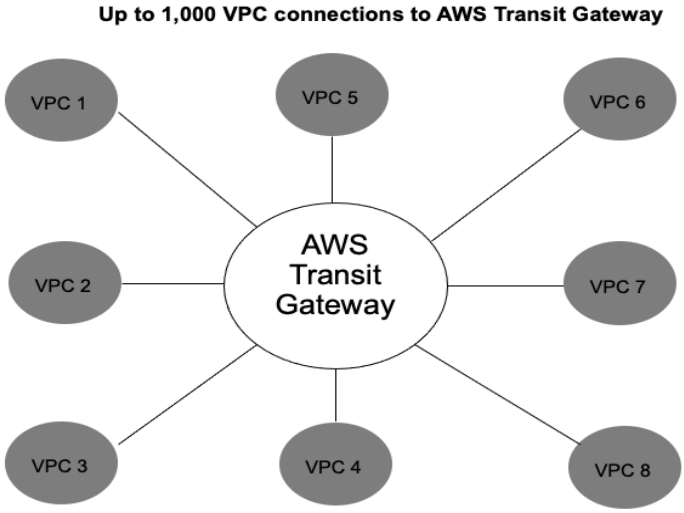
AWS Transit Gateway **connects VPCs and on-premises networks through a central hub**. This simplifies your network and puts an end to complex peering relationships. It acts as a cloud router – each new connection is only made once. It can connect up to 1,000 VPCs

Once you click ***Transit Gateway*** on the left side of your screen, you will see screen below. I have created Transit Gateway earlier on screen below



Screen 76

Please understand the difference between VPC Peering vs. AWS Transit Gateway. Both are to be used to connect VPC, the difference is that VPC Peering only connects between two VPCs while AWS Transit Gateway can connect up to 1,000 VPC connections.

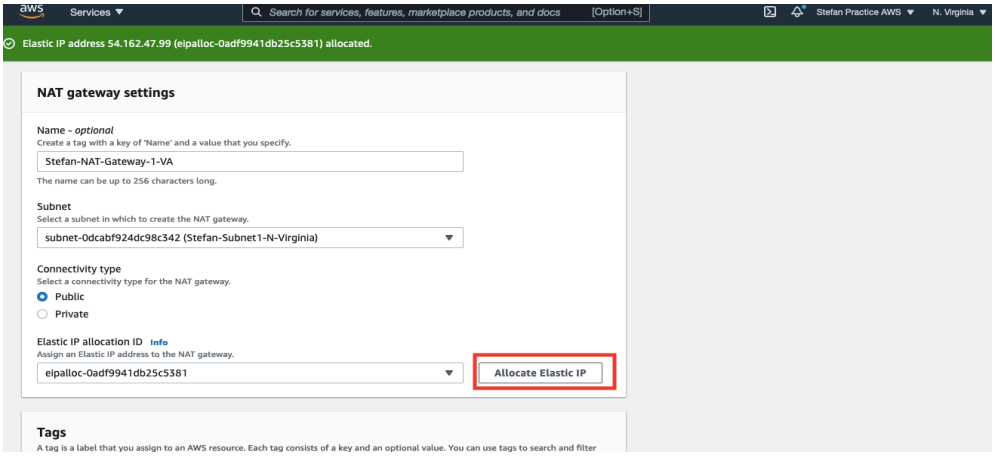


Screen 77

7.3 VPC – NAT Gateway

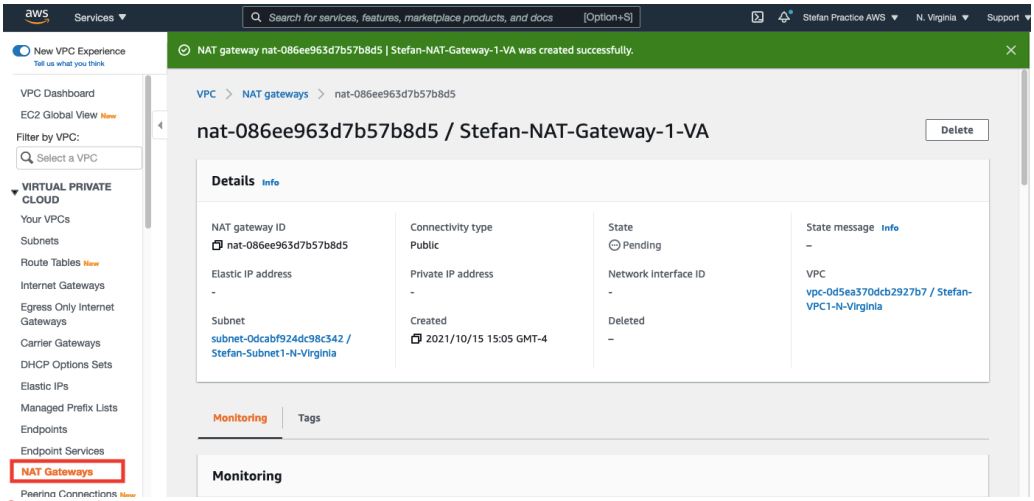
NAT Gateway is an AWS Service that allows a private subnet to have access to the internet but prevents the internet from initiating a connection directly to the instances.

Click ***VPC*** from AWS Management Console and once you're on VPC screen, scroll down and click ***NAT Gateways*** on the left side of your screen and start creating your NAT Gateway. Make sure you click ***Allocate Elastic IP*** button shown on screen below



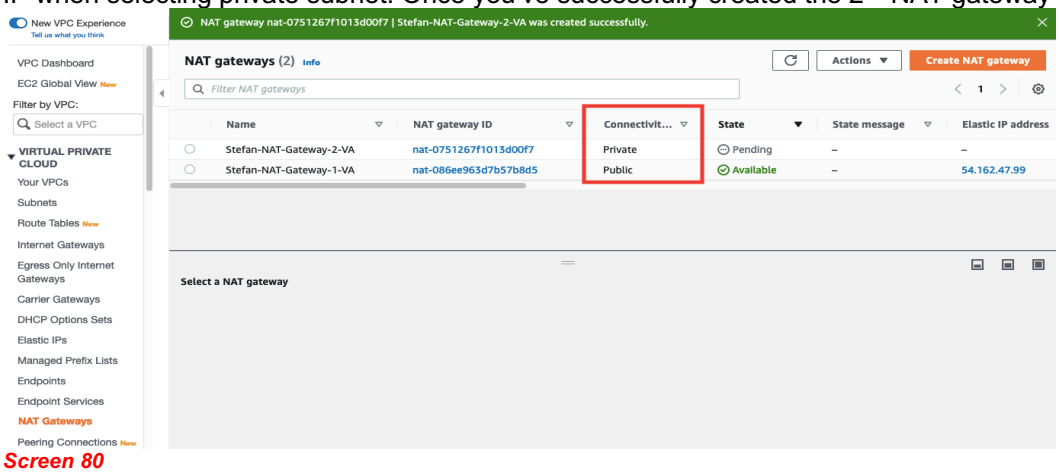
Screen 78

After successfully created NAT Gateway, you will see screen below



Screen 79

Create another one, and this time make sure you select Private Subnet, you don't need to Allocate Elastic IP when selecting private subnet. Once you've successfully created the 2nd NAT gateway displayed below



Screen 80

Notice on screen above that you have 2 NAT gateway records; 1 public subnet and 1 private subnet.

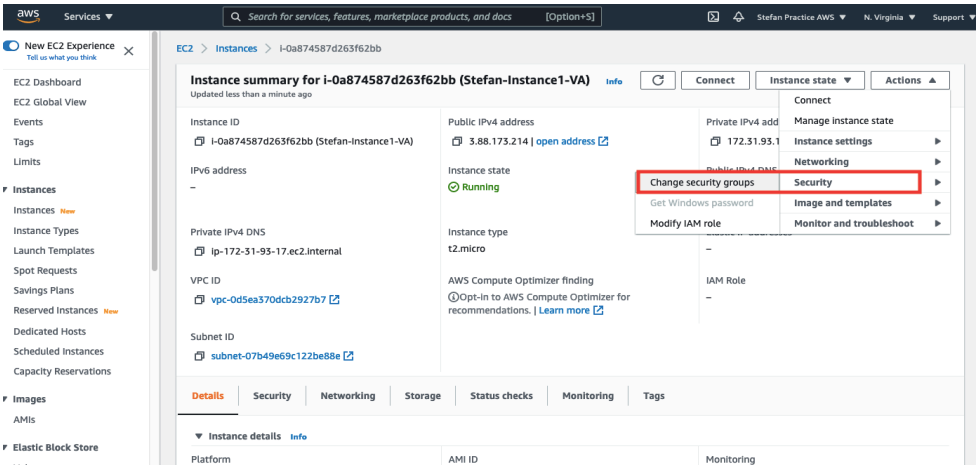
7.4 VPC Firewall – Security Group

A *security group* acts as a virtual firewall for your instance to control inbound and outbound traffic.

- It acts as a Firewall at the Instance Level

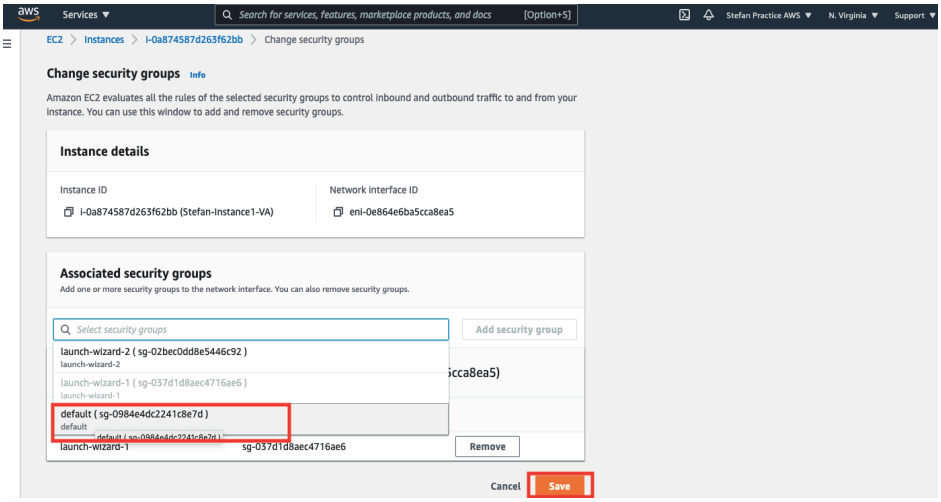
- Allow Rule (Only Allow rules are specified but not Deny rules) & by default deny everything. Hence, you need to specific which one is allowed to access certain ports & IP address
- It cannot block a specific IP address
- Stateful – return traffic is automatically allowed regardless any rules
- Can create 500 security groups per VPC and 5 security groups per instance

Go to AWS Management Console and go to your EC2 Instance Dashboard and select an instance, for example ***Stefan-Instance1-VA*** and you will see screen 81 below.



Screen 81

On this screen above, under ***Action***, select ***Security*** and ***Change Security Groups*** & you will see screen below



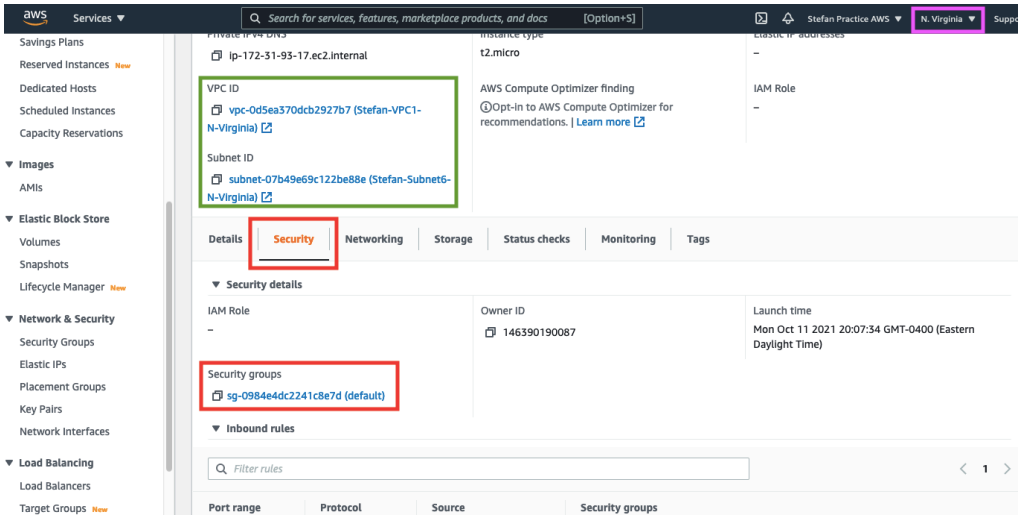
Screen 82

Select security group, in this scenario, default security group has been selected.

Default security groups: *An AWS created default security group has* ***one default inbound rule allowing traffic from other instances associated with the same security group****.*

The rule enables the instances to communicate with each other without needing to go out to the internet

Click ***Save*** on screen above and click ***Security*** tab and you will see screen below

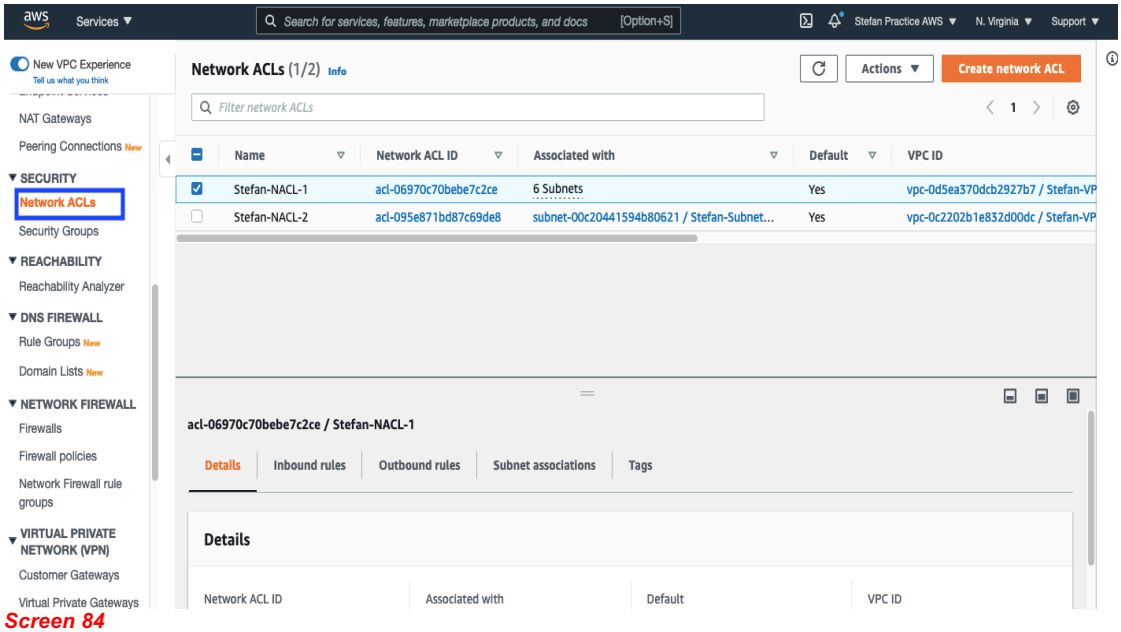


Screen 83

You can see that default security has been successfully added to your EC2 Instance ***Stefan-Instance1-VA*** You can add up to 5 security groups per instance and you can create 500 security groups per VPC. You can also find VPC & Subnet information on screen above.

7.5 VPC Firewall – NACL

Click ***Network ACLs*** on the left side of your screen and you will be able to see screen below



Screen 84

Make sure you are fully aware the differences between Security Group vs. NACLs

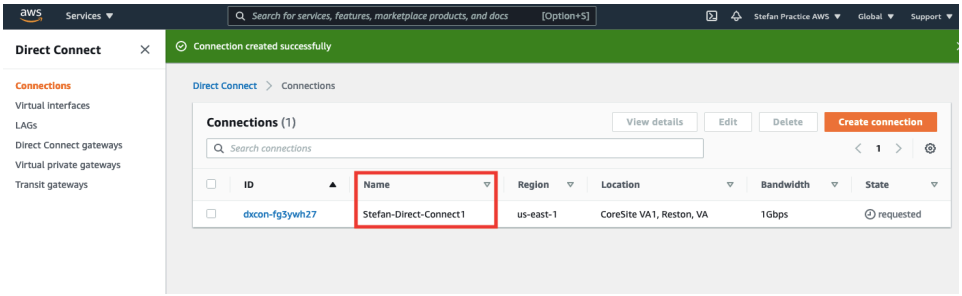
Security Group	***Network Access Control Lists (NACLs)***
Act as a firewall at the Instance Level.	Act as a firewall at the Subnet Level.
Allow Rule (Only “Allow” rules are specified but not “Deny” rules)	“Allow” and “Deny” rules
By default, ***deny everything*** – Hence, you need to specify which one is allowed to access certain ports & IP addresses	By default, ***allow everything***, it doesn’t restrict or deny anything
Cannot block specific IP address (deny everything)	Able to block certain IP address known for abuse
STATEFUL – return traffic is automatically allowed regardless of any rules	STATELESS – Responses to allowed inbound traffic are subject to the rules for outbound traffic (vice versa)
Control incoming/outgoing traffic to your EC2 instances	Controlling traffic in and out of one or more subnet

Screen 85

7.6 ON-PREM to AWS Cloud – AWS Direct Connect

Establish a dedicated network connection from your ON-PREM to AWS Cloud bypassing the internet. Instead, it uses dedicated, private network connections between your Network and AWS.

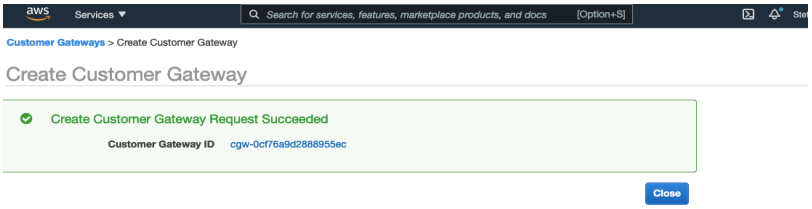
Connect company's ON-PREM environment to VPC without using public Internet. From AWS Console Management type AWS Direct Connect and you will see screen below



Screen 86

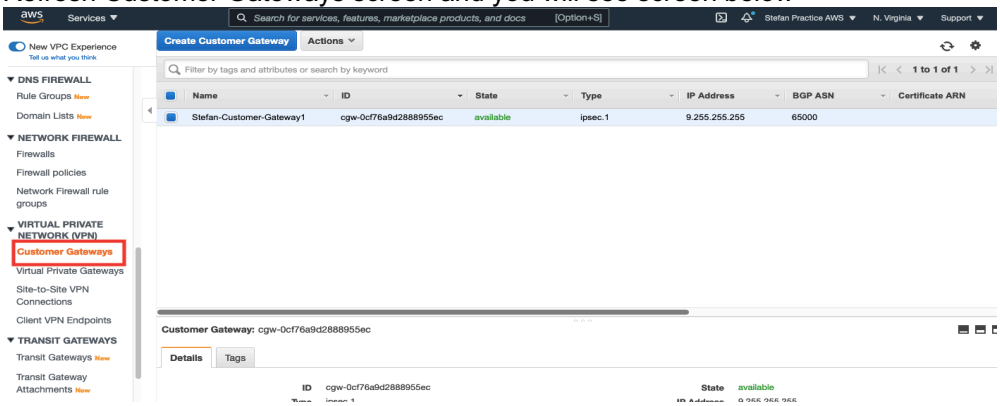
7.7 VPN (Client Side) – Customer Gateway

It's a physical or software application that you own /manage in your ON-PREM (on your side of a site-to-site VPN connection). On your left side menu, click ***Customer Gateways*** and follow instructions to create Customer Gateway. Keep in mind that you need to provide ***public IP address*** when creating Customer Gateways. Once you've successfully created it, you will see screen below



Screen 87

Refresh Customer Gateways screen and you will see screen below

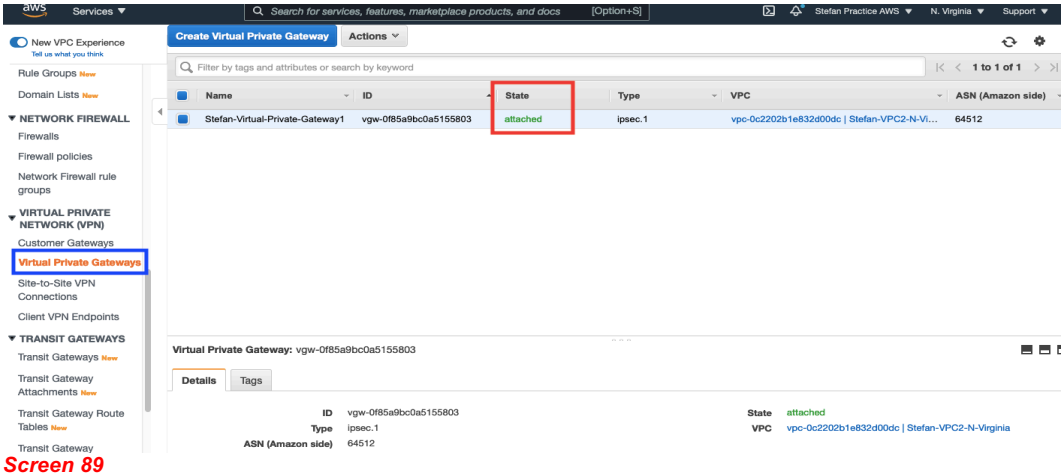


Screen 88

7.8 VPN (AWS Side) – Virtual Private Gateway

Virtual Private Gateway (VPG) are **VPN concentrator on AWS side of the VPN connection between the two networks**.

Customer Gateway (CGW) represents a physical device or a software application on the customer's side of the VPN connection. From your left side of your screen, click Virtual Private Gateways and follow instruction to create one. Make sure you attach to a VPC. Otherwise, the status will be ***detached***. After successfully attaching to a VPC you will see status ***attached*** as displayed on screen below

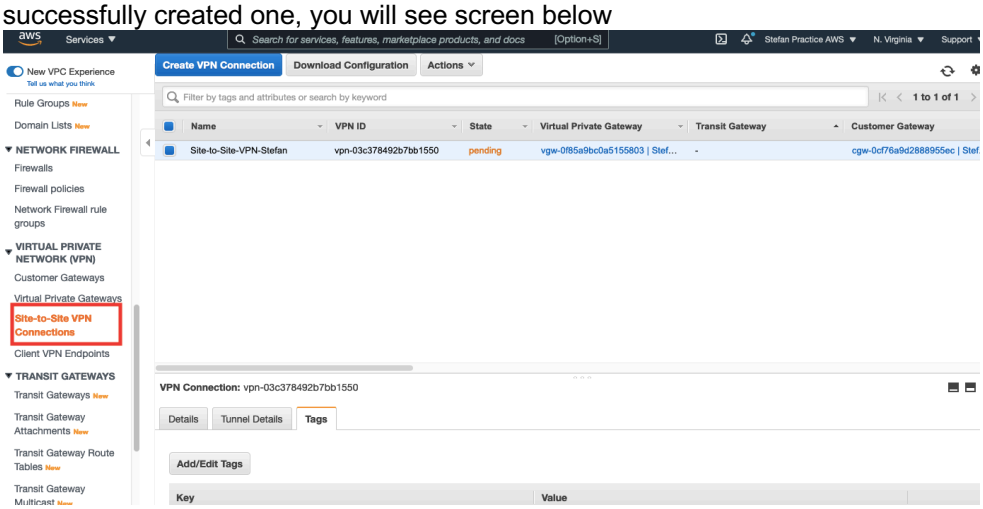


Screen 89

7.9 VPN – Site-to-Site VPN Connection

AWS Site-to-Site VPN is **a fully managed service that creates a secure connection between your data center or branch office and your AWS resources using** IP Security (IPSec) tunnels.

Click ***Site-to-Site VPN Connections*** and create one and please follow the instruction. Once you have successfully created one, you will see screen below



Screen 90

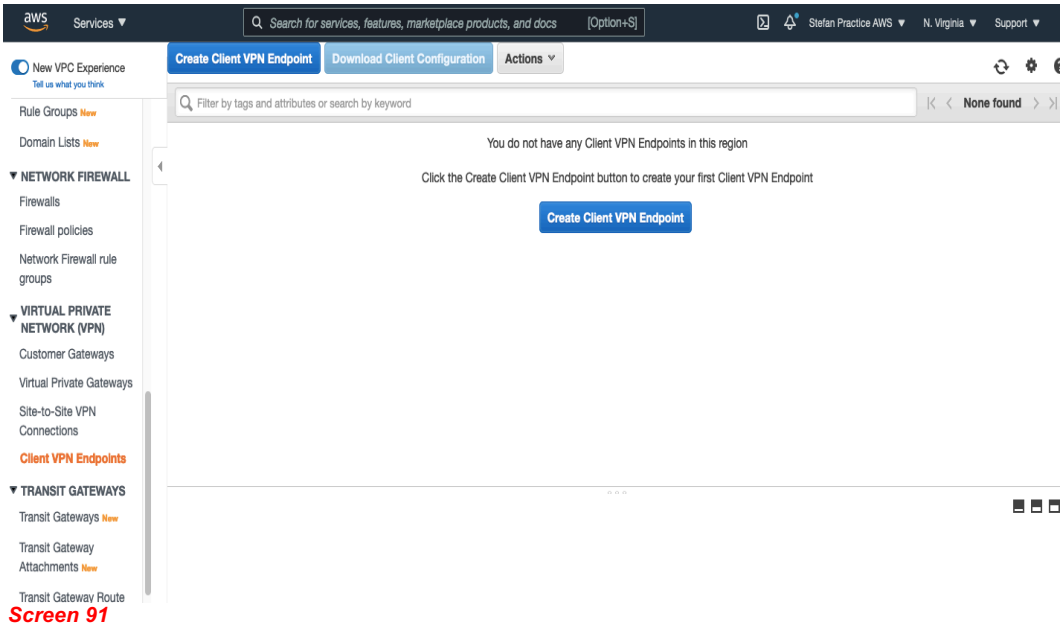
AWS Site-to-Site VPN Components:

1. Transit Gateway
2. Virtual Gateway
3. Customer Gateway
4. Customer Device Gateway

7.10 VPN – Client VPN Endpoint

The Client VPN endpoint is **the resource that you create and configure to enable and manage client VPN sessions**. It is the resource where all client VPN sessions are terminated. Target network. A target network is the network that you associate with a Client VPN endpoint. A subnet from a VPC is a target network.

Please note that all client VPN sessions terminate at the Client VPN endpoint. You configure the Client VPN endpoint to manage and control all client VPN sessions.

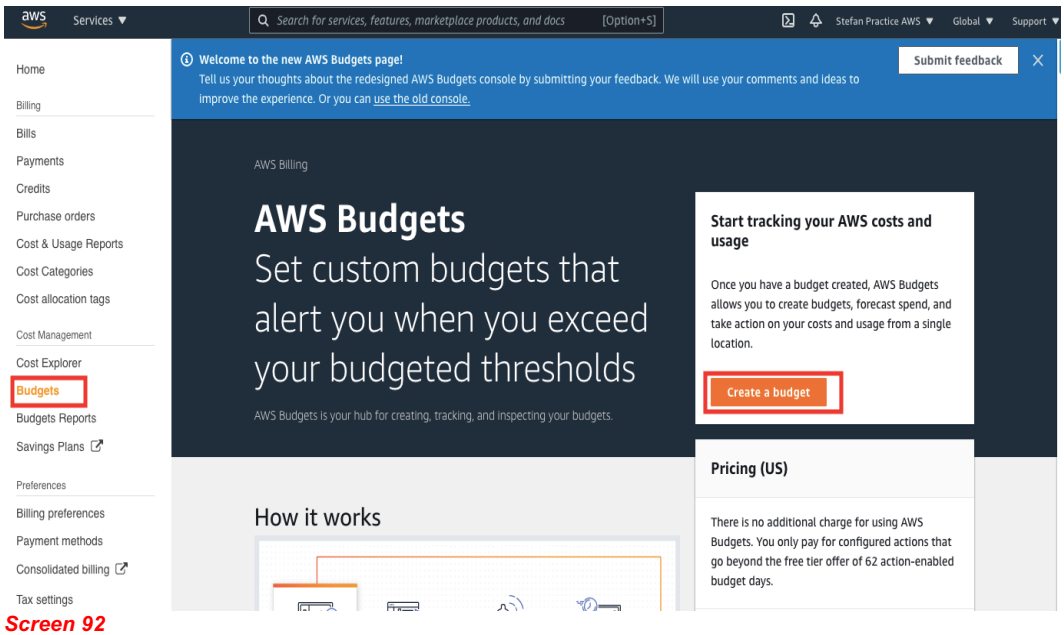


Screen 91

8 Billing and Dashboard

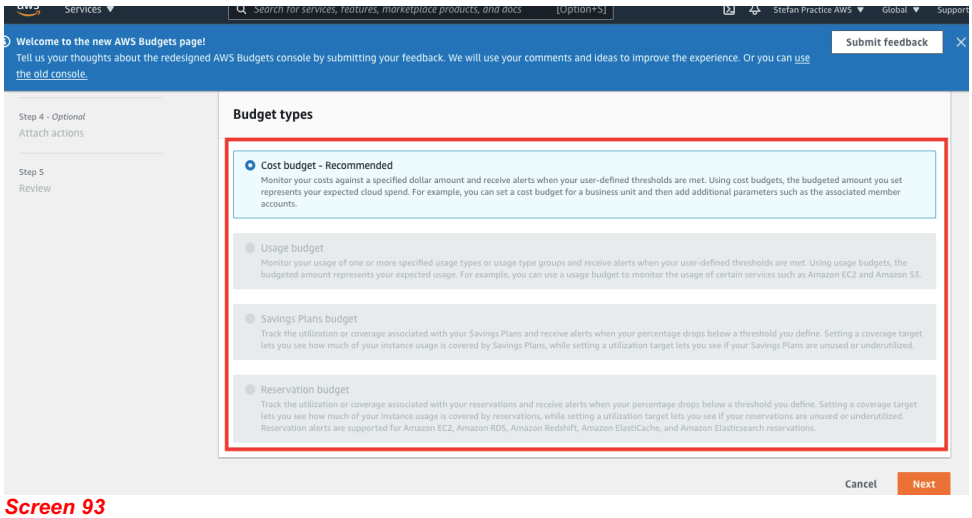
8.1 AWS Budget

It gives you the ability to set custom budgets that alert you when your costs or usage exceed or are forecasted to exceed your budgeted amount.



Screen 92

From AWS Management console, click ***Bill***, scroll down, and click ***Budgets*** and you will see screen above. Click ***Create a Budget*** and you will see screen below.

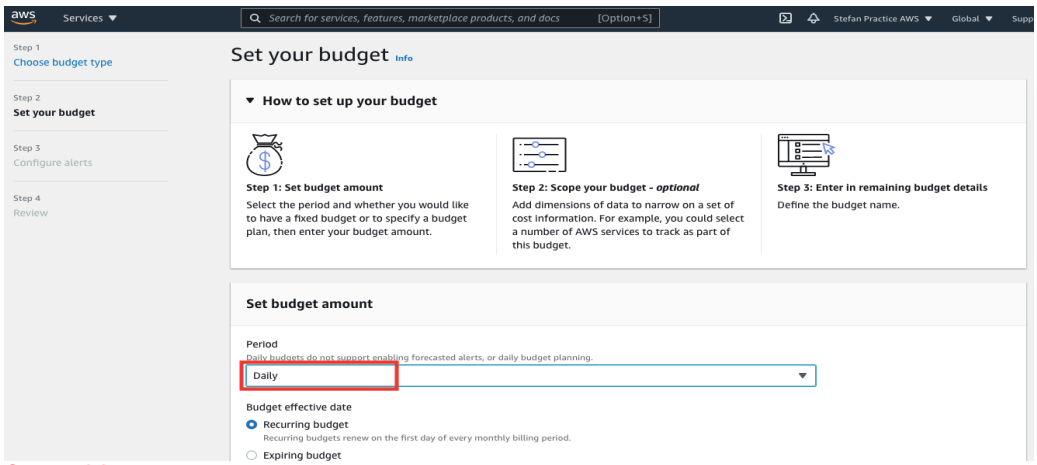


Screen 93

As you can see from screen above. AWS Budget can used to create the following budget types:

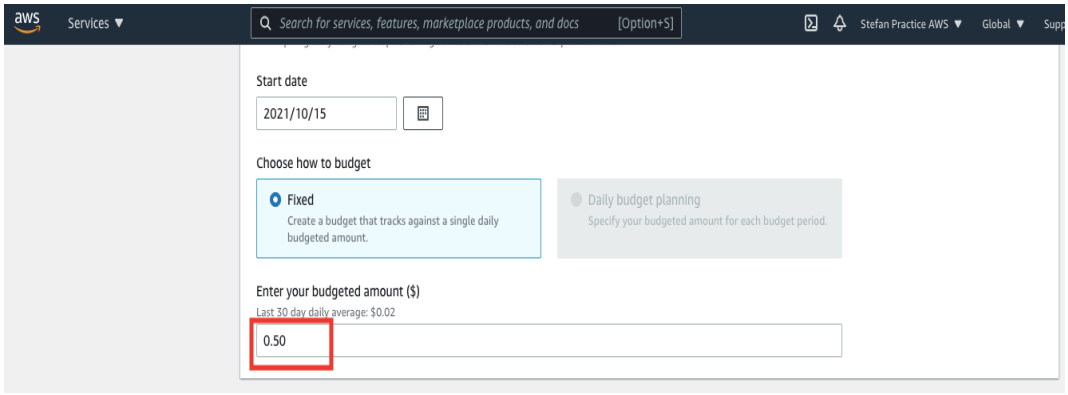
- ***Usage Budget***: *Plan how much you want to USE one or more services*
- ***Cost Budget***: *Plan how much you want to SPEND on a service*
- ***Reservation Budget***: *Track the usage of your reserved instances*
- ***Savings Plan Budget*****:** *Track the utilization or coverage associated with your Savings Plans and receive alerts when your percentage drops below a threshold you define*

Setting up a threshold in AWS Budget. From screen above simply click ***Next*** & you will see screen 94



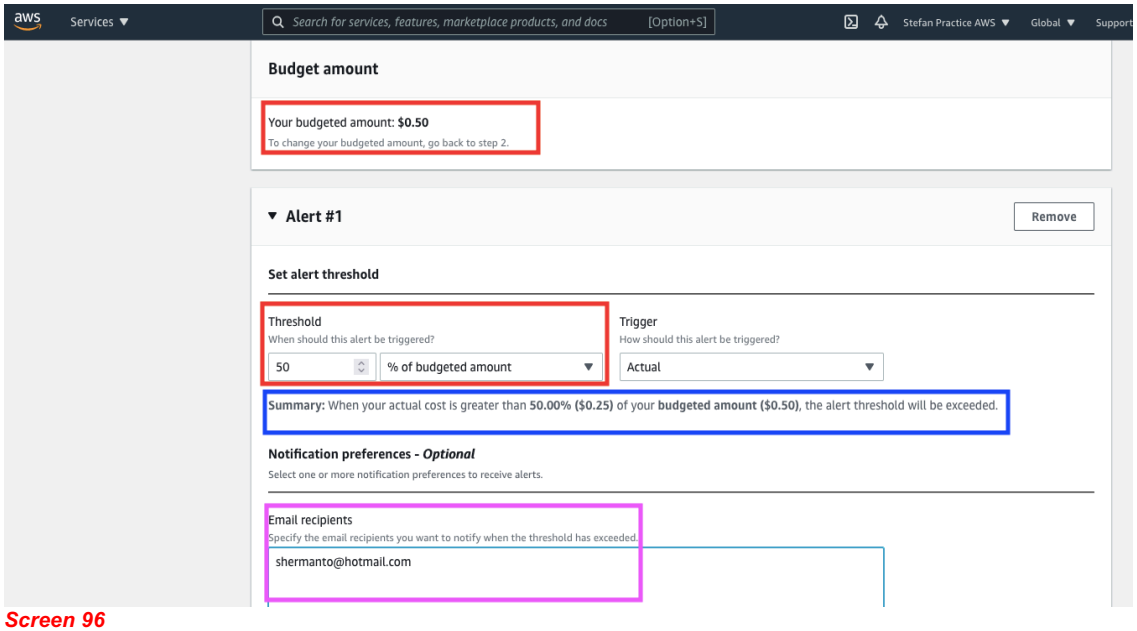
Screen 94

Here you can choose your Period as Daily, Monthly, Quarterly or Annually



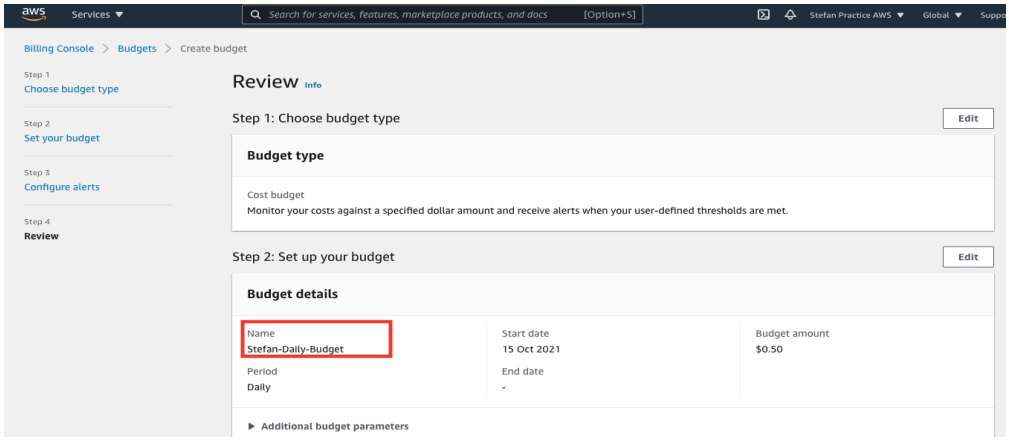
Screen 95

Enter your budgeted amount. Let's say you enter $0.50



Screen 96

Once you have your budgeted amount set, you can also create an alert like displayed on screen 97



Screen 97

Daily budget has been successfully created on screen above.

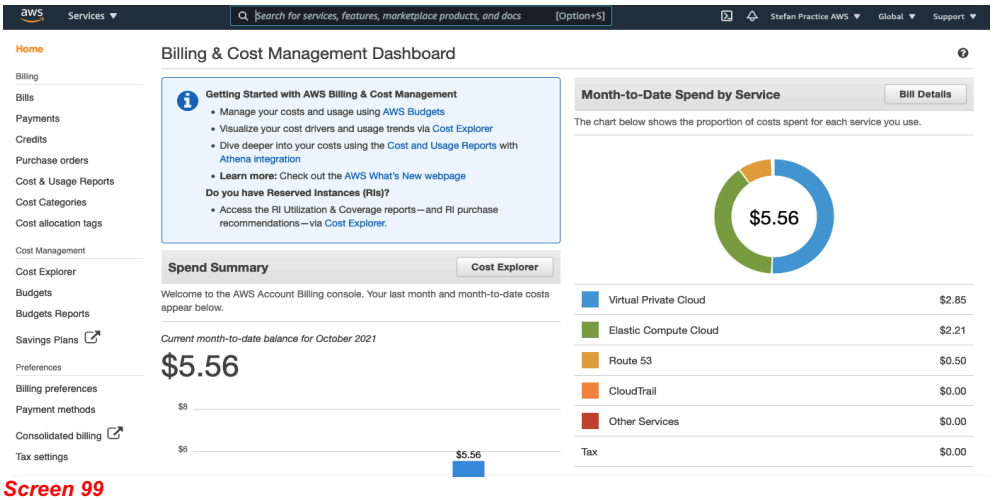
8.2 Billing & Cost Management Dashboard

AWS Billing and *Cost* Management is a web service that provides features that helps you monitor your costs and pay your *bill*. From AWS Management Console click Bill and you will see screen below

This is your bill as of Friday, 10/15/2021

Screen 98

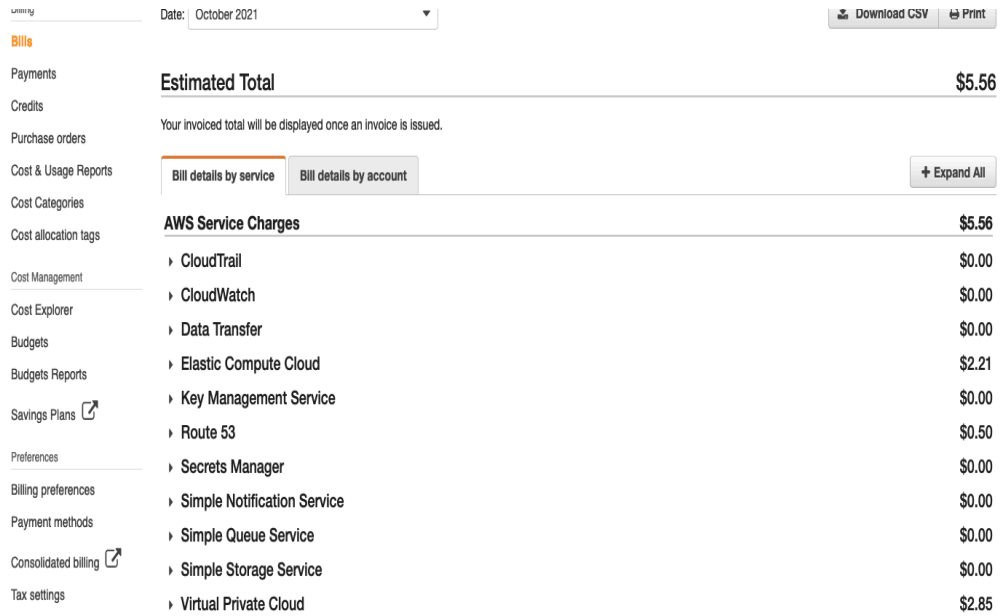
The next day on 10/16/2021, this is my current bill now



Screen 99

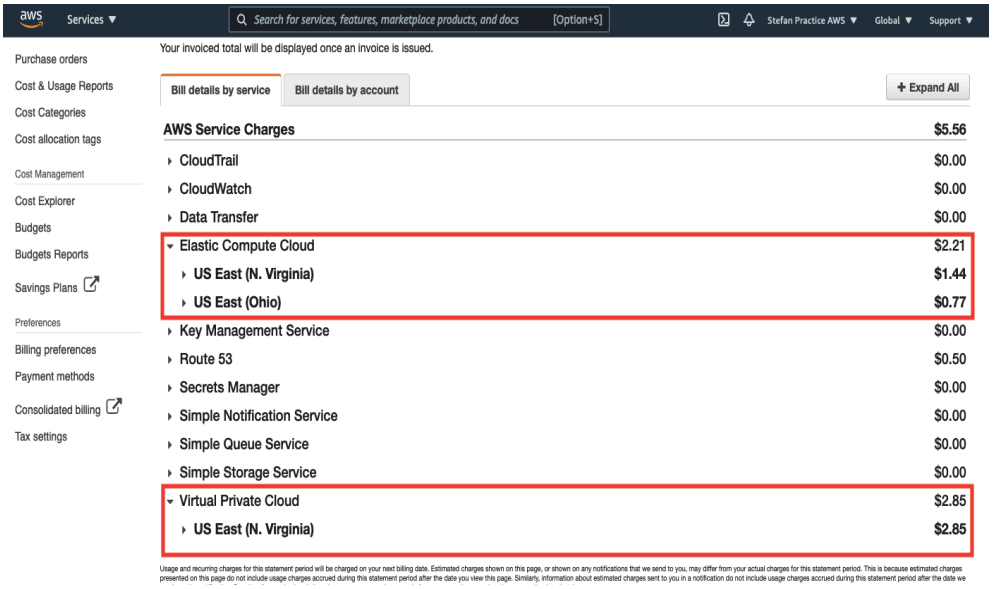
8.2.1 Breakdown the Bill

Let's breakdown the bill. Click ***Bill Details*** from screen above and you will see screen below



Screen 100

Break down EC2 for $2.21 and VPC for $2.85 and you will see screen below

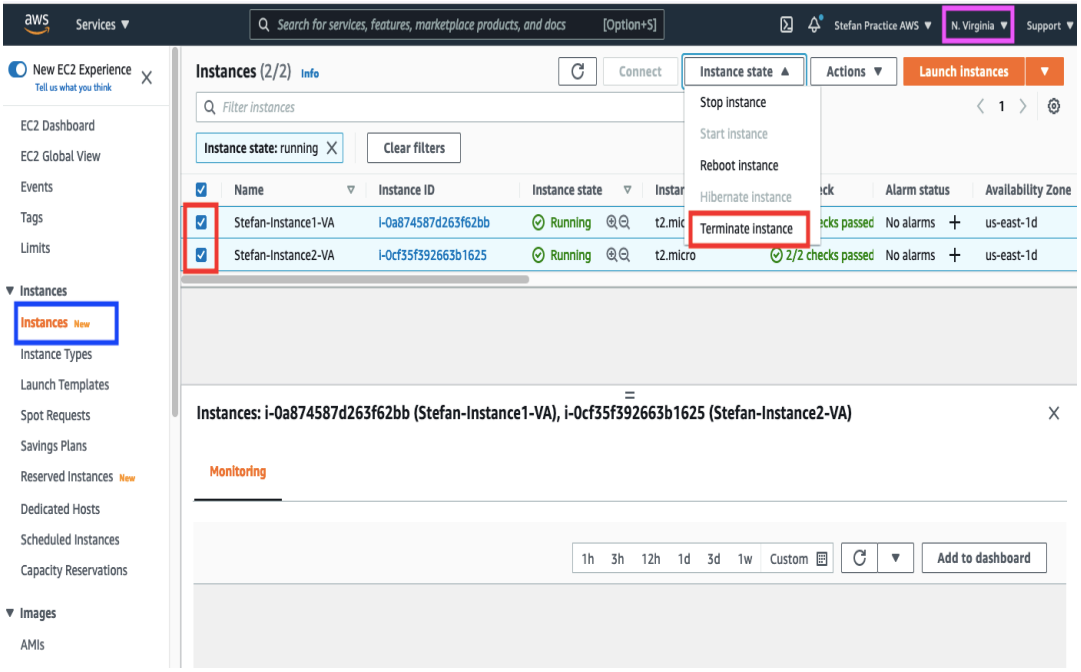


Screen 101

8.2.2 Terminate EC2 From Your Account (Northern Virginia)

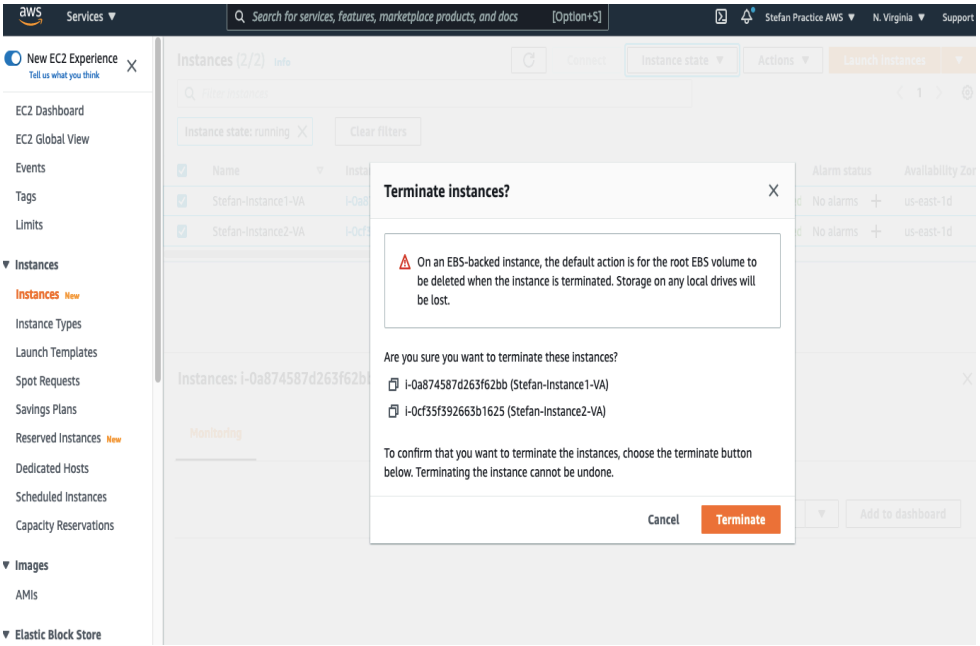
Let's remove EC2 from your account so that you will no longer be charged daily. From the information on screen 97 above, you have EC2 in two different regions: Northern Virginia and Ohio.

Go to your AWS Management Console and click ***EC2*** scroll down and click ***Instances*** and you will see screen below. Make sure that you are in Northern Virginia Region.



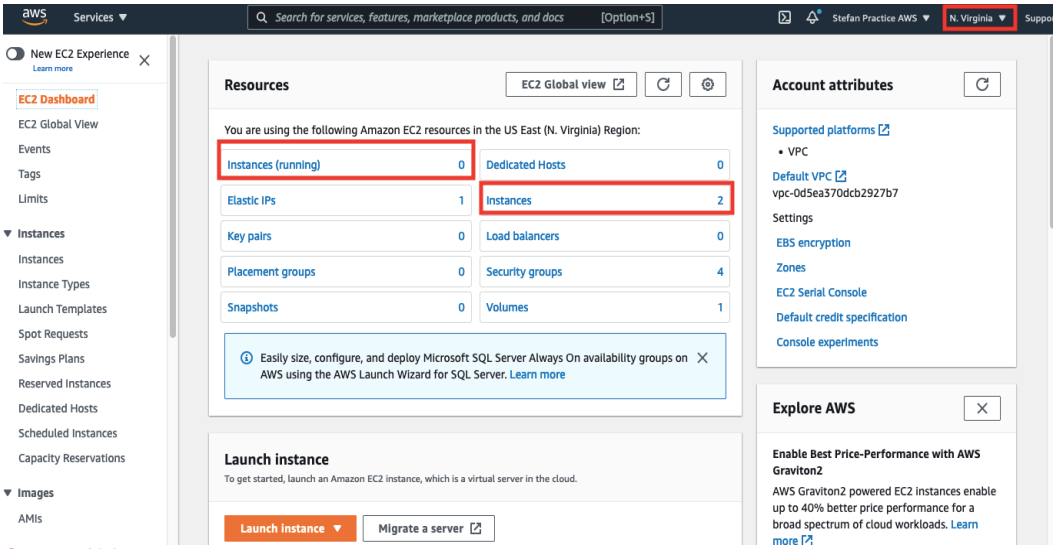
Screen 102

Select both EC2 Instances displayed on screen above, under ***Instance State***, select ***Terminate Instance*** and you will see screen confirmation below on screen 103



Screen 103

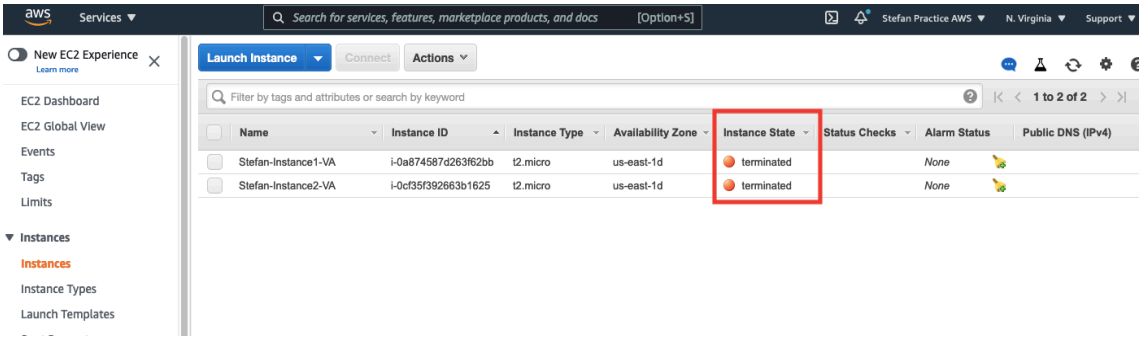
Click ***Terminate*** from screen above and your EC2 Instances will be terminated.
Go back to EC2 Dashboard and you will see this screen again



Screen 104

However, notice the following

- Instances (running) = 0 *(you already terminated both ECs Instances)*
- Instances = 2 *(click it and you will see screen 105 below)*

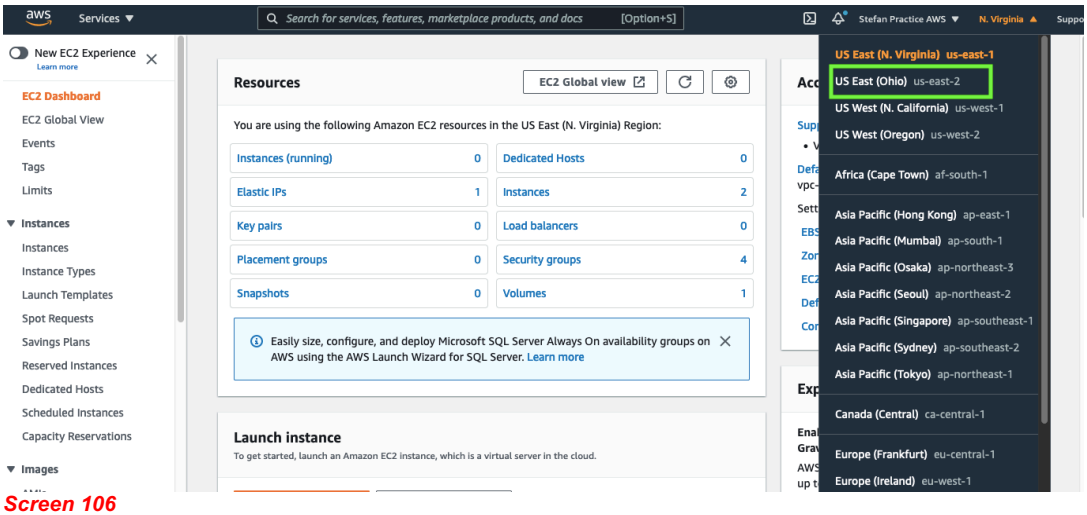


Screen 105

Both instances in Northern Virginia Region are now terminated and you will no longer be charged. Now let's go to Ohio region and terminate the EC2 instance there.

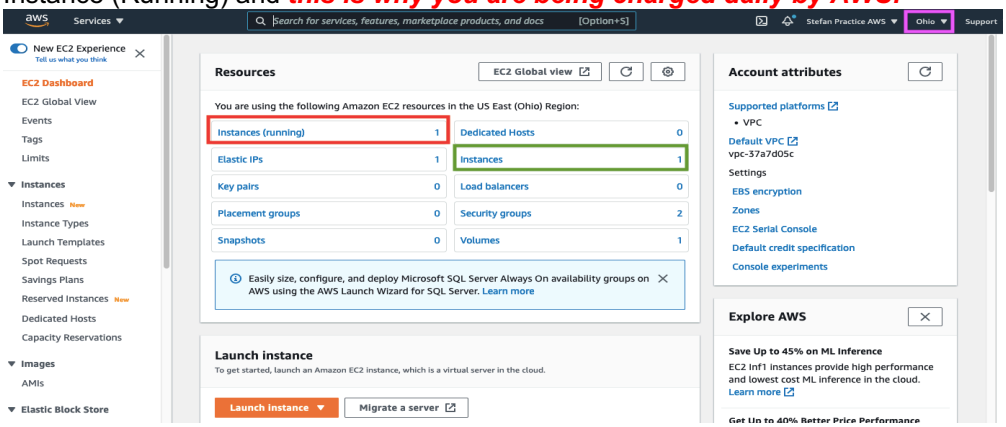
8.2.3 Terminate EC2 From Your Account (Ohio)

Change the Region from Northern Virginia to Ohio displayed on screen 106 below



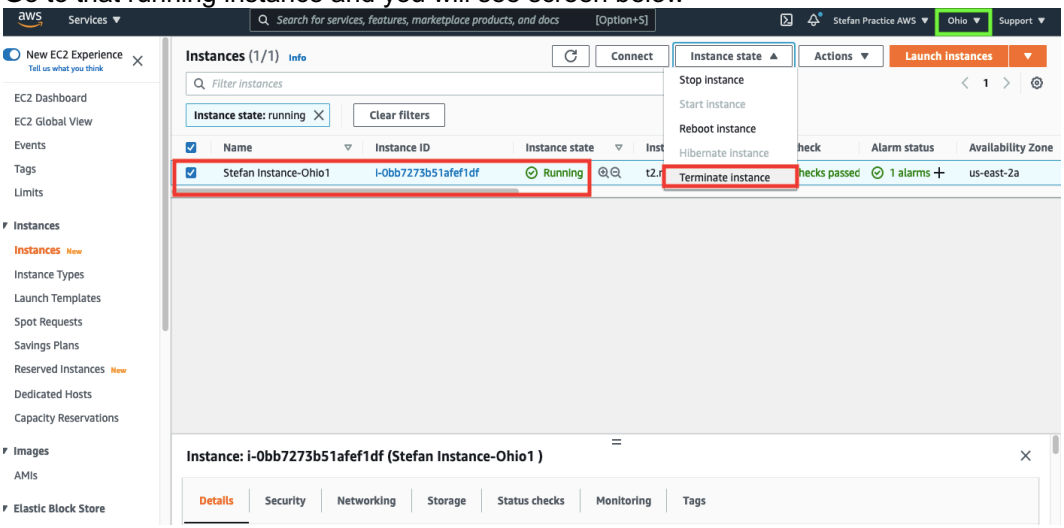
Screen 106

After changing the region to Ohio, you will see EC2 Dashboard screen below. Notice that you have 1 Instance (Running) and ***this is why you are being charged daily by AWS!***



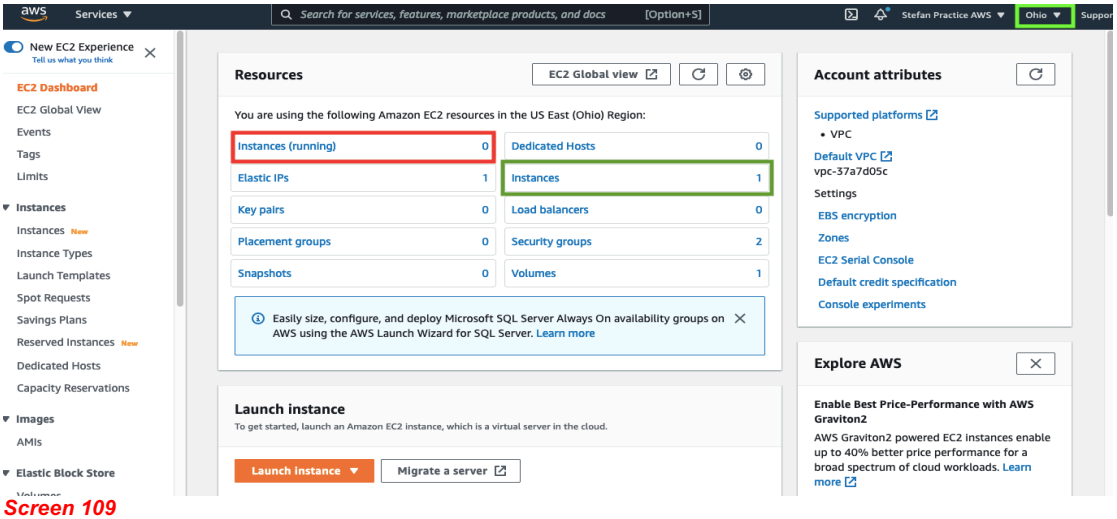
Screen 107

Go to that running instance and you will see screen below



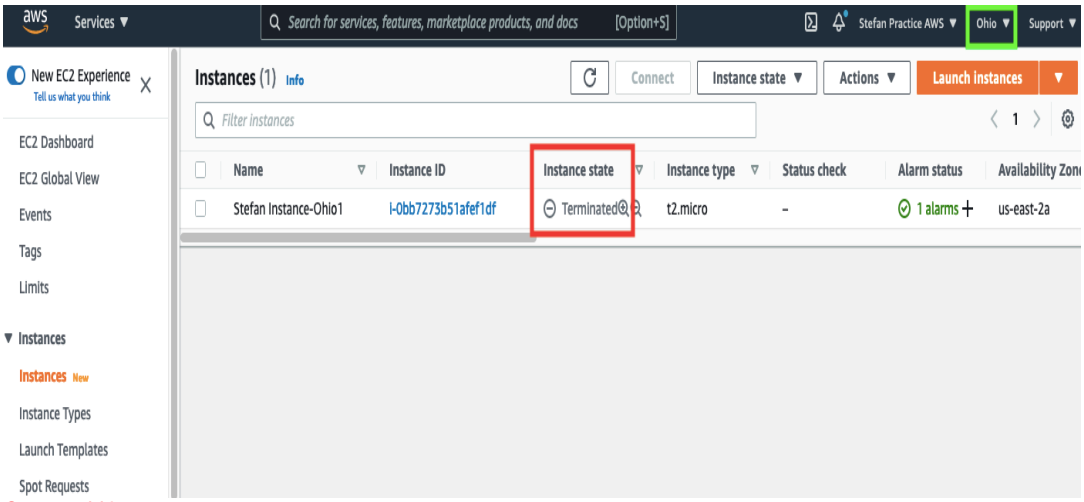
Screen 108

Select you active/running EC2 Instance in Ohio and click ***Terminate Instance*** from screen above. You will see the same confirmation screen as what you saw when you terminated instances in Northern Virginia just confirmed it and refresh your EC2 Dashboard in Ohio and you will see screen below



Screen 109

Notice the running Instance in Ohio is now ZERO! Click the ***Instance*** again and you will see screen 110

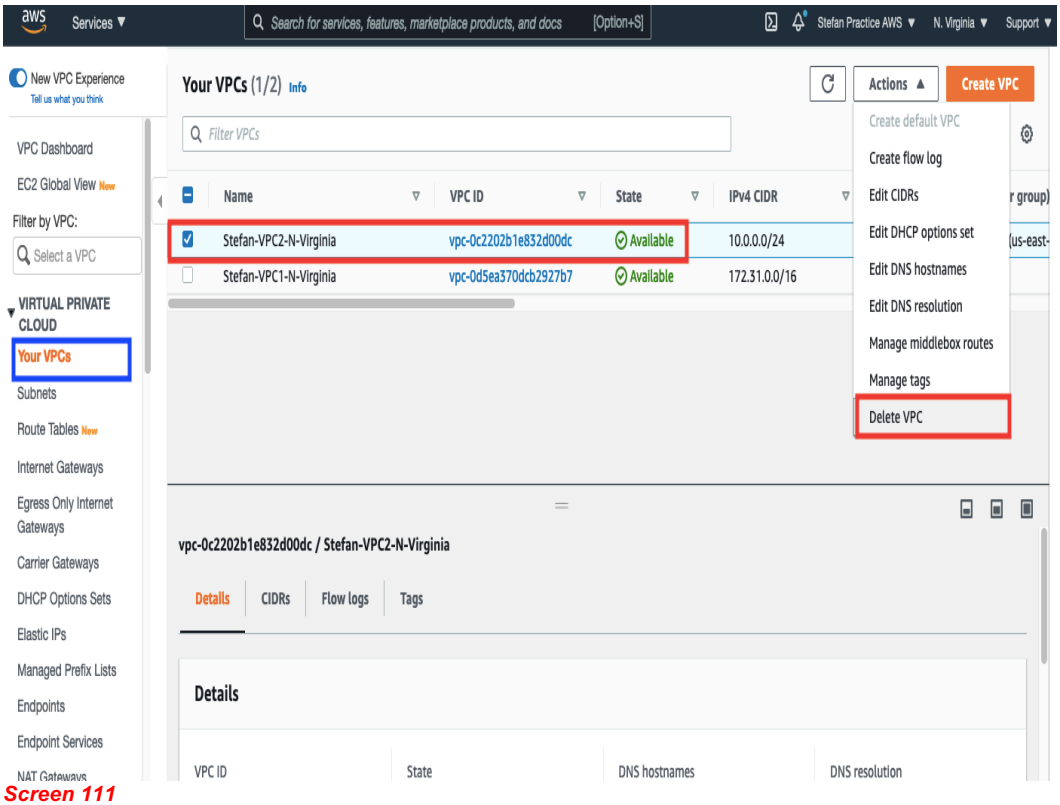


Screen 110

Your EC2 Instance in Ohio has been successfully terminated and you will no longer be changed for any EC Instances since you have no EC2 Instances running (active).

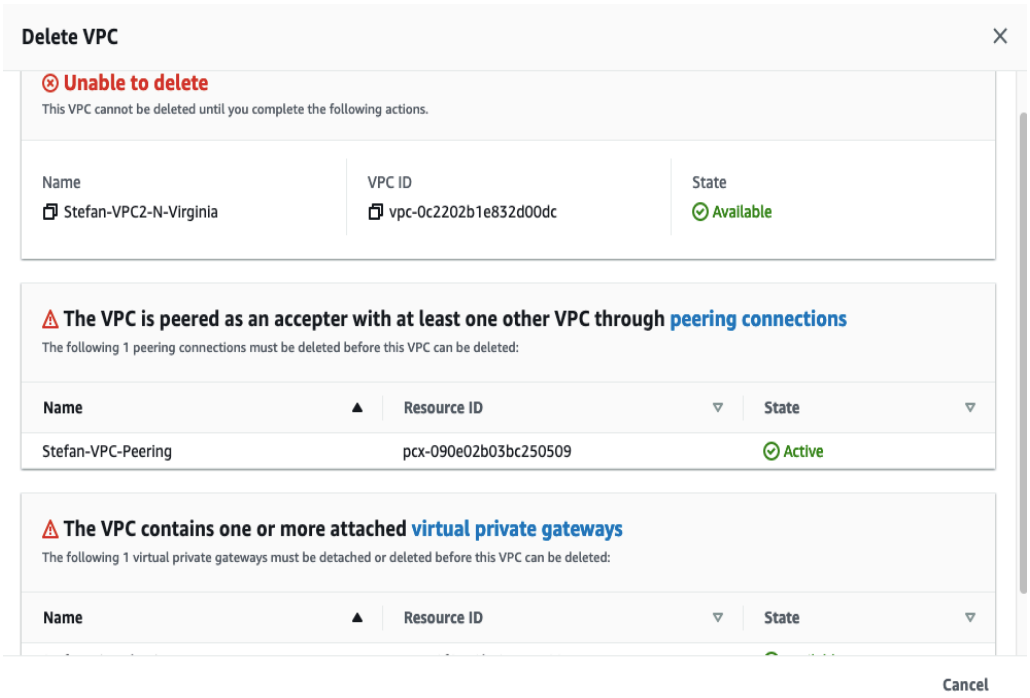
8.2.4 Delete VPCs from your Account

Let's remove VPC from your account so that you will no longer be charged daily. According to the bill you don't have any VPCs in Ohio Region, only in Northern Virginia. Let's go back to Northern Virginia Region and click ***VPC*** from your AWS Console Management, you will see screen below



Screen 111

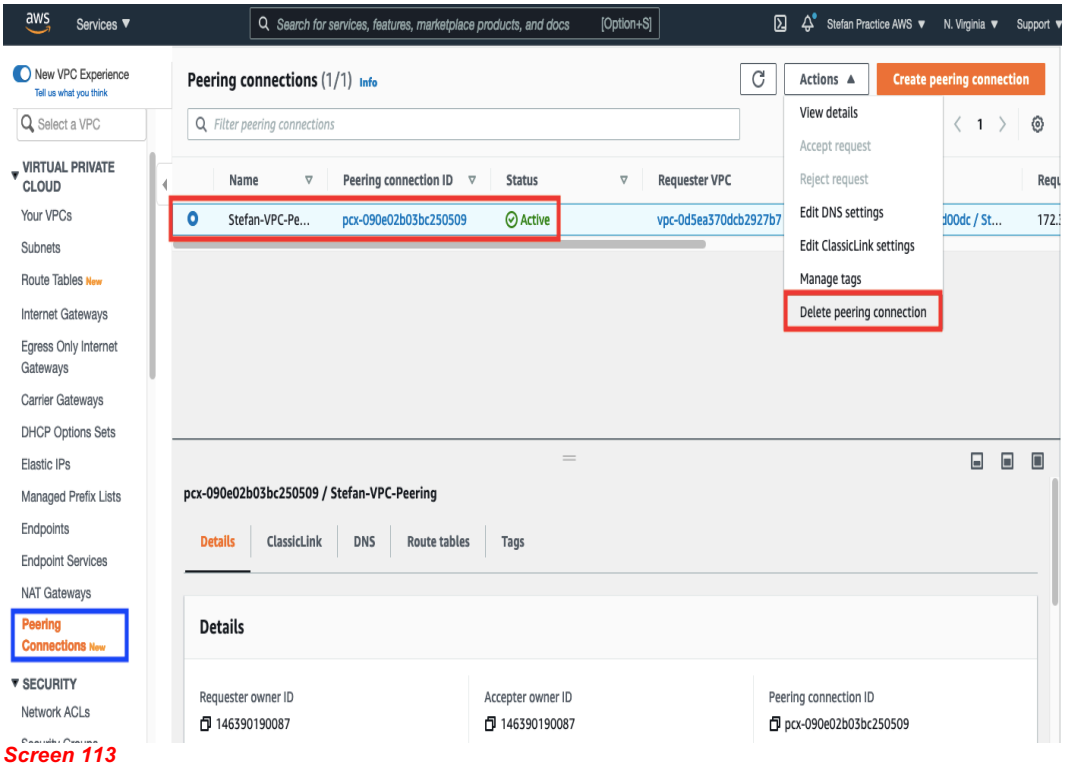
Well, you cannot delete your VPC since you use your VPC for VPC Peering and Virtual Private Gateway



Screen 112

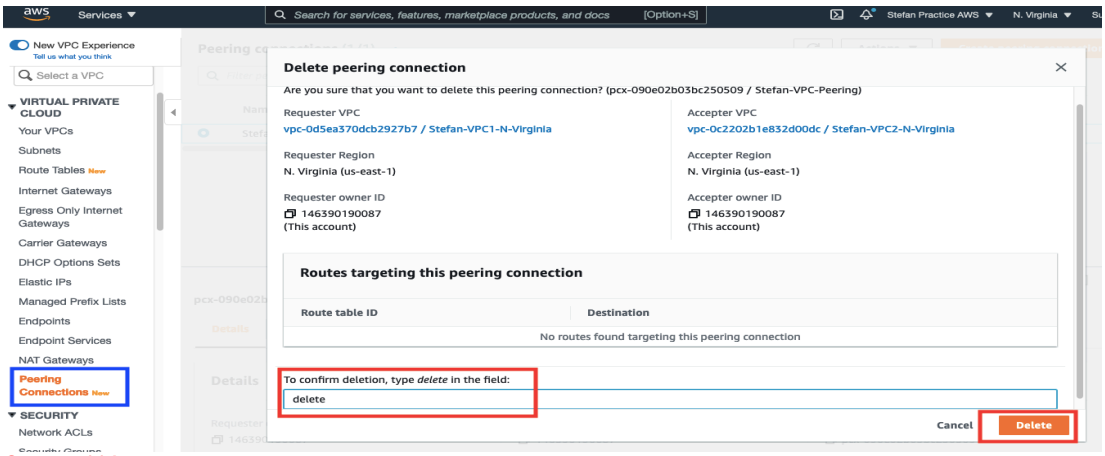
8.2.5 Delete VPC Peering Connection

Click ***Peering Connections*** and you will see screen below



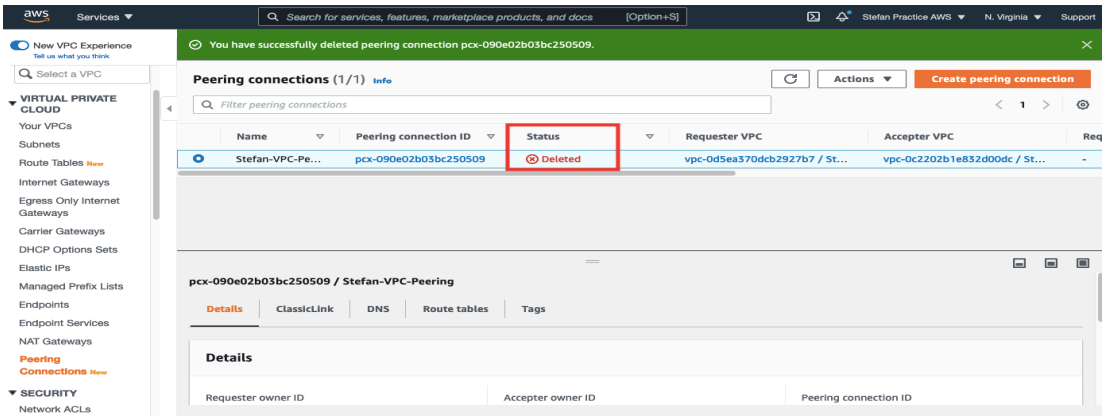
Screen 113

Click Delete Peering Connection from screen above and you will see screen below



Screen 114

Make sure that you type ***Delete*** on the provided column above. Otherwise, the ***Delete*** button won't be enabled. Click ***Delete*** and you will see screen below

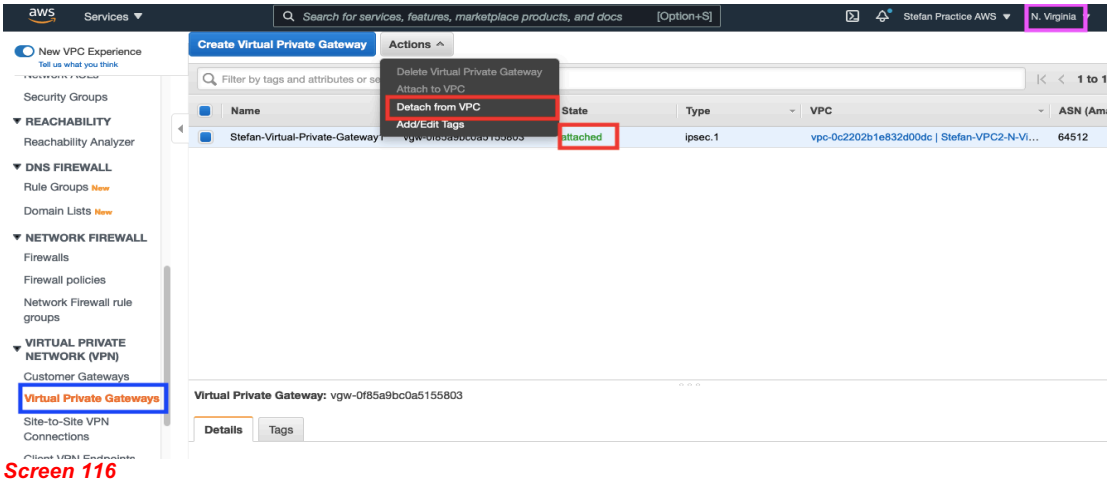


Screen 115

You have successfully deleted a VPC Peering Connection.

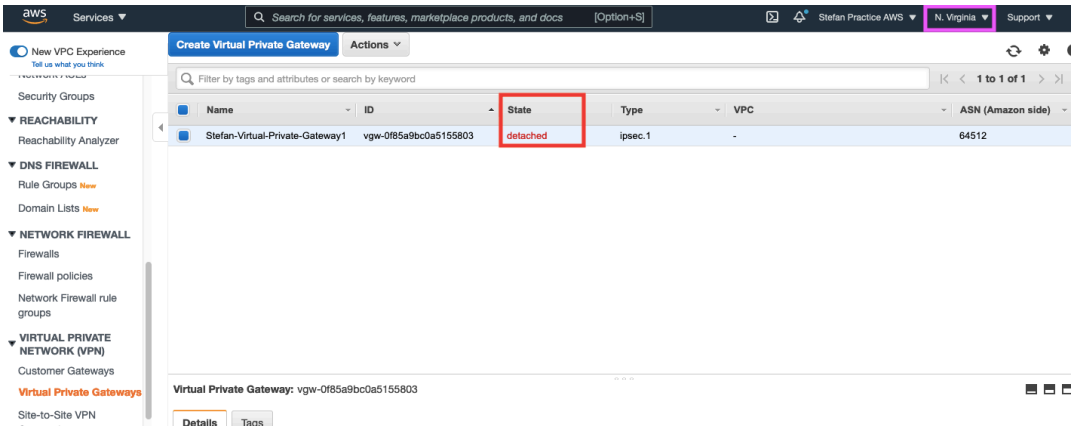
8.2.6 Detach Virtual Private Gateway from VPC

Click Virtual Private Gateways and you will see screen below



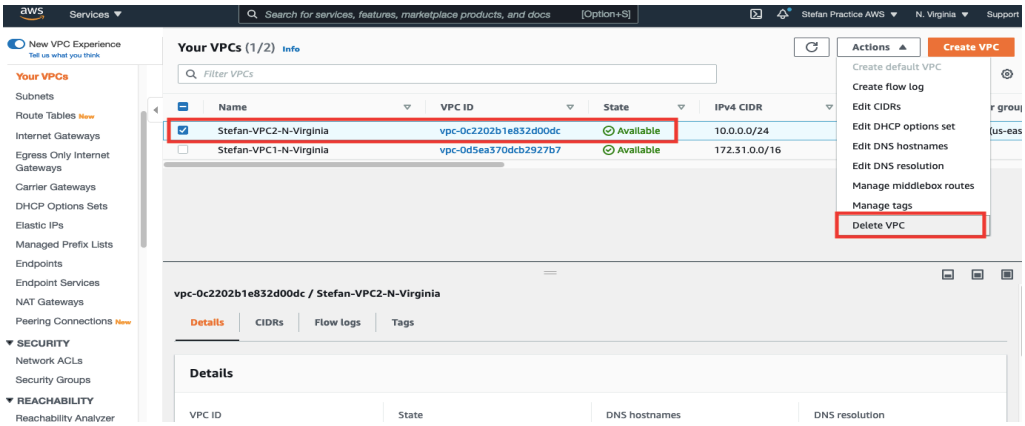
Screen 116

Click Detach from VPC on screen above and a confirmation screen will show up. After confirming, you will see screen below



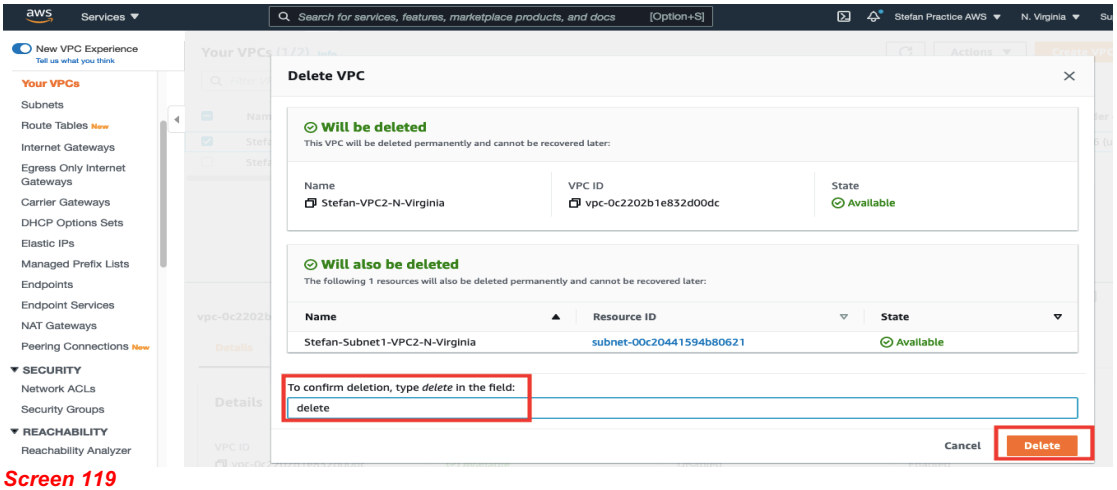
Screen 117

You have successfully detached your Virtual Private Gateway to your VPC. Now you can remove your VPC#2 in Northern Virginia Region



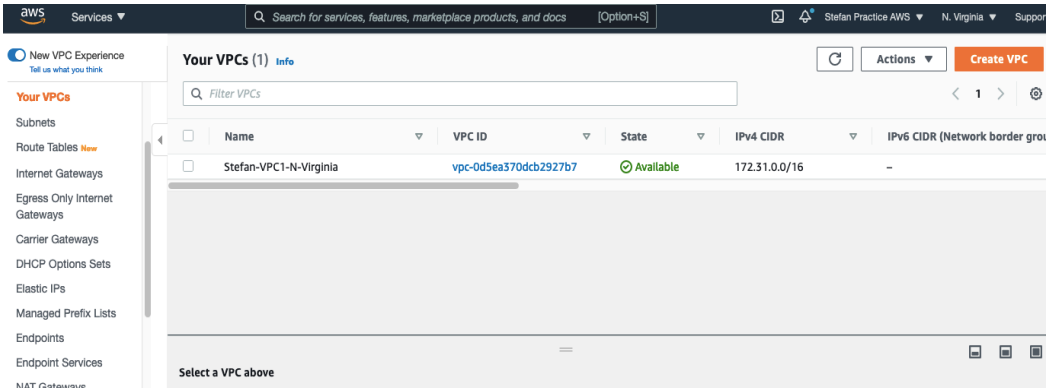
Screen 118

Click ***Delete VPC*** – after clicking ***Delete VPC***, you will see the confirmation screen below.



Screen 119

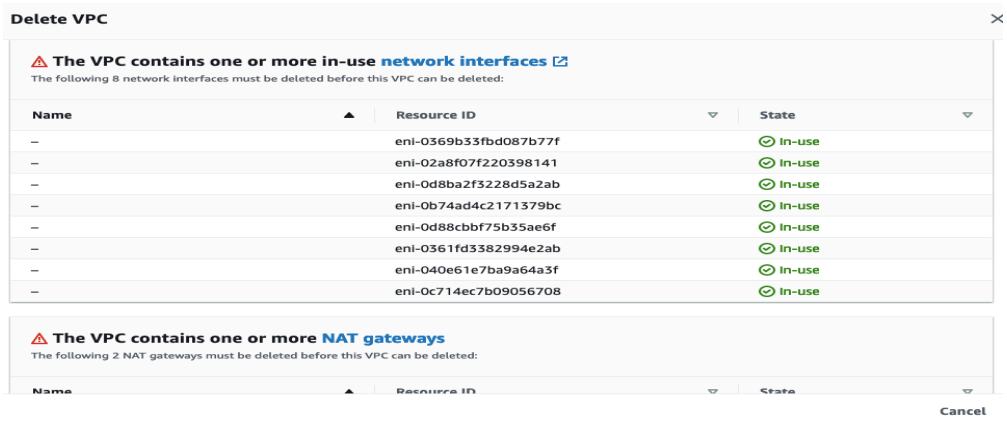
Refresh Your VPCs screen and now you are only seeing 1 VPC is running since you already deleted the other one



Screen 120

Please also delete this ***Stefan-VPC1-N-Virginia*** displayed on screen above. Otherwise, you will continue be billed daily by AWS

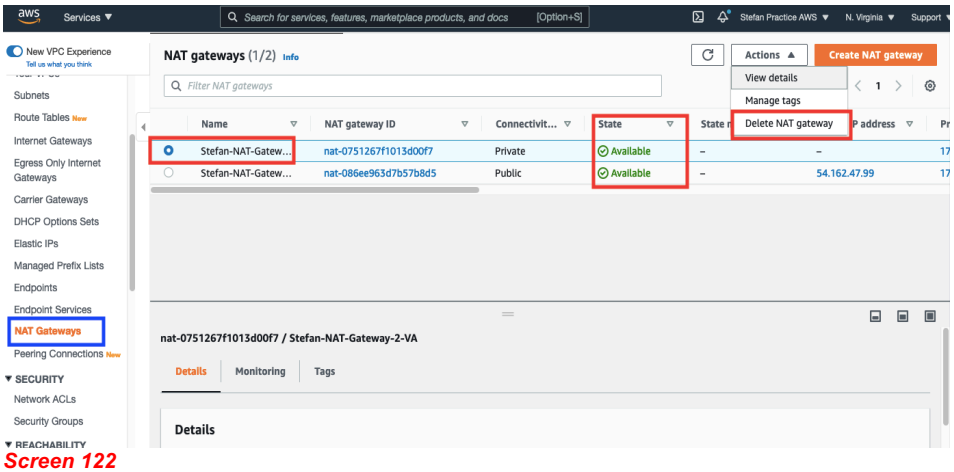
Notification message displayed that you're unable to delete this VPC because of the following dependencies displayed on screen below



Screen 121

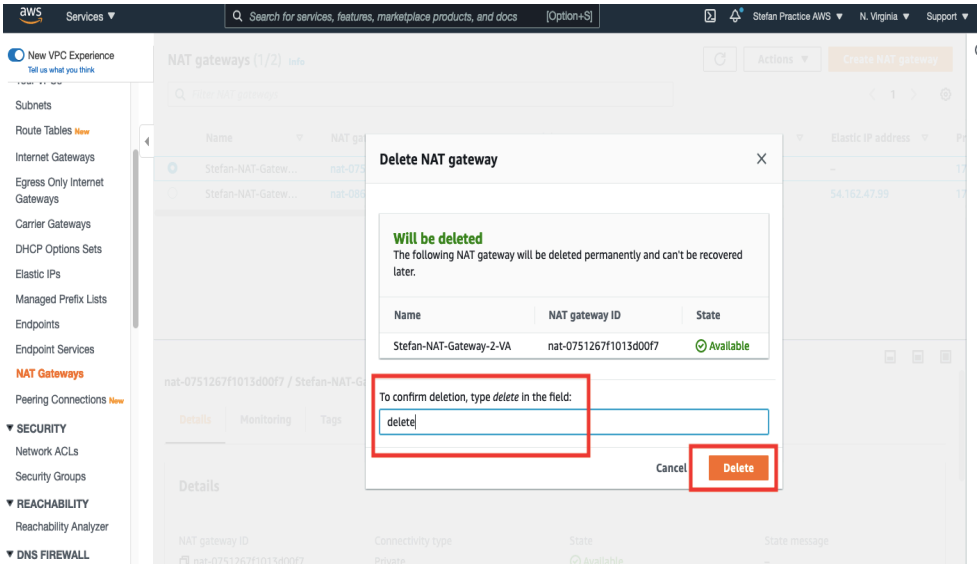
8.2.7 Delete NAT Gateway Connections

Click ***NAT Gateway*** and you will see screen below



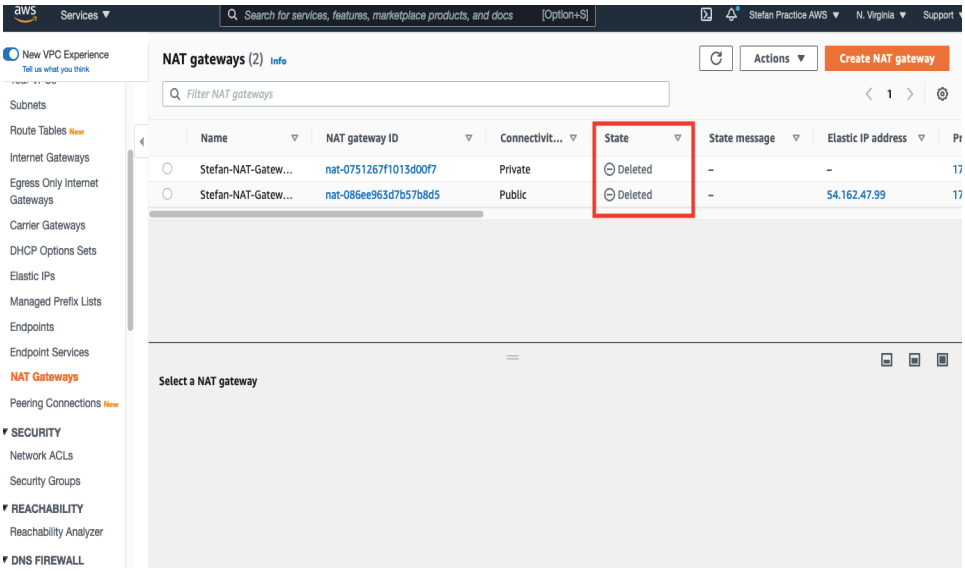
Screen 122

Click ***Delete NAT Gateway*** and you will see screen below



Screen 123

Make sure you type ***Delete*** so that the delete button is enabled. Click ***Delete.*** Please also delete the other NAT Gateway.



Screen 124

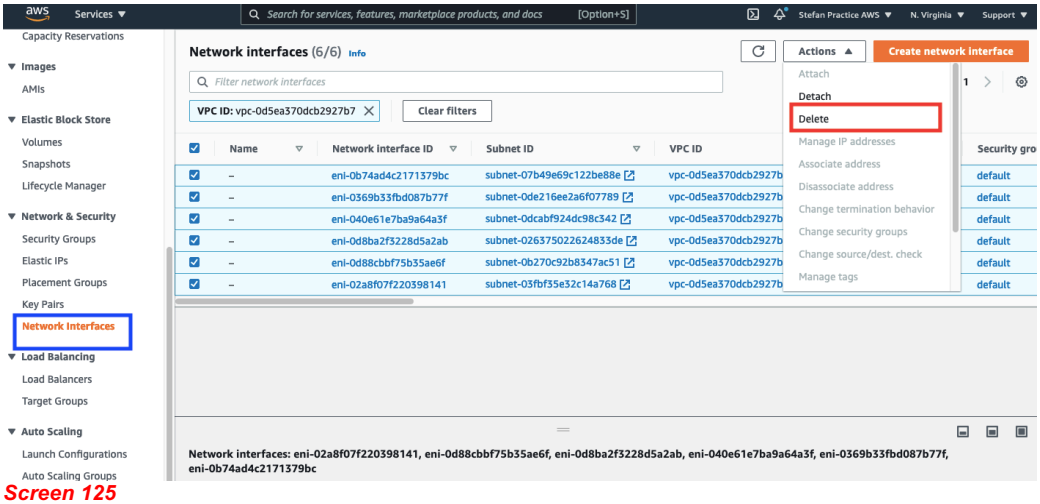
After successfully deleted both NAT Gateways, refresh NAT Gateways screen and you will see screen above. You have successfully deleted both NAT Gateway connections!

8.2.8 Reducing VPC Cost

You can reduce your VPC cost by **removing internet gateway from your network architecture**, avoid incurring cost associated with NAT Gateway access, and maintaining firewalls. What you just did by removing NAT Gateway is reducing VPC Cost.

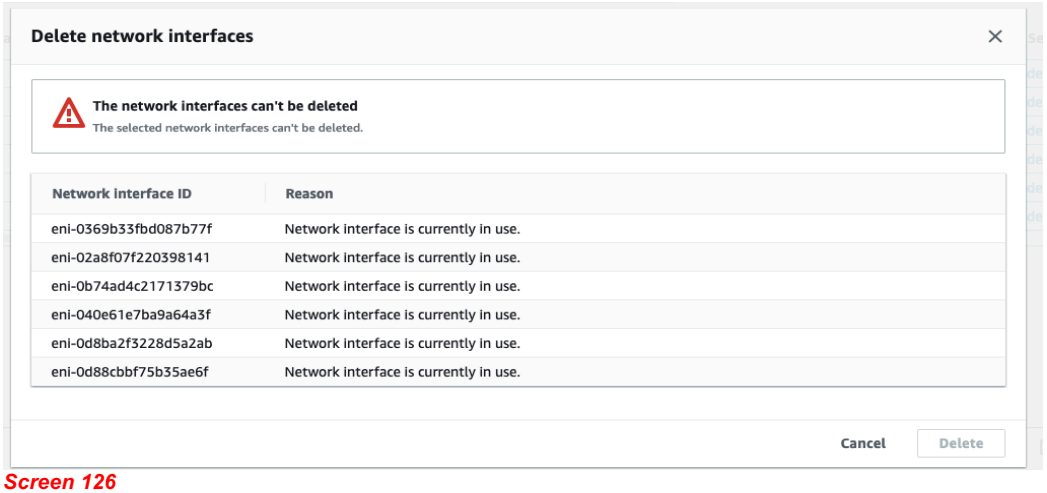
8.2.9 Delete Network Interfaces

Click ***Network Interfaces*** and you will see screen below



Screen 125

Select all network interfaces and click ***Delete*** and you will see screen below

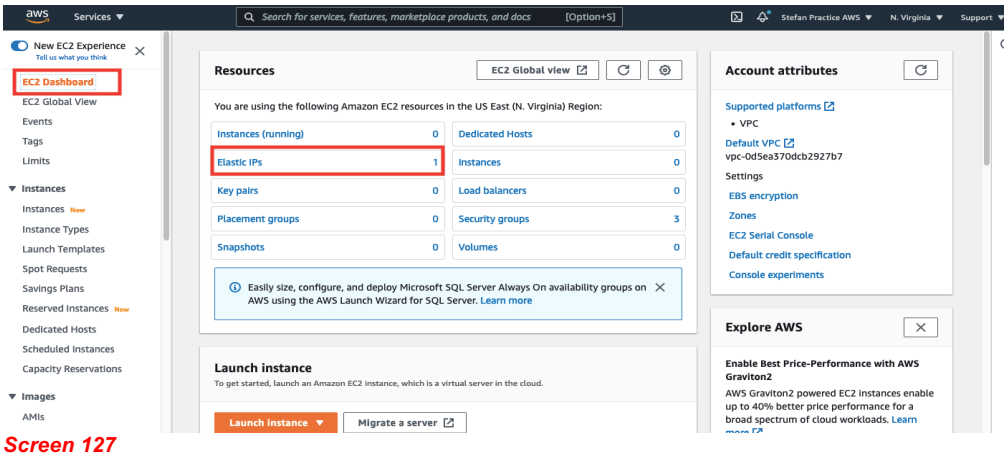


Screen 126

You cannot delete/detach these Network Interfaces since they are currently in use.

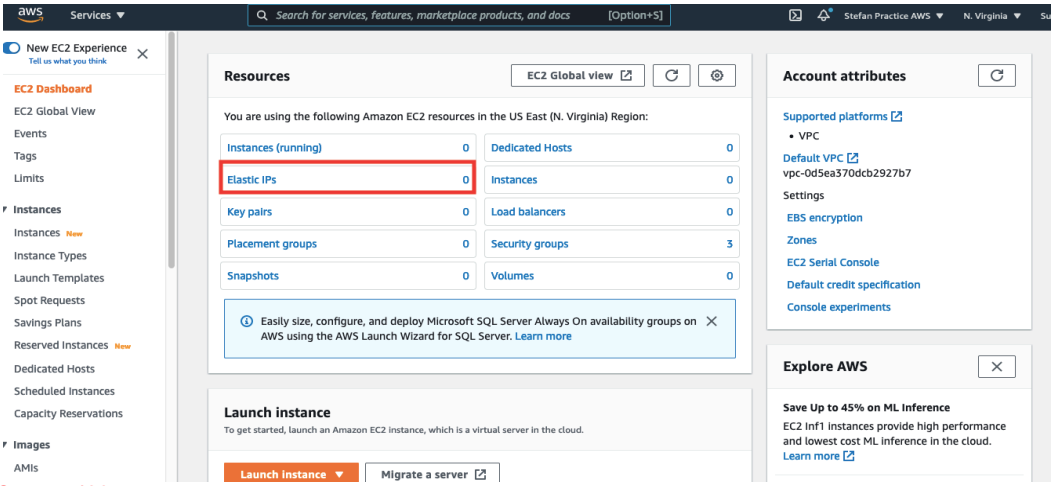
8.2.10 Delete Elastic IP Address (Under EC2)

The reason why you're getting error on screen 117 above is because your Elastic IP is still running, and you need to delete your Elastic IP Address. Go to EC2 Dashboard and you will see screen below.



Screen 127

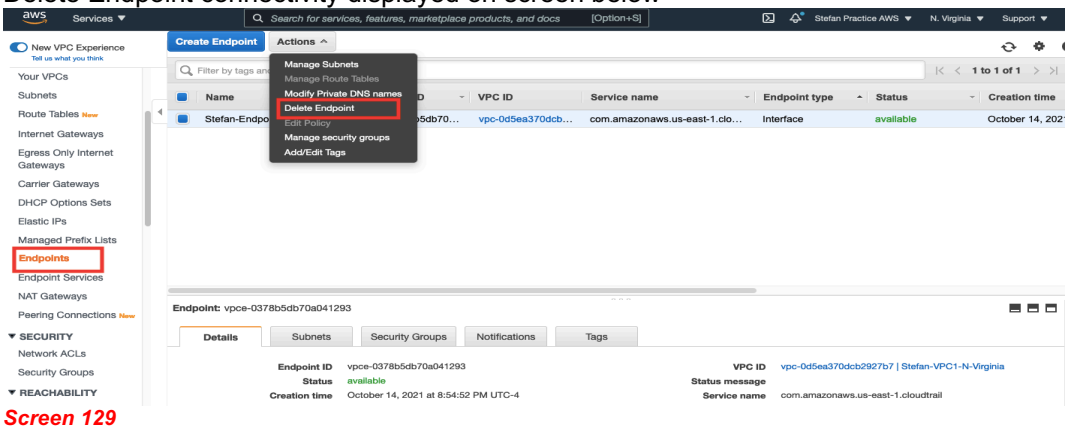
Although your Instances (Running) = ZERO, but you still have one Elastic IP, and you need to ***Release Elastic IP Address*** and after you've successfully done it, go back to EC2 Dashboard screen and you will see screen below showing Elastic Ips = ZERO



Screen 128

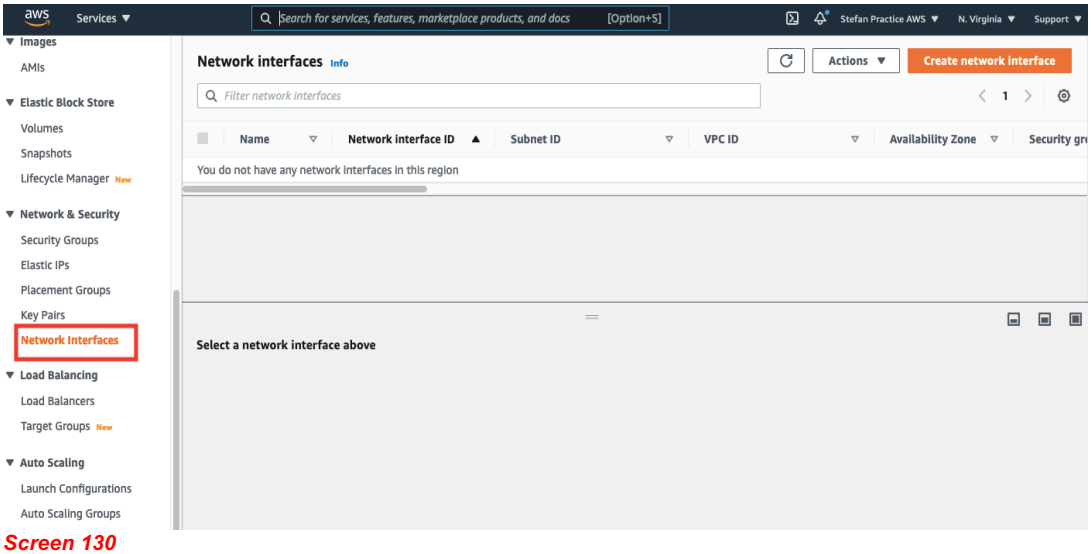
8.2.11 Delete Endpoint Connectivity

Delete Endpoint connectivity displayed on screen below



Screen 129

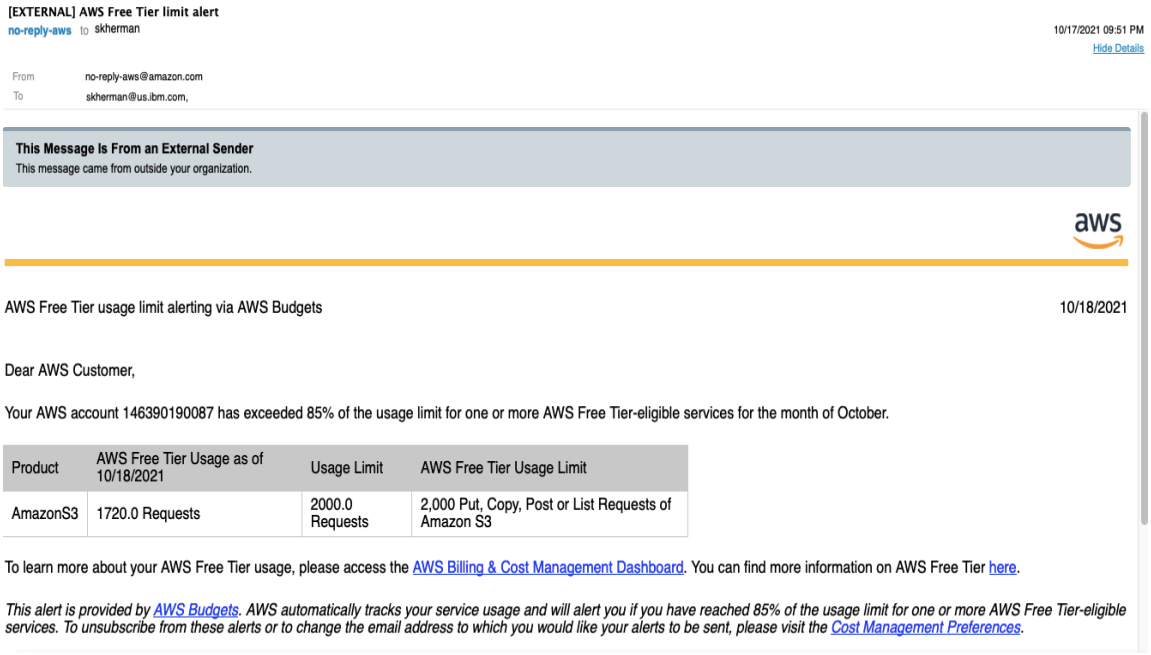
Go back to Network Interfaces screen again and you will see that you have no longer any network interfaces in your Northern Virginia region displayed on screen below



Screen 130

8.2.21 AWS Budget Email Notification (Threshold reached)

If you've set up your threshold to notify you when AWS reached a certain threshold you've defined, you will be receiving email alert displayed on screen below



[EXTERNAL] AWS Free Tier limit alert

no-reply-aws to skherman 10/17/2021 09:51 PM

Hide Details

From no-reply-aws@amazon.com

To skherman@us.ibm.com,

This Message Is From an External Sender

This message came from outside your organization.

aws

AWS Free Tier usage limit alerting via AWS Budgets 10/18/2021

Dear AWS Customer,

Your AWS account 146390190087 has exceeded 85% of the usage limit for one or more AWS Free Tier-eligible services for the month of October.

Product	AWS Free Tier Usage as of 10/18/2021	Usage Limit	AWS Free Tier Usage Limit
AmazonS3	1720.0 Requests	2000.0 Requests	2,000 Put, Copy, Post or List Requests of Amazon S3

To learn more about your AWS Free Tier usage, please access the AWS Billing & Cost Management Dashboard. You can find more information on AWS Free Tier here.

This alert is provided by AWS Budgets. AWS automatically tracks your service usage and will alert you if you have reached 85% of the usage limit for one or more AWS Free Tier-eligible services. To unsubscribe from these alerts or to change the email address to which you would like your alerts to be sent, please visit the Cost Management Preferences.

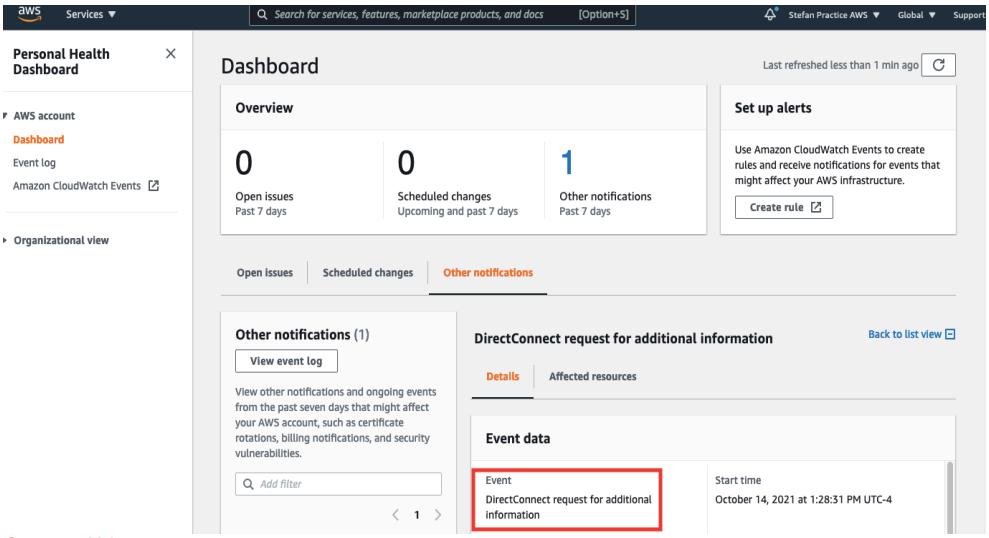
Screen 131

8.3 AWS Health Dashboard

8.3.1 AWS Personal Health Dashboard

It's available in **ALL** support plan for FREE. It provides alerts and remediation guidance when AWS is experiencing events that may impact you. It gives you personalized view of the status of AWS services that are part of your cloud architecture so that you can quickly assess the impact on your business when AWS services have issues. Provides alerts & guidance for AWS events that might affect your environment.

At AWS Management Console click Personal Health Dashboard & you will see screen below.



aws Services Search for services, features, marketplace products, and docs [Option+S] Stefan Practice AWS Global Support

Personal Health Dashboard

AWS account

Dashboard

Event log

Amazon CloudWatch Events

Organizational view

Dashboard

Last refreshed less than 1 min ago

Overview

0 Open issues Past 7 days

0 Scheduled changes Upcoming and past 7 days

1 Other notifications Past 7 days

Set up alerts

Use Amazon CloudWatch Events to create rules and receive notifications for events that might affect your AWS infrastructure.

Create rule

Open issues | Scheduled changes | Other notifications

Other notifications (1)

View event log

View other notifications and ongoing events from the past seven days that might affect your AWS account, such as certificate rotations, billing notifications, and security vulnerabilities.

Add filter

1

DirectConnect request for additional information

Back to list view

Details | Affected resources

Event data

Event

DirectConnect request for additional information

Start time

October 14, 2021 at 1:28:31 PM UTC-4

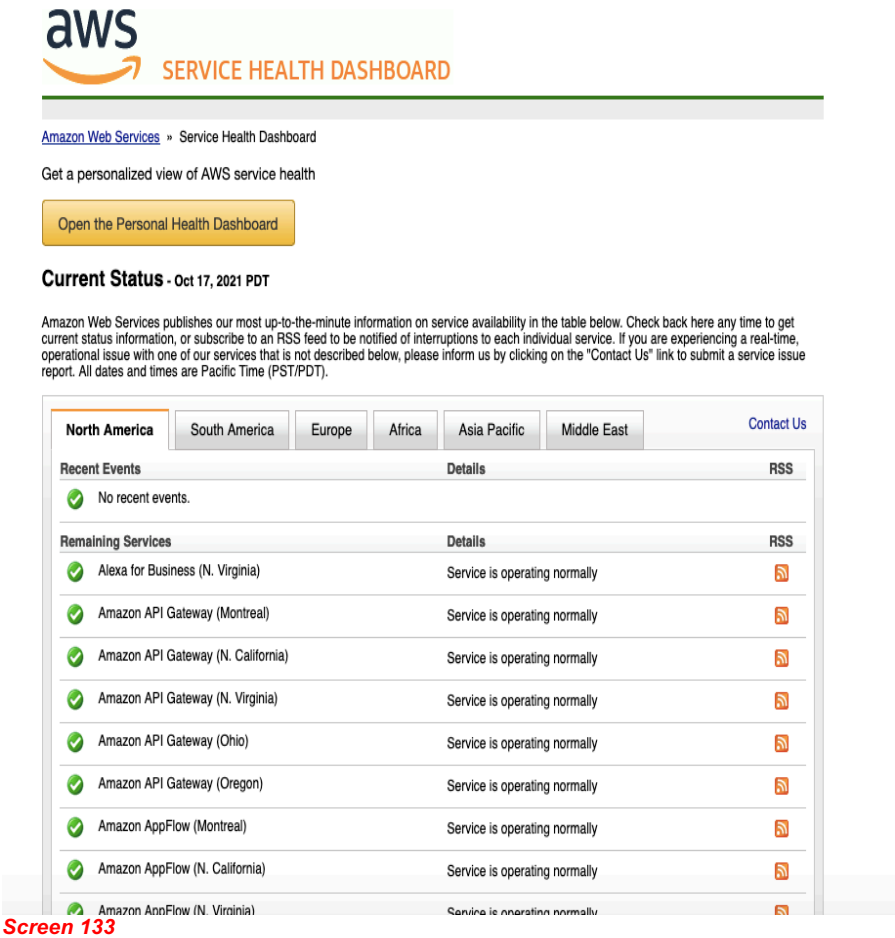
Screen 132

AWS Personal Health Dashboard reminds you that you need to provide more info about Direct Connect that you ordered few days ago and failure to provide additional info to AWS might affect your environment.

8.3.2 AWS Service Health Dashboard

It publishes up to the minute info on general status – general statistic of all AWS Services. It also provides status of history – log all services interruptions across the AWS Network & Resources of incidents persistent for a year.

Screen below displays General status of all AWS Services



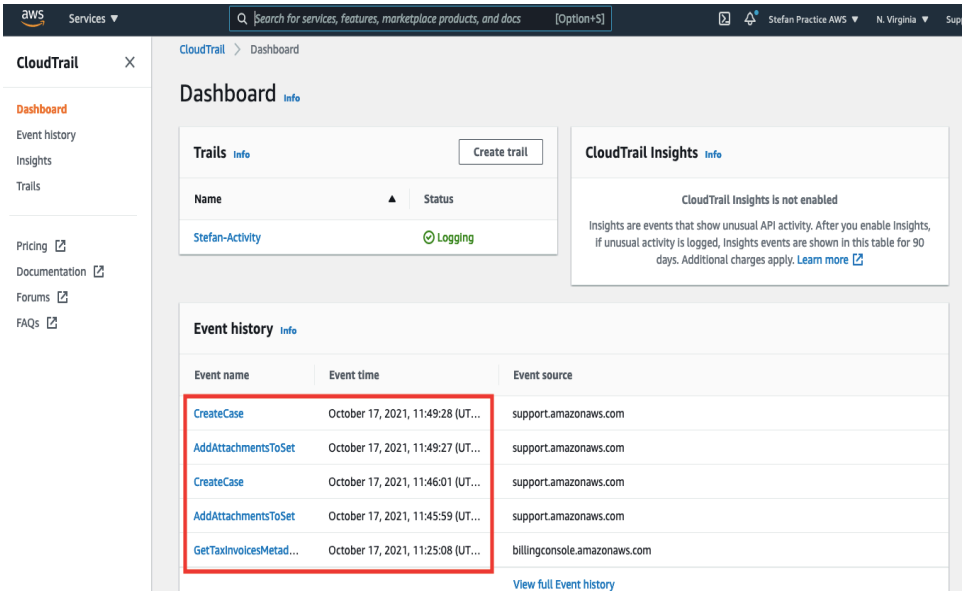
Screen 133

8.4 AWS CloudTrail and AWS CloudWatch

8.4.1 AWS CloudTrail

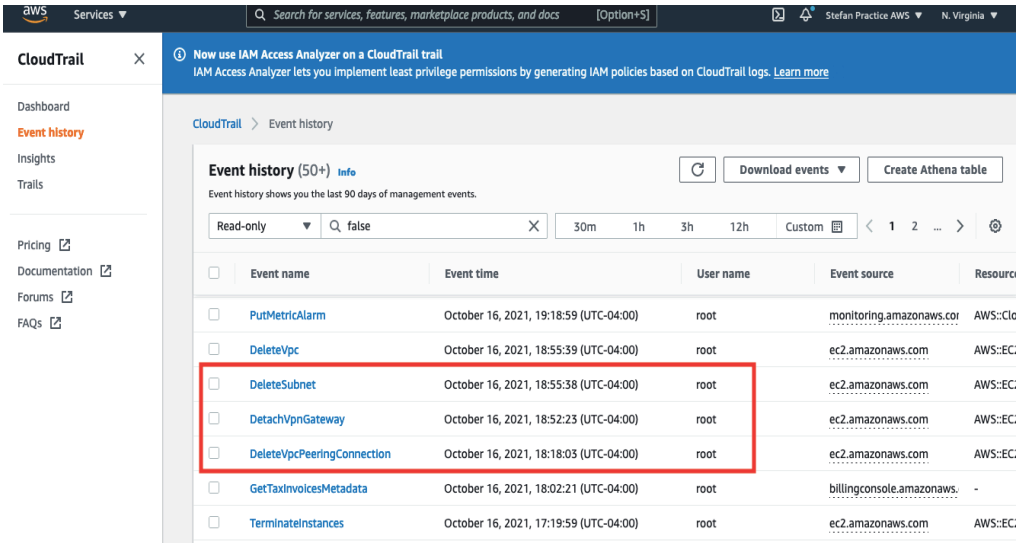
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

CloudTrail is enabled on your AWS account when you create it. It answers the question on who did what on your AWS Cloud. CloudTrail Log is encrypted by default.



Screen 134

Screen above displays AWS CloudTrail captures all activities that you performed. For example, you have just opened case to AWS support help asking about your billing inquiry and you can see it is being captured on your CloudTrail above. More on CloudTrail, it also captured the activities that you performed last night, the deletions of VPCs, Subnet, VPN Gateway and VPC Peering



Screen 135

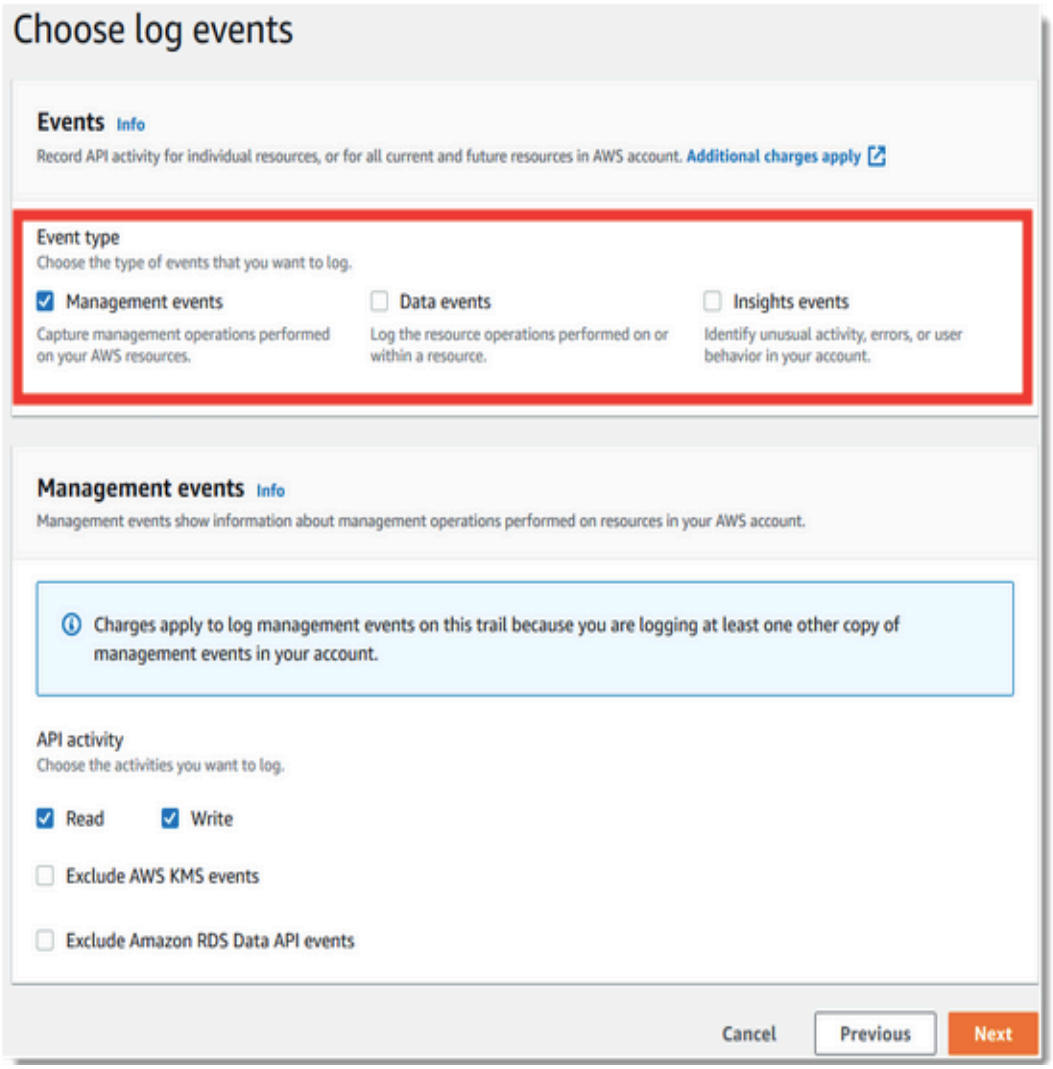
Keep in mind that an event in CloudTrail is the record of an activity in AWS account. This activity can be an action taken by a user, role, or service that is monitorable by CloudTrail. CloudTrail events provide a history of both API and non-API account activity made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

There are three types of events that can be logged in CloudTrail

- Management events
- Data events
- CloudTrail Insights events.

By default, CloudTrail logs all management events and does not include data events or Insights events. Additional charges apply for data and Insights events. All event types use the same CloudTrail JSON log format.

Please refer to screen below and you will see all those 3 events on CloudTrail and Management Event is a default.



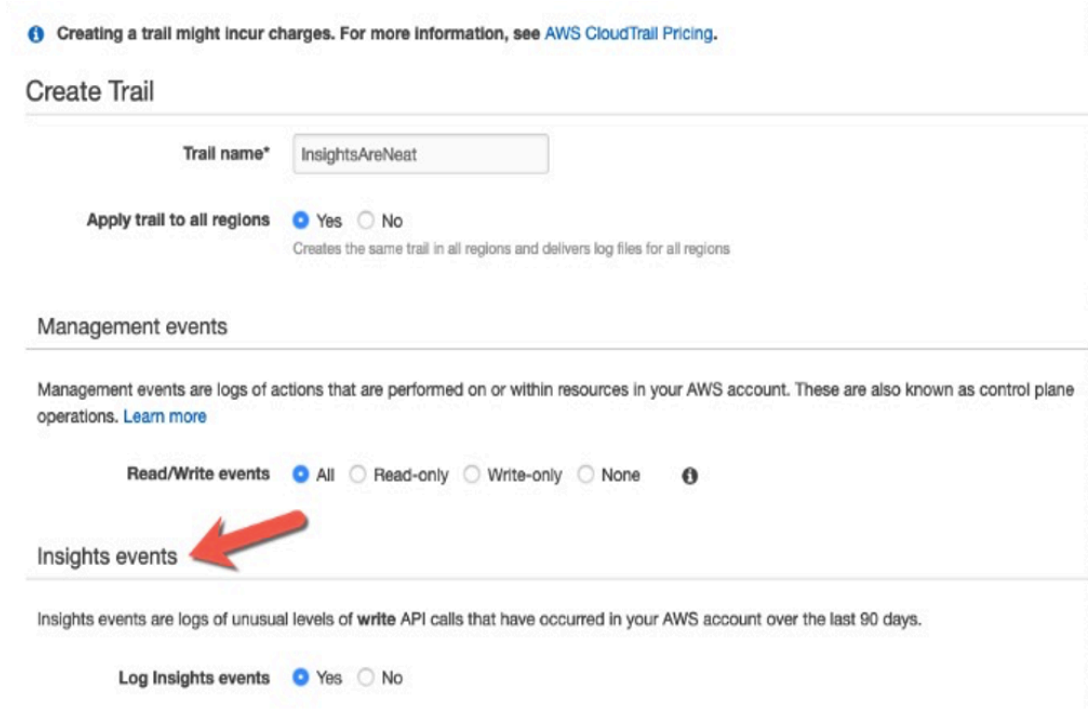
Screen 136

8.4.2 AWS CloudTrail Insight

AWS CloudTrail Insights is designed to automatically analyze management events from your CloudTrail trails to establish a baseline for normal behavior, and then raise issues by generating Insights events when it detects unusual patterns.

AWS CloudTrail	***AWS CloudTrail Insight***
CloudTrail tracks user activity and API usage. It provides an event history of AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, CLI, and other AWS Services	*You can enable Machine Learning models that detect unusual activity in these logs with just a few clicks. It will analyze historical API calls and identify usage patterns and generate Insight Events for unusual activity*

Screen 137



Screen 138

AWS CloudTrail Insights helps AWS users identify and respond to unusual activity associated with write API calls by continuously analyzing CloudTrail management events.

Insights events are logged when CloudTrail detects unusual write management API activity in your account. If you have CloudTrail Insights enabled, and CloudTrail detects unusual activity, Insights events are delivered to the destination S3 bucket for your trail.

CloudTrail Insights can help you detect unusual API activity in your AWS account by raising Insights events.

CloudTrail Insights measures your normal patterns of API call volume, also called the baseline, and generates Insights events when the volume is outside normal patterns.

CloudTrail Insights continuously monitors CloudTrail write management events and uses mathematical models to determine the normal levels of API and service event activity for an account.

8.4.3 AWS CloudWatch (Dashboard, Alarm & CloudWatch Log)

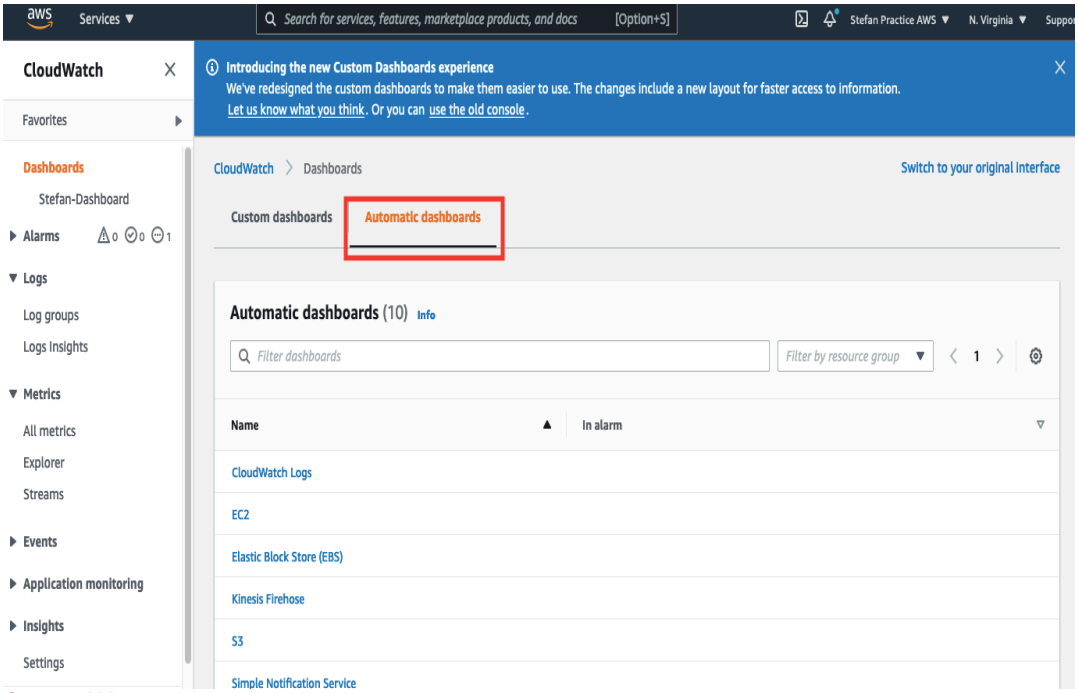
Amazon CloudWatch is **basically a metrics repository**. An AWS service—such as Amazon EC2—puts metrics into the repository, and you retrieve statistics based on those metrics. You can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met.

If you need to know on what's happening with AWS Resources (Health & Performance), optimize resource utilization.

It enables you to centralize the logs from all your system, applications, and AWS services that you use in a single highly scalable service.

It provides billing alarms to monitor estimated charges – resources utilization & application performance.

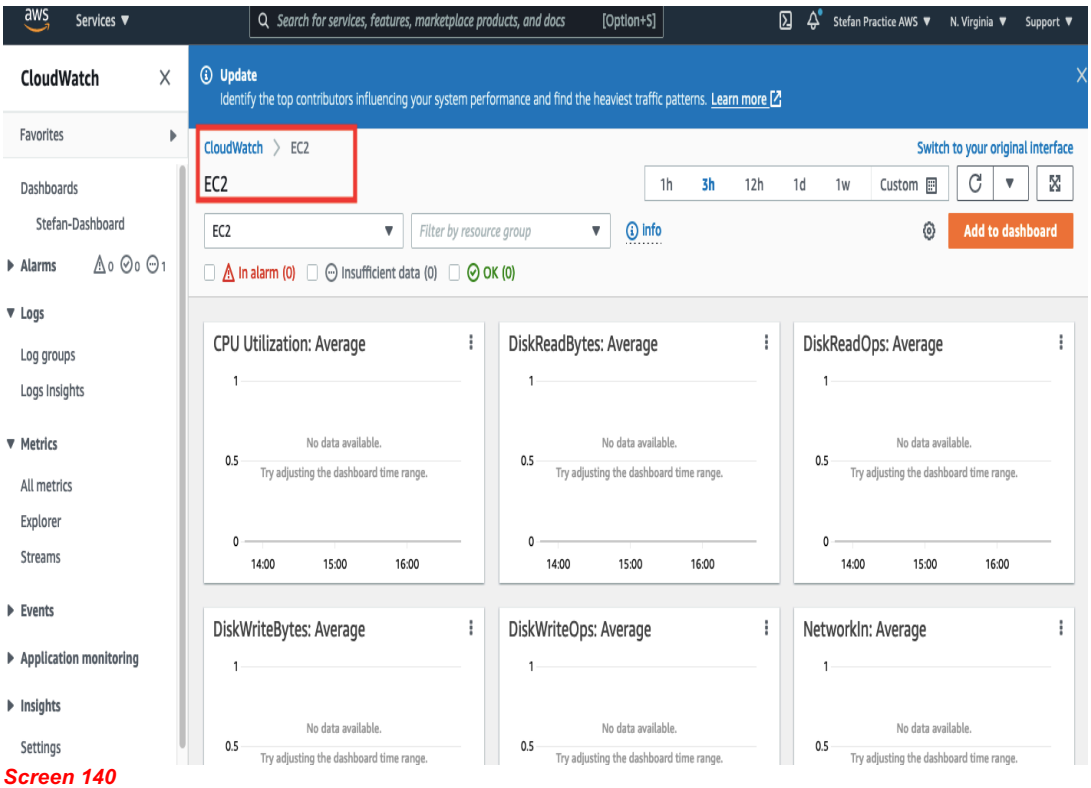
Click ***CloudWatch*** from AWS Console Management and you will see screen below



Screen 139

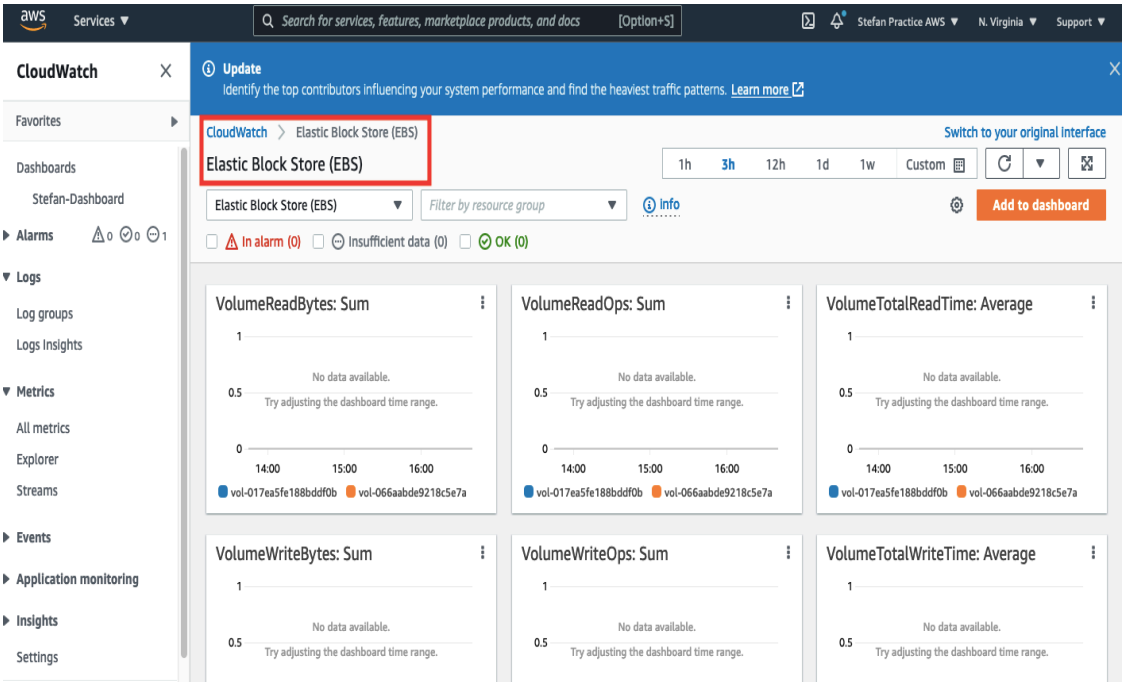
You can have Custom Dashboards or Automatic Dashboards. Click Automatic Dashboards tab and you will see screen above

If you want to know anything about EC2 *(what's happening with EC2, regarding its health & performance)*, just click EC2 and you will see screen below



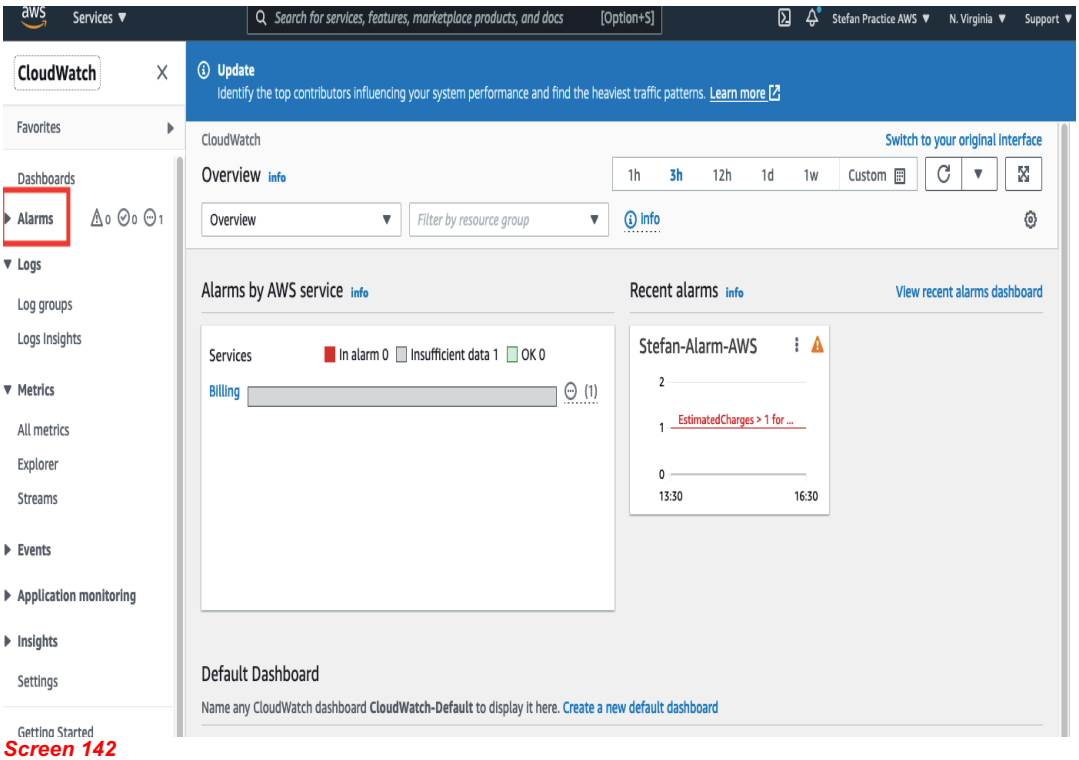
Screen 140

If you want to know anything about EBS *(what's happening with EBS, regarding its health & performance)*, just click EBS and you will see screen below



Screen 141

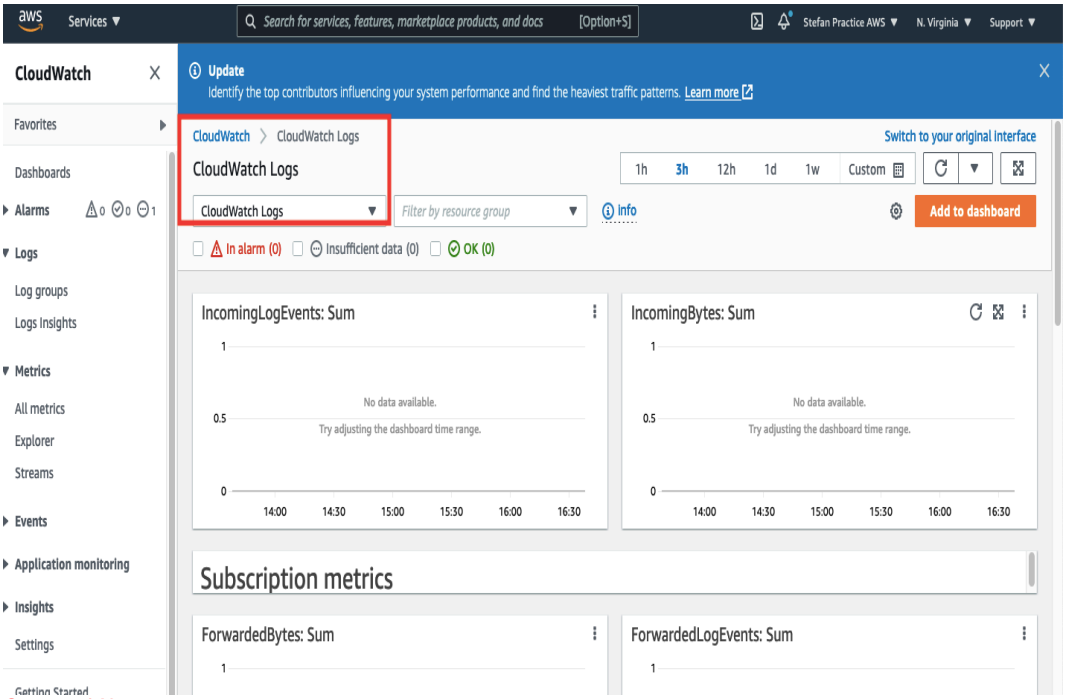
If can also activate alarm on CloudWatch, just click ***Alarms*** and you will see screen below



Screen 142

You can also check the CloudWatch Log displayed on screen below:
AWS CloudWatch Log

- It monitors, stores, and accesses your log file from EC2 instances, AWS CloudTrail, Route 53
- Enables you to centralize the logs from all your system, applications and AWS Services that you use in a single highly scalable service

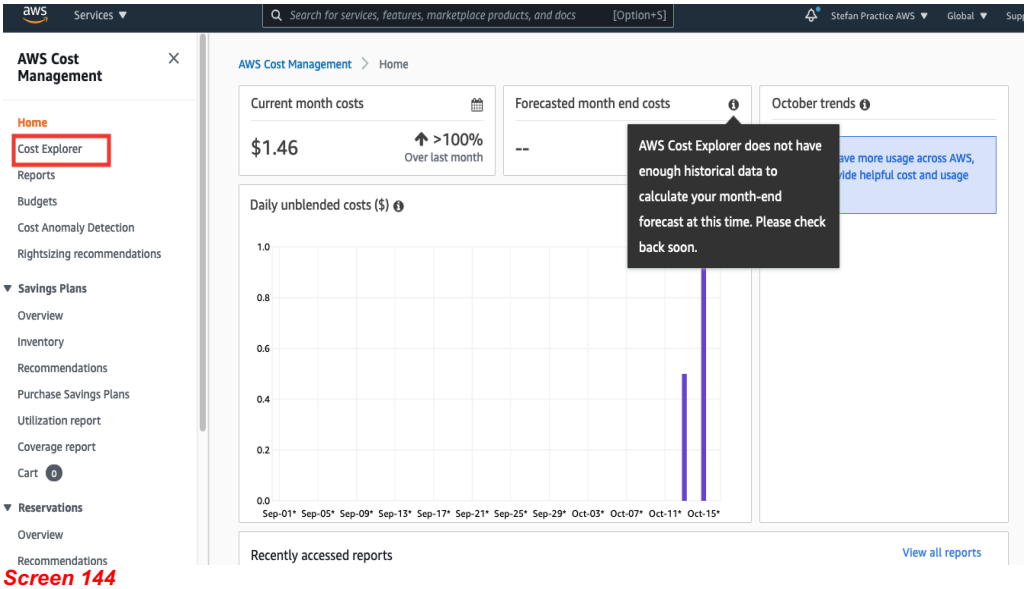


Screen 143

8.5 AWS Cost Explorer

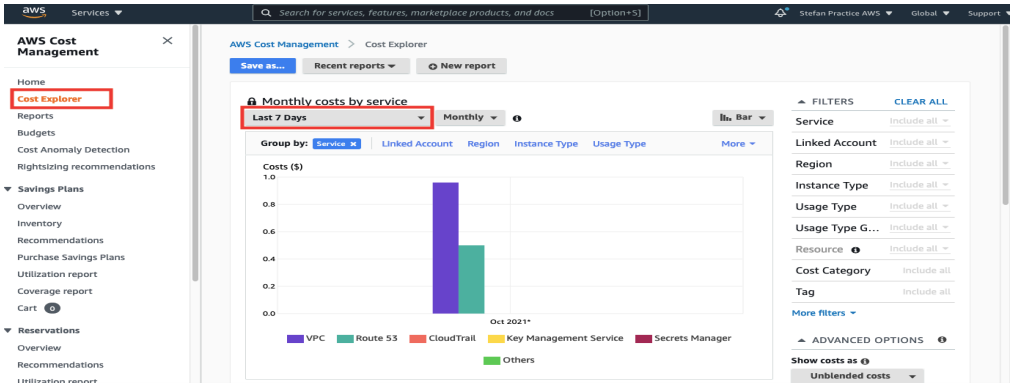
It is used to visualize usage over time, understand & manage your AWS Cost & Usage over time. It helps forecast your next bill prediction on how much you will use AWS service over forecast time-period. It's also able to provide historical data (12 months back) & forecast data (12 months in the future).

AWS Cost Explorer also able to provide optimal saving plan recommendation. From AWS Cost Management, click ***Cost Explorer*** and you will see screen below. Please note currently it is not able to provide you with the forecast since it doesn't have enough data to analyze since this AWS account has just created 3 days ago *(today is 10/15/2021)*.



Screen 144

You can customize your AWS Cost Explorer and you will see screen below



Screen 145

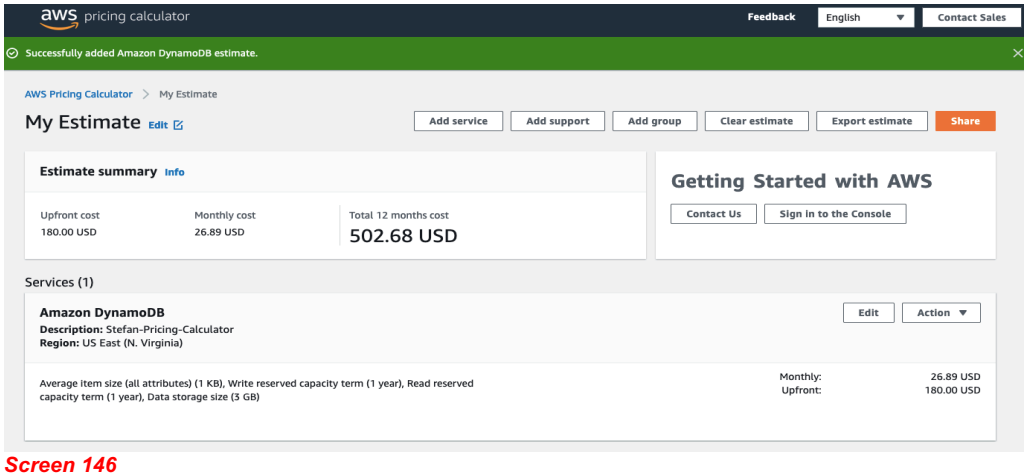
Please note you can customize your report by daily, monthly, quarterly. Screen above displays Last 7 days activity.

AWS Cost Explorer can be used for:

- *Visualize usage over time, understand & manage your AWS Cost & Usage overtime*
- *Provide historical data (12 months back) & Forecast data (12 months in the future)*
- *Monitor cost on the AWS Cloud & able to provide an optimal Savings Plan*
- *Forecast your AWS account usage and costs*
- *Help you with costs & usage may look like in the future*

8.6 AWS Pricing Calculator/Simple Monthly Calculator

Please note that as of 10/15/2021, there is no more AWS Simple Monthly Calculator. It has been replaced by AWS Pricing Calculator.

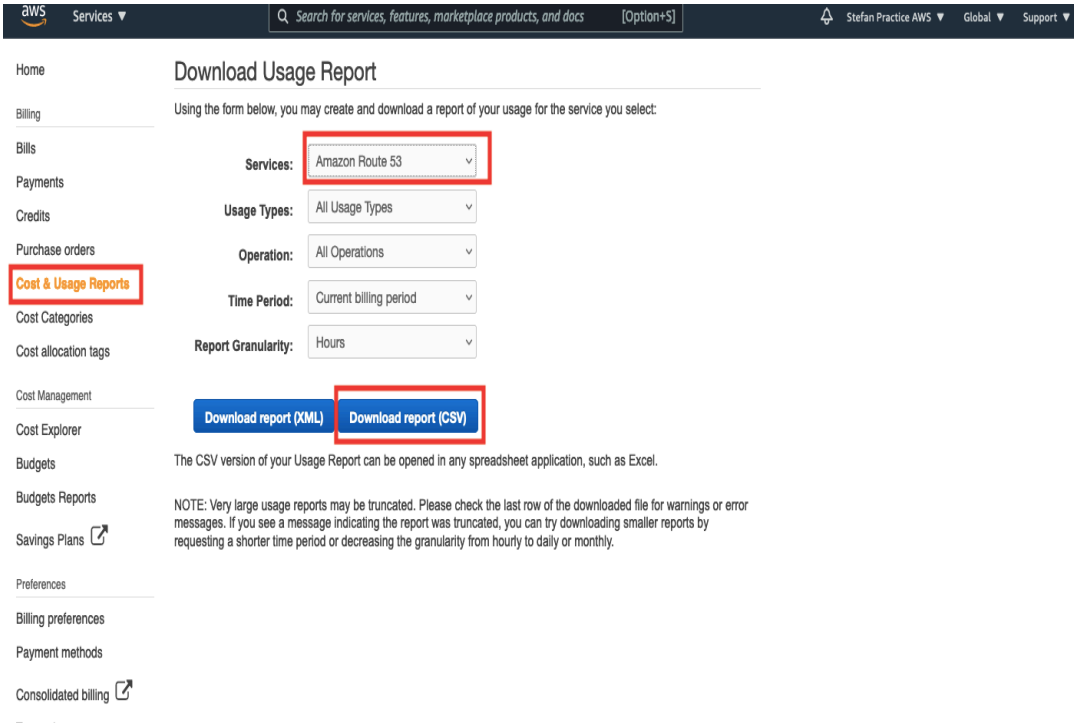


Screen 146

AWS Pricing Calculator explores AWS service and create an estimate for the cost of your use cases on AWS. It also estimates the monthly costs of AWS services for your use case based on your expected usage. Screen above gives you the monthly & yearly estimated cost for DynamoDB.

8.7 AWS Cost and Usage Report

It can provide reports that breakdown your cost by the hour into your S3 bucket. This is the most detailed cost and usage data on your AWS account. It can generate granular reports in CSV format. Click Cost & Usage Reports and you will see screen 140. You know that you are currently being charged for Amazon Route 53. Hence, select Amazon Route 53 on screen below and you can download it as XML or CSV.



Screen 147

Let's download it as CSV and you will see screen below and you can see exactly the detailed charge of the service that you used on that day

	A	B	C	D	E	F	G	H
1	Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue	
2	AmazonRoute53	HostedZone	HostedZone	arn:aws:route53:::hostedzone/Z03786043J297PISCIZ69	10/13/21 13:00	10/13/21 14:00	1	
3								
4								
5								

Screen 148

8.8 AWS Total Cost of Ownership (TCO) Calculator

AWS Pricing Calculator allows **you to explore AWS services based on your use cases and create a cost estimate**.

You can model your solutions before building them, explore the price points and calculations behind your estimate, and find the available instance types and contract terms that meet your needs.

9 AWS Storage Services

9.1 Object Storage

Object storage provides a very high level of durability, with high availability and high performance. The main advantage of object storage is that you can group devices into large storage pools and distribute those pools across multiple locations.

This not only allows unlimited scale, but also improves resilience and high availability of the data

Benefits of Object storage:

- Scalability
- Faster Data Retrieval and Better Recovery
- Fewer Limitation
- Cost Effectiveness

9.1.1 Object Storage – S3 Standard

It's for frequent access data (Active data) and it's not suitable for data archival. It stores data in Flat nonhierarchical structure – *refer to section 9.1.8 for detail comparison with other S3 Object Storages.*

9.1.2 Object Storage – S3 Intelligent Tier

It works by storing objects in two access tiers:

- One tier is optimized for frequent access
- Another lower-cost tier is optimized for infrequent access

Refer to section 9.1.8 for detail comparison with other S3 Object Storages.

9.1.3 Object Storage – S3 Standard – IA

For data that is access less frequently but requires rapid access when needed. It's ideal for long-term storage.

Refer to section 9.1.8 for detail comparison with other S3 Object Storages.

9.1.4 Object Storage – S3 One Zone – IA

For data that is access less frequently but requires rapid access when needed. Keep in mind that S3 One Zone – IA is NOT suitable for data archival since data only stored in One Availability Zone.

Refer to section 9.1.8 for detail comparison with other S3 Object Storages.

9.1.5 Object Storage – S3 Glacier

For data archiving and long-term backup – infrequent access (Cold Data). *Refer to section 9.1.8 for detail comparison with other S3 Object Storages.*

9.1.6 Object Storage – S3 Glacier Deep Archive

For data archiving and long-term backup – infrequent access (Cold Data). Most time to retrieve data 12 to 48 hours. *Refer to section 9.1.8 for detail comparison with other S3 Object Storages.*

9.1.7 Object Storage – S3 Glacier Vault Lock

S3 Glacier Vault Lock allows you to easily deploy and enforce compliance controls for individual S3 Glacier vaults with a vault lock policy. You can specify controls such as "write once read many" (WORM) in a vault lock policy and lock the policy from future edits. *Once locked, the policy can no longer be changed.*

A vault lock policy can be locked to prevent future changes, providing strong enforcement for your compliance controls. You can use the vault lock policy to deploy regulatory and compliance controls, which typically require tight controls on data access.

9.1.8 Object Storage – Summary Table

Topics	S3 Standard	S3 Intelligent Tier	S3 Standard – IA	S3 One Zone – IA	S3 Glacier	S3 Glacier Deep Archive
Purpose & Characteristics	Stores data in Flat nonhierarchical structure Not Suitable for data archival	Storing objects in 2 access tiers; 1 tier that is optimized for frequent access & another low-cost tier that is optimized for infrequent access	Data for less frequent access, but requires rapid access when needed	Data for less frequent access, but requires rapid access when needed Not suitable for data archival. Data only stored in One AZ	For data archiving & long-term backup	For data less frequently accessed Most time to retrieve data
Availability	99.99%	99.99%	99.99%	99.50% Lowest Availability – the cheapest 20% less than S3 Standard – IA	99.99%	99.99%
Data Accessibility	Frequent Access (Active Data)	Frequent Access (Active Data) AND Infrequent Access (Cold Data)	Infrequent Access (Cold Data)	Infrequent Access (Cold Data)	Infrequent Access (Cold Data)	Infrequent Access (Cold Data)
Data Stored in	3 AZs	3 AZs	3 AZs	1 AZ	3 AZs	3 AZs
Retrieval Time	Milliseconds	Milliseconds	Milliseconds	Milliseconds	Minutes to hours	12 to 48 hours Longest time to retrieve
Retrieval Fee	N/A	N/A	Per GB retrieved	Per GB retrieved	Per GB retrieved	Per GB retrieved
Minimum Storage Duration Charge	No constraint of a minimum storage duration charge	30 days	30 days	30 days	90 days	180 days

Screen 149

You pay for ALL bandwidth IN and OUT S3 except:

- Data transferred IN from the Internet
- Data transferred between S3 buckets in the same AWS Region
- Data transferred FROM S3 bucket TO any AWS services within the same AWS Region as the S3 bucket
- Data transferred OUT to AWS CloudFront

Manage your object on S3 so that they are stored cost effectively on their lifecycle by configuring they S3 lifecycle.

Number of S3 buckets is not an attribute to the costing of using S3. AWS Lambda can be used for processing of data BEFORE it is stored in S3 bucket

9.2 Block Storage

The main advantage of object storage is that you can group devices into large storage pools and distribute those pools across multiple locations.

9.2.1 Elastic Block Storage (EBS)

AWS Elastic Block Store (EBS) is **Amazon's block-level storage solution used with the EC2 cloud service to store persistent data**.

EBS offers the same high availability and low-latency performance within the selected availability zone, allowing users to scale storage capacity at low subscription-based pricing model.

EBS Characteristics:

- Automated replicated
- EBS Vol can be attached to a single instance in the same Availability Zone
- EBS Vol can only be mounted with Amazon EC2
- It's a network attached drive which result in slow performance, but data is persistent meaning even if you reboot the instance data is still there unlike Instance Store

Charging concept of EBS Vol:

- Volume Type
- Provisioned IOPS

9.2.2 Instance Storage

It provides *temporary* block-level storage for your EC2 instance. This storage is located on disks that are physically attached to the hist computer.

Instance store is ideal for the *temporary storage* of information that changes frequently, such as buffers, caches, scratch data, and other temporary content, or for data that is replicated across a fleet of instances, such as load-balanced pool of web servers.

Instance storage is temporary, data is lost if instance experiences failure or is terminated. It's optimizing Caching Capability

9.3 File Storage

Elastic File System (EFS) can be mounted on instances across multiple Availability Zones. EC2 Instances can access files on EFS File system across many Availability Zones, Regions and VPCs. EFS is serverless!

Characteristics of EFS

- File-based
- Multiple Instances
- High performance storage for networking computing
- Multiple hosts need to access same data

10 AWS Database Services

Please note that Amazon S3 ***IS NOT*** a Database Service! Please understand the difference between Storage vs. Database

Storage could be a file or object storage which is a physical disk. Database is some sort of organized data store is a logical store.

WARNING: Your Credit Card will be charged if you decide to use most of these AWS Database Services. Please read their policy thoroughly i.e., Amazon DynamoDB is always FREE with the caveat free tier provides 25 GB of storage for the first 12 months and Amazon Redshift offers two-month free trail, etc.

10.1 Amazon Relational Database Services (RDS)

Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while **automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups**

10.2 AWS Aurora

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases.

The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

10.2.1 Amazon RDS vs. AWS Aurora

With Aurora, you can provision up to 15 replicas, and replication is performed in milliseconds. By contrast, **RDS allows only five replicas**, and the replication process is slower than Amazon Aurora. However, Aurora is more expensive than RDS.

10.3 AWS Redshift

It's a fully managed, petabyte scale data warehouse service in the cloud. It is a complete data warehouse solution in the cloud. It can be used for online analytical processing, and it reads by column instead of row.

10.4 Amazon DynamoDB

Amazon DynamoDB is a fully managed, serverless, key-value NoSQL database designed to run high-performance applications at any scale. DynamoDB offers built-in security, continuous backups, automated multi-region replication, in-memory caching, and data export tools.

Amazon DynamoDB has flexible schema *unlike Amazon RDS, AWS Redshift, and AWS Aurora, they don't have flexible schema*. Additionally, Amazon DynamoDB handles unstructured data.

10.4.1 Amazon DynamoDB Accelerator (DAX)

It is designed for scale and performance. DAX delivers fast response times for accessing eventually consistent data with fast memory performance.

Considered the following scenario below:

Weather tracking application is built using DynamoDB. The performance of the application has been consistently reliable. But lately, team has realized during holidays and travel seasons, the load on the application is high and the read requests consume most of the database resource and it has drastically increase overall application's latency/delay.

Based on the above scenario, upgrading to Amazon DynamoDB Accelerator (DAX) would solve that latency issue.

10.5 Amazon ElastiCache

Amazon Elasticache allows you to seamlessly set up, run, and scale popular open-source compatible in-memory data/database in the cloud. It is popular choice for real-time use cases like caching, session stores, and gaming.

If Amazon EC2 Instances are *intensively reading data* from Database, Amazon Elasticache can cache some values *to take the load off* the Database.

10.6 AWS EMR

AWS EMR is the industry-leading Cloud Big Data Platform for processing vast amount of data using open-source tools i.e., Hadoop, Sparks, Hive, & Presto. It manages provisioning, management & scaling of the EC2 instances.

10.7 Amazon Neptune

It is a fast, reliable, and fully managed graph database services. It managed graph database. It can also be used to combat Fraud Detection.

10.8 Amazon DocumentDB

Amazon DocumentDB is a scalable, highly durable, and fully managed database service for operating mission-critical MongoDB workloads.

10.9 Amazon Keyspaces

Amazon Keyspaces (for Apache Cassandra) is **a scalable, highly available, and managed Apache Cassandra–compatible database service**.

With Amazon Keyspaces, you can run your Cassandra workloads on AWS using the same Cassandra application code and developer tools that you use today.

10.10 Amazon Timestream

Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to 1,000 times faster and at as little as 1/10th the cost of relational databases.

10.11 Amazon QLDB

Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log. It's normally used in Supply Chain Industry.

10.12 Query Engine: AWS Athena

Please note that AWS Athena ***IS NOT*** a database but rather a query engine. This means that: Compute and storage are separate: databases both store data in rest, and provision the resources needed in order to perform queries and calculations. Amazon Athena is an interactive query service that makes it easy to analyze data in

Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. *It is best used to perform SQL based analysis with minimum effort.*

10.12.1 AWS Aurora vs. AWS Athena

Developers describe **Amazon Athena** as "*Query S3 Using SQL*". Amazon Athena is an interactive query service that makes it easy to analyze data in Amazon S3 using standard SQL. Athena is serverless, so there is no infrastructure to manage, and you pay only for the queries that you run. On the other hand, **Amazon RDS for Aurora** is detailed as "*MySQL and PostgreSQL compatible relational database with several times better performance*". Amazon Aurora is a MySQL-compatible, relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. Amazon Aurora provides up to five times better performance than MySQL at a price point one tenth that of a commercial database while delivering similar performance and availability. Amazon Athena can be classified as a tool in the **"Big Data Tools"** category, while Amazon RDS for Aurora is grouped under **"SQL Database as a Service"**.

10.13 AWS Database Services – Summary Table

Category	Database Services	Best Used For & Characteristic	Characteristic
Relational Database ***Traditional application, ERP, CRM, e-commerce***	Amazon RDS (Paas)	*Amazon Relational Database Service (Amazon RDS) makes it easy to set up, operate, and scale a relational database in the cloud. It provides cost-efficient and resizable capacity while automating time-consuming administration tasks such as hardware provisioning, database setup, patching and backups*	• *RDS Doesn't support Flexible Schema* • *Benefit of deploying RDS in read replica configuration – Read Replica improves database scalability*
	AWS Aurora (SaaS)	*Amazon Aurora is a relational database engine. It is designed to deliver the speed and reliability of high-end commercial databases in a simple and cost-effective manner.*	• *Aurora can provision up to 15 replicas while RDS allows only 5 replicas* • *Aurora doesn't support flexible schema*
	AWS Redshift (SaaS)	*Amazon Redshift makes it easy to add nodes to your data warehouse and enables you to maintain fast query performance as your data warehouse grows. Redshift Spectrum: Redshift Spectrum enables you to run queries against exabytes of data in Amazon S3.*	• *Datawarehouse service in the cloud* • *Can be used for Online Analytical Processing* • *Read by column instead of row* • *Redshift doesn't support flexible schema*
Key Value Database ***High Traffic web, gaming application***	Amazon DynamoDB (PaaS)	*Amazon DynamoDB is often used for low-scale operations because of its simplicity, but it also excels at ultrahigh-scale operations such as those demanded by Amazon* *Can use DynamoDB Accelerator (DAX) to deliver fast response times – fast memory performance*	• *Support flexible schema unlike RDS, Redshift & Aurora* • *No SQL Database* • *Handle unstructured data*
In Memory Database ***Caching, Geospatial APP***	Amazon ElastiCache	*Amazon ElastiCache improves the performance of web applications by allowing you to retrieve information from a fast, managed, in-memory system, instead of relying entirely on slower disk-based databases.*	• *Can be used to take the load off the database when EC2 instances are intensively reading data from DB*
Big Data	AWS EMR	*It's industry leading Cloud Big Data platform for processing vast amount of data using open-source tools such as Hadoop/spark/hive/presto*	*Provision resources to run big data workloads*
Graph	Amazon Neptune	*Amazon Neptune is a new fully managed cloud graph database. With Amazon Neptune, customers can manage data within a graph model – a semantic structure in nodes, edges, and properties.*	• *Suitable for Graph & Fraud Detection*
Document ***Catalog, user profile***	Amazon DocumentDB	*A document database is a type of nonrelational database that is designed to store and query data as JSON-like documents. Document databases make it easier for developers to store and query data in a database by using the same document-model format they use in their application code*	*Amazon DocumentDB is a scalable, highly durable, and fully managed database service for operating mission-critical MongoIDB workloads.*
Wide Column ***High Scale Industrial APP***	Amazon Keyspaces	*Amazon Keyspaces (for Apache Cassandra) is a scalable, highly available, and managed Apache Cassandra–compatible database service.*	*With Amazon Keyspaces, you can run your Cassandra workloads on AWS using the same Cassandra application code and developer tools that you use today.*
Time Series ***IoT, Industrial Telemetry***	Amazon Timestream	*Amazon Timestream is a fast, scalable, and serverless time series database service for IoT and operational applications that makes it easy to store and analyze trillions of events per day up to*	*Amazon Timestream saves you time and costs in managing the lifecycle of time series data by keeping recent data in memory and moving historical data to a*

		1,000 times faster and at as little as 1/10th the cost of relational databases.	*cost-optimized storage tier based upon user-defined policies.*
Ledger ***Supply Chain***	Amazon QLDB	*Amazon Quantum Ledger Database (QLDB) is a fully managed ledger database that provides a transparent, immutable, and cryptographically verifiable transaction log.*	• *Typically used in Supply Chain* • *Used to record a history of economic & financial activity in an organization*

Screen 150

11 Data Migration

11.1 AWS Database Migration Services

AWS Database Migration Service **helps you migrate your databases to AWS with virtually no downtime**. All data changes to the source database that occur during the migration are continuously replicated to the target, allowing the source database to be fully operational during the migration process. AWS offers four types of Migration Services.

11.1.1 Database Migration Services

Database Migration Service (DMS) is **a software tool for migrating an on-premises database to the Amazon Web Services cloud**. AWS DMS allows replication tasks to begin in minutes, and monitors the data replication process, providing the administrator with performance data in real-time.

11.1.2 Server Migration Services

Server Migration Service (SMS) from AWS is an agentless service that enables customers to simplify the AWS Migration process by automatically replicating live server volumes from their on-premises servers into AWS.

11.1.3 Application Discovery Service

AWS Application Discovery Service helps enterprise customers plan migration projects by gathering information about their on-premises data centers. Planning data center migrations can involve thousands of workloads that are often deeply interdependent. Server utilization data and dependency mapping are important early first steps in the migration process. AWS Application Discovery Service collects and presents configuration, usage, and behavior data from your servers to help you better understand your workloads.

11.1.4 AWS Snowball

AWS Snowball is a **data transport solution** that accelerates moving terabytes to petabytes of data into and out of AWS using storage appliances designed to be secure for physical transport.

11.2 Snow Family

11.2.1 AWS Snowcone

AWS Snowcone is the smallest member of the AWS Snow Family of edge computing, edge storage, and data transfer devices. Weighing in at 4.5 pounds (2.1 kg), AWS Snowcone is equipped with 8 terabytes of usable storage.

It is used by the Edge computing applications for IoT use cases for facilitating the collection and processing of data to gain immediate insights and then transfer the data to AWS.

11.2.2 AWS Snowball – Snowball Edge STORAGE Optimized

As a rule of thumb, if it takes more than one week to upload your data to Amazon Web Services using the spare capacity of your existing Internet connection, then you should consider using Snowball. Snowball Edge Storage Optimized devices provide both block storage and Amazon S3-compatible object storage, and 40 vCPUs. They are well suited for local storage and large scale-data transfer.

11.2.3 AWS Snowball – Snowball Edge COMPUTE Optimized

Snowball Edge Compute Optimized devices provide 52 vCPUs, block and object storage, and an optional GPU for use cases like advanced machine learning and full motion video analysis in disconnected environments.

11.2.4 AWS Snowmobile

AWS Snowmobile is an Exabyte-scale data transfer service used to move extremely large amounts of data to AWS. You can transfer up to 100PB per Snowmobile, a 45-foot long ruggedized shipping container, pulled by a semi-trailer truck. Snowmobile makes it easy to move massive volumes of data to the cloud, including video libraries, image repositories, or even a complete data center migration. Transferring data with Snowmobile is more secure, fast and cost effective.

11.2.5 AWS OpsHub

AWS OpsHub is a Graphical User Interface (GUI) for AWS Snowball. It manages your AWS Snowball devices, enabling you to rapidly deploy edge computing workloads and simplify data migration to the Cloud.

11.2.6 Snow Family Comparison Table

CATEGORY	*AWS Snowcone*	*AWS Snowball Edge STORAGE Optimized*	*AWS Snowball Edge COMPUTE Optimized*	*AWS Snowmobile*
Usage Scenario	*Edge Computing* *Data Transfer* *Edge Storage*	*Data Transfer* *Edge Storage*	*Edge Computing* *Data Transfer*	*Data Transfer*
Storage	*8 TB*	*80 TB*	*42 TB*	*100 PB* *1 PB = 1,000 TB*
Device Weight	*4.5 lbs (2.1 Kg)*	*49.7 lbs (22.3 Kg)*	*49.7 lbs (22.3 Kg)*	*Shipping Container pulled by a semi-trailer truck*

Screen 151

12 AWS Serverless Services & Managed Services

12.1 Serverless – Compute

12.1.1 AWS Lambda

AWS Lambda is *a serverless compute service that runs your code in response to events and automatically manages the underlying compute resources for you*. You can use AWS Lambda to extend other AWS services with custom logic or create your own back-end services that operate at AWS scale, performance, and security.

12.1.2 AWS Fargate

AWS Faregate is **a serverless, pay-as-you-go compute engine** that lets you focus on building applications without managing servers. AWS Fargate is compatible with both Amazon Elastic Container Service (ECS) and Amazon Elastic Kubernetes Service (EKS).

12.1.3 AWS Fargate vs. EC2

Elastic Computing Cloud (EC2) – Managed Services	***AWS Fargate – Serverless/Pay as you go***
Deployment & manage your own cluster on EC2 instance for running container *ECS without EC2 is useless – ECS uses EC2 to run your container* *Need to patch, secure and update to the latest version of docker*	*Run container directly without any EC2 instances* *No need to patch, secure or update server* *Instead of paying EC2 instance, AWS Fargate to run container when you need and STOP paying when you don't need it*

Screen 152

12.2 Serverless – Application Integration

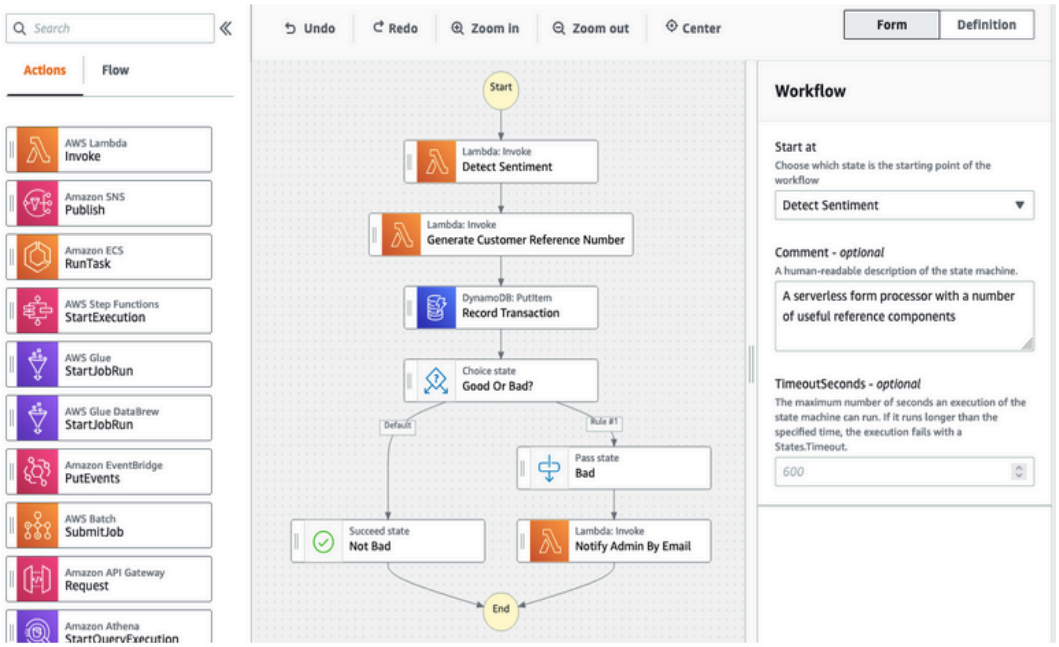
12.2.1 Amazon Eventbridge

Serverless event bus that makes it easier to build even-driven applications at scale using events generated from your applications, integrated SaaS application & AWS Service

12.2.2 AWS Step Function

It is a low-code visual workflow service used to orchestrate AWS services, automate business processes, and build serverless applications. *VIZUALIZE your workflow* – as you write your code, Step Function gives VIRTUAL Workflow (VIZUALIZE) your code like a Flowchart.

Please refer screen below for example of AWS Step Function.



Screen 153

12.2.3 AWS APPSYNC

It enables developers to manage and synchronize mobile app data in real time across devices and users, but still allows the data to be accessed and altered when the mobile device is in an offline state.

Create, publish, maintain, monitor, and secure Graph-QL APIs and subscriptions at any scale.

12.2.4 Amazon SQS

It is a fully managed message queuing service that enables you to decouple and scale microservices, distributed systems, and serverless applications.

Can be used to decouple components of a microservices – Guaranteed delivery

12.2.5 Amazon SNS

It is a highly available, durable, secure, fully managed pub/sub messaging service that enable you to decouple microservices, distributed systems, and serverless applications

Amazon SNS	***Amazon SQS***
Pass along messages (PUB-SUB)	*Guaranteed delivery*
Send plain text-emails	*Places messages into a queue*
Good for web hook, simple email, triggering Lambda functions	*Send, store, receive messages between software components at any volume to decouple application tiers*

Screen 154

12.2.6 Amazon API Gateway

It is an AWS Service for creating, publishing, maintaining, monitoring and securing REST HTTP, and Web Socket APIs at any scale.

A great example of an API Gateway is the Netflix API Gateway. The Netflix streaming service is available on hundreds of different kinds of devices including televisions, set-top boxes, smartphones, gaming systems, tablets, etc. Initially, Netflix attempted to provide a one-size-fits-all API for their streaming service.

API Gateway can call an AWS Lambda function to create the front door of a serverless application - Amazon API Gateway is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud. API Gateway acts as a ***"front door"*** for applications to access data, business logic, or functionality from your backend services, such as workloads running on Amazon Elastic Compute Cloud (Amazon EC2), code running on AWS Lambda, any web application, or real-time communication applications.

API Gateway can be configured to send data directly to Amazon Kinesis Data Stream - Amazon API Gateway can execute AWS Lambda functions in your account, start AWS Step Functions state machines, or call HTTP endpoints hosted on AWS Elastic Beanstalk, Amazon EC2, and also non-AWS hosted HTTP based operations that are accessible via the public Internet.API Gateway also allows you to specify a mapping template to generate static content to be returned, helping you mock your APIs before the backend is ready. You can also integrate API Gateway with other AWS services directly – for example, you could expose an API method in API Gateway that sends data directly to Amazon Kinesis.

12.2.7 AWS Glue

It's a fully managed ETL service that makes it easy for customers to prepare and load their data for analytics. To be used for ETL Data Processing. It is serverless Data Integration Service

12.3 Serverless – Data Store

12.3.1 Amazon S3

Store any amount of data with industry leading scalability data availability, security & performance

12.3.2 Amazon DynamoDB

Get single digit millisecond performance at any scale with this key-value & document database

12.3.4 Amazon Athena

Athena is serverless. You can quickly query your data without having to setup and manage any servers or data warehouses. Just point to your data in Amazon S3, define the schema, and start querying using the built-in query editor.

Amazon Athena allows you to tap into all your data in S3 without the need to set up complex processes to extract, transform, and load the data (ETL).

12.3.5 Amazon RDS Proxy

Increase scalability, resiliency, and security with this proxy for Amazon relational database service.

12.3.6 Amazon Aurora Serverless

Automatically scale capacity based on your application's need with this configuration for Amazon Aurora

12.4 Serverless – Other Serverless Resources

12.4.1 Elastic File System (EFS)

Amazon Elastic File System (Amazon EFS) automatically grows and shrinks as you add and remove files with no need for management or provisioning. It's simple, serverless elastic file system

12.4.2 Amazon Kinesis

You can use Amazon Kinesis Data **Streams to collect and process large streams of data records in real time**. You can create data-processing applications, known as Kinesis Data Streams applications. A typical Kinesis Data Streams application reads data from a data stream as data records.

12.5 Managed Services

12.5.1 Amazon Elastic Compute Cloud (EC2)

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable compute capacity in the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon EC2's simple web service interface allows you to obtain and configure capacity with minimal friction. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment.

12.5.2 Amazon RDS

Amazon Relational Database Service (Amazon RDS) is a fully managed services that makes it easier to set up, operate, and scale a relational database in the AWS Cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks.

Not to be confused with Amazon RDS Proxy which is serverless

12.5.3 Amazon Aurora

Amazon Aurora (Aurora) is a fully managed relational database engine that's compatible with MySQL and PostgreSQL. You already know how MySQL and PostgreSQL combine the speed and reliability of high-end commercial databases with the simplicity and cost-effectiveness of open-source databases. The code, tools, and applications you use today with your existing MySQL and PostgreSQL databases can be used with Aurora. With some workloads, Aurora can deliver up to five times the throughput of MySQL and up to three times the throughput of PostgreSQL without requiring changes to most of your existing applications.

Not to be confused with Amazon Aurora Serverless which is obviously serverless

12.5.4 AWS Redshift

AWS Redshift is a fast, fully managed cloud data warehouse that makes it simple and cost-effective to all your data using standard SQL and your existing business intelligence (BI) tools. Customers tell us that they want extremely fast query response times so they can make equally fast decisions

12.5.5 Amazon LightSail

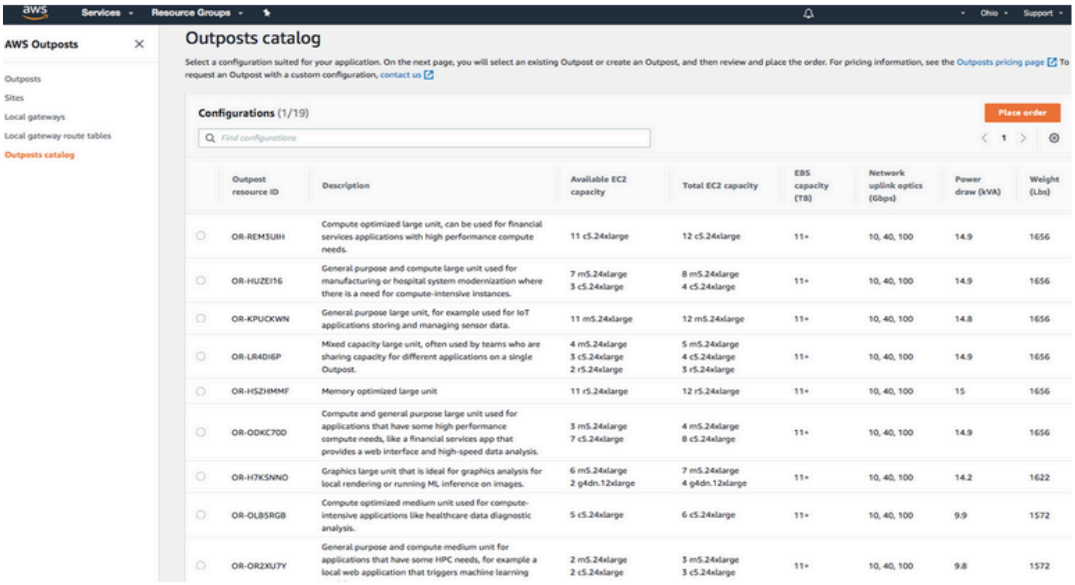
Amazon Lightsail provides a number of features designed to help make your project quickly come to life. Designed as an easy-to-use VPS, Lightsail offers you a one-stop-shop for all your cloud needs. Take a look to see how we can help you get started on a virtual private server on AWS infrastructure.

12.5.6 Amazon Elastic Beanstalk

Elastic Beanstalk is the fastest and simplest way to deploy your application on AWS. You simply use the AWS Management Console, a Git repository, or an integrated development environment (IDE) such as Eclipse or Visual Studio to upload your application, and Elastic Beanstalk automatically handles the deployment details of capacity provisioning, load balancing, auto-scaling, and application health monitoring. Within minutes, your application will be ready to use without any infrastructure or resource configuration work on your part.

12.5.7 AWS Outposts

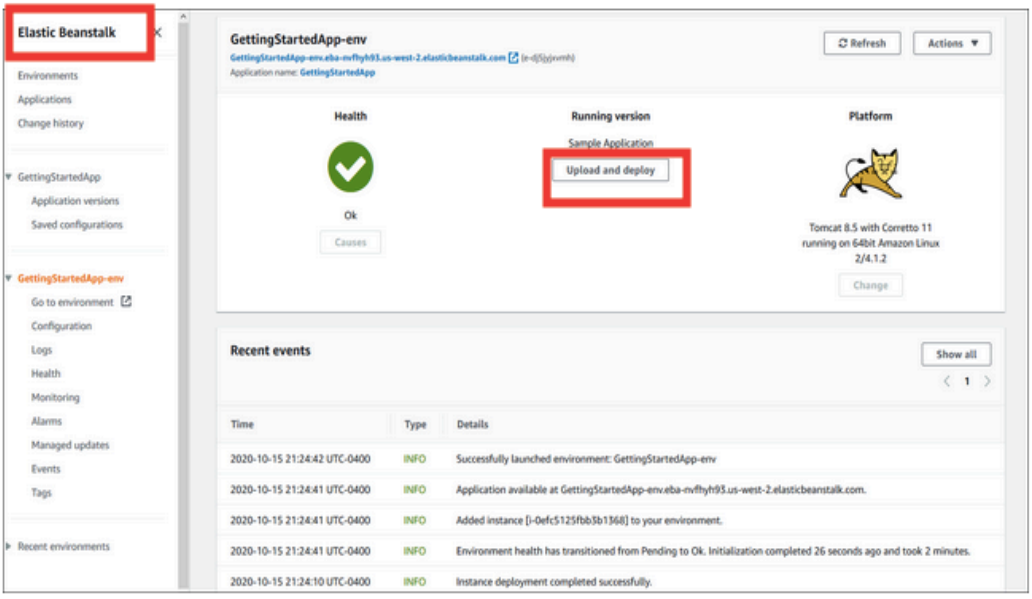
AWS Outposts is **a fully managed service** that offers the same AWS infrastructure, same AWS services, same APIs, and tools to virtually any datacenter, co-location space, or on-premises facility for a truly consistent hybrid experience.


aws
Services
Resource Groups
Ohio
Support
AWS Outposts
Outposts
Sites
Local gateways
Local gateway route tables
Outposts catalog
Outposts catalog
Select a configuration suited for your application. On the next page, you will select an existing Outpost or create an Outpost, and then review and place the order. For pricing information, see the Outposts pricing page To request an Outpost with a custom configuration, contact us
Configurations (1/19)
Place order
Find configurations
1
Outpost resource ID
Description
Available EC2 capacity
Total EC2 capacity
EBS capacity (TB)
Network uplink optics (Gbps)
Power draw (kVA)
Weight (Lbs)
OR-REM3UIH
Compute optimized large unit, can be used for financial services applications with high performance compute needs.
11 c5.24xlarge
12 c5.24xlarge
11+
10, 40, 100
14.9
1656
OR-HUZEI16
General purpose and compute large unit used for manufacturing or hospital system modernization where there is a need for compute-intensive instances.
7 m5.24xlarge
3 c5.24xlarge
8 m5.24xlarge
4 c5.24xlarge
11+
10, 40, 100
14.9
1656
OR-KPUCKWN
General purpose large unit, for example used for IoT applications storing and managing sensor data.
11 m5.24xlarge
12 m5.24xlarge
11+
10, 40, 100
14.8
1656
OR-LR4DI6P
Mixed capacity large unit, often used by teams who are sharing capacity for different applications on a single Outpost.
4 m5.24xlarge
3 c5.24xlarge
2 r5.24xlarge
5 m5.24xlarge
4 c5.24xlarge
3 r5.24xlarge
11+
10, 40, 100
14.9
1656
OR-H5ZHMMF
Memory optimized large unit
11 r5.24xlarge
12 r5.24xlarge
11+
10, 40, 100
15
1656
OR-ODKC70D
Compute and general purpose large unit used for applications that have some high performance compute needs, like a financial services app that provides a web interface and high-speed data analysis.
3 m5.24xlarge
7 c5.24xlarge
4 m5.24xlarge
8 c5.24xlarge
11+
10, 40, 100
14.9
1656
OR-H7KSNNO
Graphics large unit that is ideal for graphics analysis for local rendering or running ML inference on images.
6 m5.24xlarge
2 g4dn.12xlarge
7 m5.24xlarge
4 g4dn.12xlarge
11+
10, 40, 100
14.2
1622
OR-OL85RGB
Compute optimized medium unit used for compute-intensive applications like healthcare data diagnostic analysis.
5 c5.24xlarge
6 c5.24xlarge
11+
10, 40, 100
9.9
1572
OR-OR2XU7Y
General purpose and compute medium unit for applications that have some HPC needs, for example a local web application that triggers machine learning
2 m5.24xlarge
2 c5.24xlarge
3 m5.24xlarge
3 c5.24xlarge
11+
10, 40, 100
9.8
1572

Screen 155

13.1 Amazon Elastic Beanstalk

It is for deploying & scaling web applications and services with JAVA, PHP, Python. You can upload your code and Elastic Beanstalk automatically handles the deployment



Screen 156

There is no additional charge for Elastic Beanstalk. You pay only for the underlying AWS resources that your application consumes.

Furthermore, with Elastic Beanstalk, you can quickly deploy and manage applications in AWS cloud without having to learn about the infrastructure that runs those applications

13.1.1 Monitoring with Amazon Elastic Beanstalk

Elastic Beanstalk can be used for health monitoring and reporting capabilities. The Elastic Beanstalk health monitoring can determine that the environment's Auto Scaling group is available and has a minimum of at least one instance.

In addition to Elastic Load Balancing health checks, Elastic Beanstalk monitors resources in your environment and changes health status to red if they fail to deploy, are not configured correctly, or become unavailable. These checks confirm that:

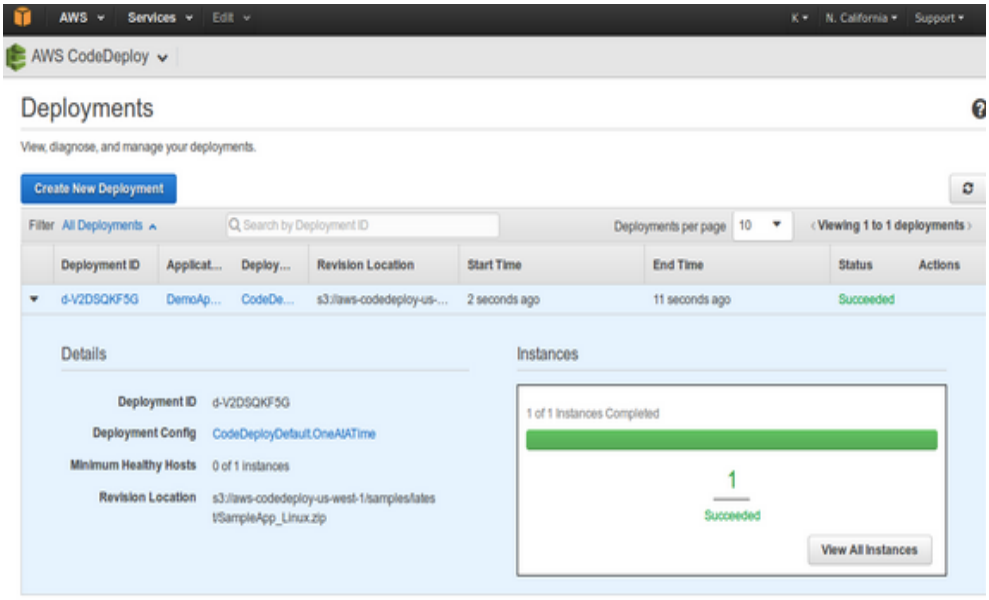
- The environment's Auto Scaling group is available and has a minimum of at least one instance.
- The environment's security group is available and is configured to allow incoming traffic on port 80.
- The environment CNAME exists and is pointing to the right load balancer.
- In a worker environment, the Amazon Simple Queue Service (Amazon SQS) queue is being polled at least once every three minutes.

With basic health reporting, the Elastic Beanstalk service *does not* publish any metrics to Amazon CloudWatch - With basic health reporting, the Elastic Beanstalk service does not publish any metrics to Amazon CloudWatch.

The CloudWatch metrics used to produce graphs on the Monitoring page of the environment console are published by the resources i

13.2 AWS CodeDeploy

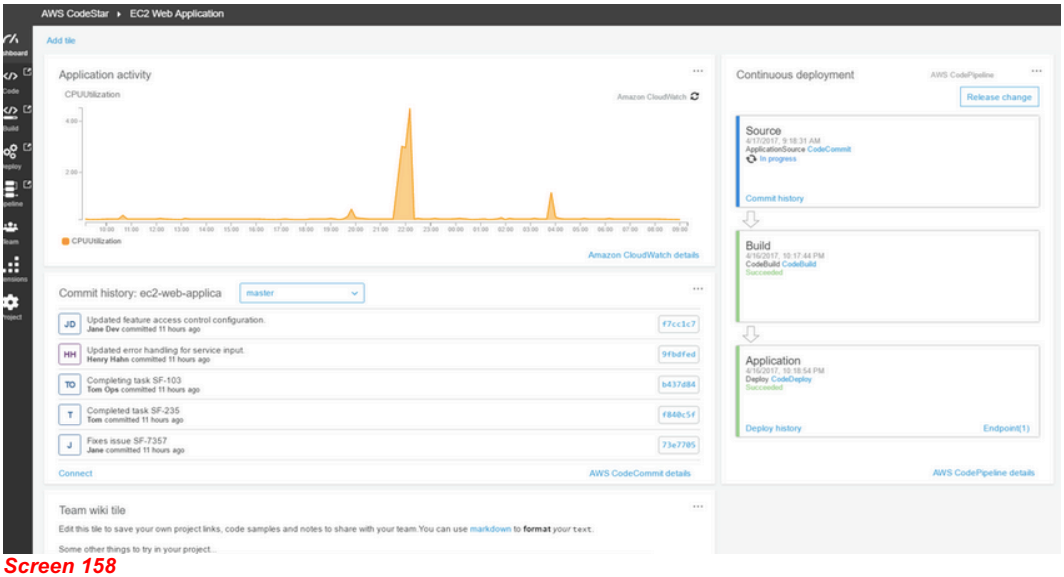
Service that automates code deployments to Amazon EC2 instances. It helps you install application code automatically to an Amazon EC2 Instance



Screen 157

13.3 AWS CodeStar

AWS CodeStar is a cloud-based development service that provides the tools you need to quickly develop, build, and deploy applications on AWS.

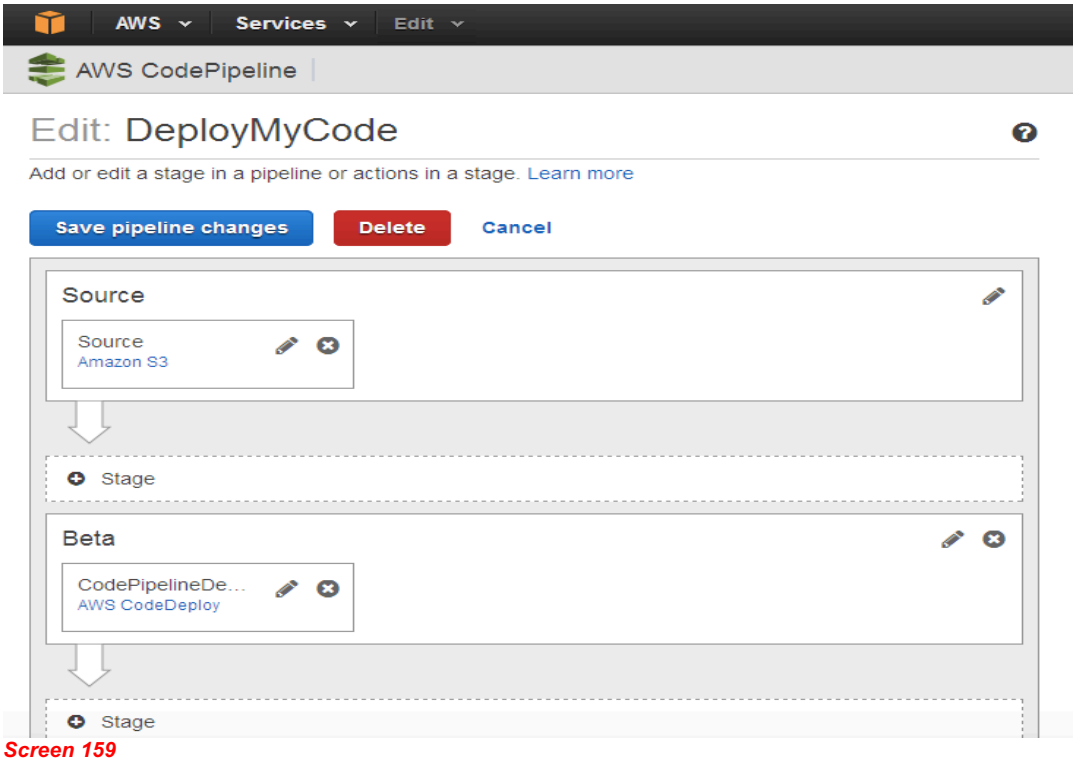


Screen 158

13.4 AWS CodePipleline

AWS CodePipeline is a fully managed continuous delivery service that helps you automate your release pipelines for fast and reliable application and infrastructure updates.

CodePipeline automates the build, test, and deploy phases of your release process every time there is a code change, based on the release model you define. This enables you to rapidly and reliably deliver features and updates.



Screen 159

13.5 AWS Quick Start

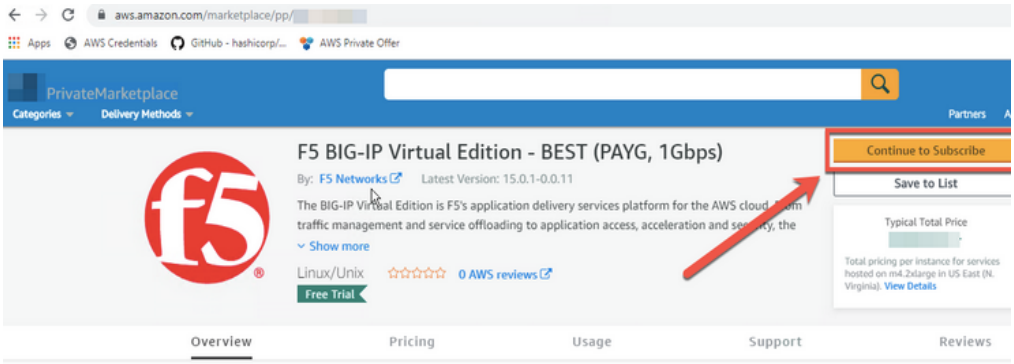
It's automated references deployment for key workloads on AWS cloud. It's a *pre-built template* by AWS to help you deploy popular stacks on WS and reduce hundreds of manual procedures. It is a deployment template.

13.6 AWS OpsWorks

It's an infrastructure deployment for cloud admin. It's a Configuration Management Service that provides managed instances of chef and puppet.

13.7 AWS Market Place

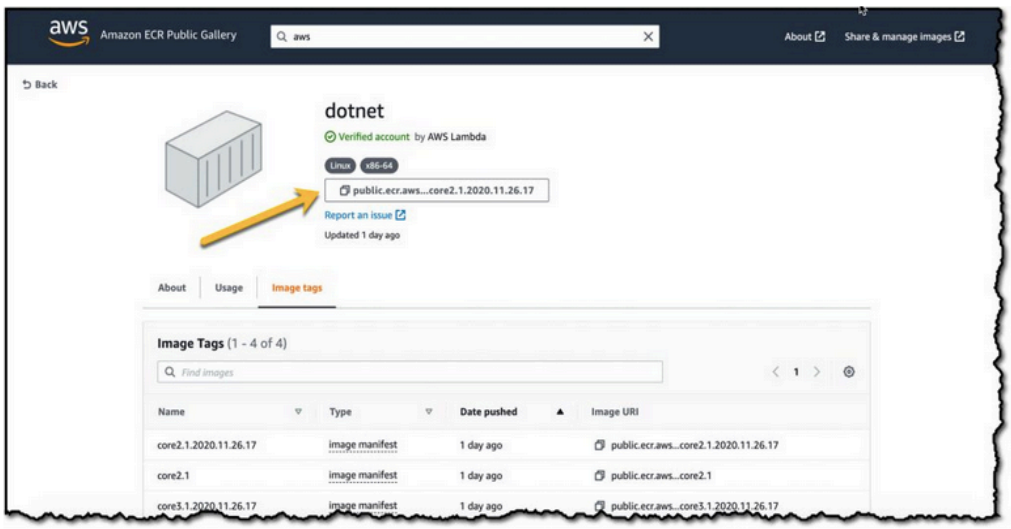
It's a digital catalog with thousands of software listing from independent software vendors that make it easy to find, test, buy and deploy software that runs on AWS



Screen 160

13.8 Amazon Elastic Container Registry (ECR)

Store, manage and deploy docket container image. It eliminates the need to operate your container repositories. It allows all AWS developers to save configuration and quickly move them into a production environment.



Screen 161

14 Machine Learning Resources

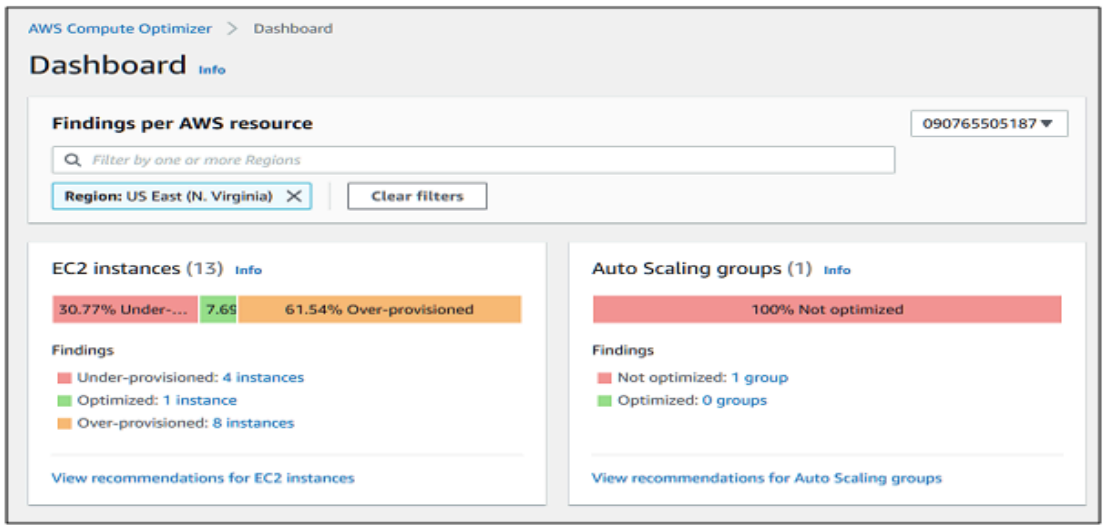
WARNING: Your Credit Card will be charged if you decide to active the following Machine Learning Resources

14.1 AWS Compute Optimizer

Using Machine Learning to analyze historical utilization metrics. It recommends optimal AWS resources for your workloads to reduce costs & improve performance by using Machine Learning to analyze historical performance.

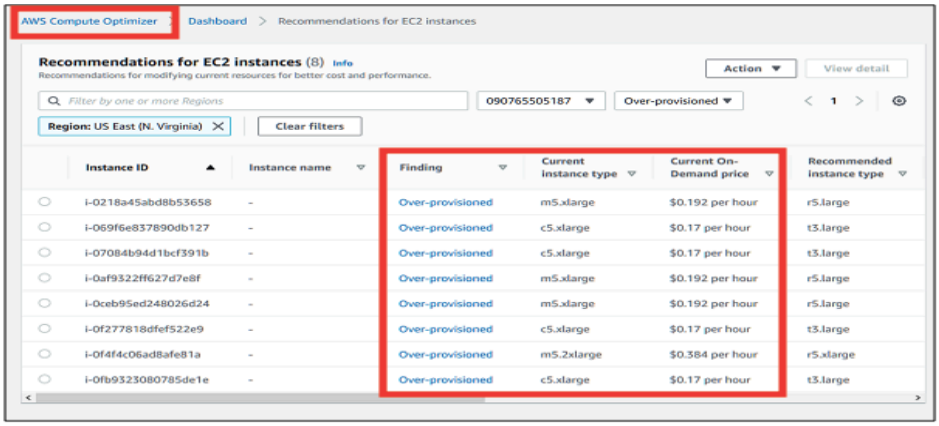
It identifies whether your AWS resources are optimal and offer recommendations to improve cost & performance.

AWS Compute Optimizer delivers recommendations for selected types of EC2 instances, EC2 Auto Scaling groups, EBS volumes, and Lambda functions.



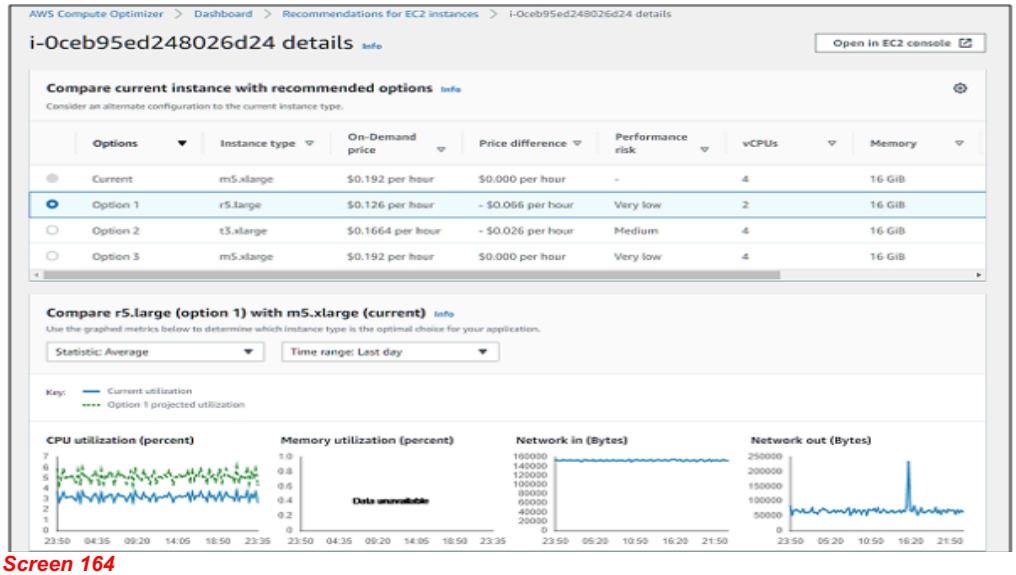
Screen 162

Screen above displays the scan result of the information running EC2 in AWS Infrastructure and provide the recommendations for all supported Instances.



Screen 163

With AWS Compute, you can Compare and control the over-provisioned and under-provisioned resources with the metrics provided.



Screen 164

You can use compute optimizer at No Cost. EC2 instance type and EC2 Auto Scaling group configuration recommendations are available for free.

14.2 Amazon Comprehend

Amazon Comprehend is a natural-language processing (NLP) service that uses machine learning to *uncover valuable insights and connections in text*. Natural Language Processing (NLP) service that uses Machine Learning to *uncover information in unstructured data*

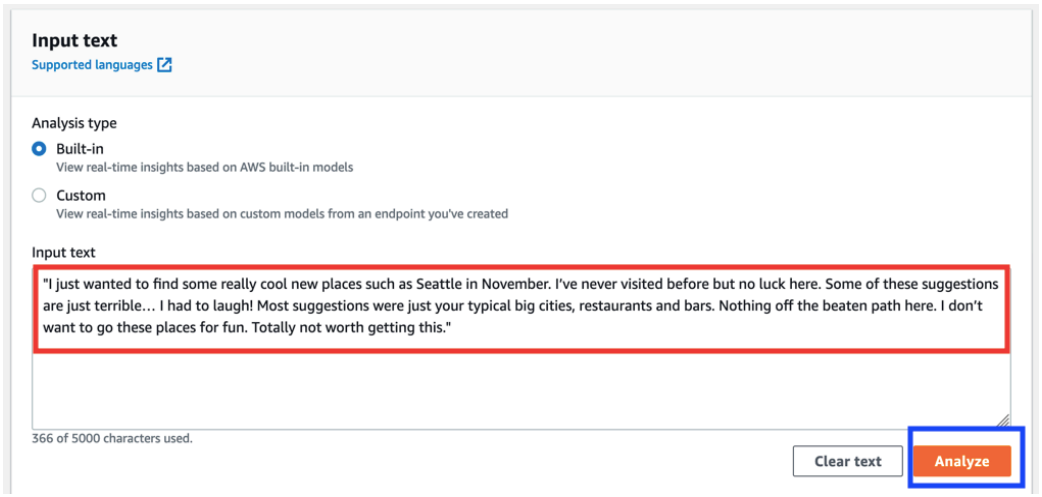
In the following steps, you use Amazon Comprehend Insights to analyze these book reviews for sentiment, syntax, and more. The results of the sentiment analysis helps you to determine whether these customers find the book valuable.

Review 1:
"I just wanted to find some really cool new places such as Seattle in November. I've never visited before but no luck here. Some of these suggestions are just terrible… I had to laugh! Most suggestions were just your typical big cities, restaurants, and bars. Nothing off the beaten path here. I don't want to go these places for fun. Totally not worth getting this."

Review 2:
"This was such a beautiful book. I wasn't even planning any travel when I came across this and just started flipping through the pages. I really like the cover and all the large glossy photographs in this book. John Smith did a wonderful job with the photography. I've found a perfect home for this on my coffee table. I'm planning a trip to Paris and Barcelona soon and I know this will come in handy. In the meantime, it's perfect for assisting this armchair traveler!"

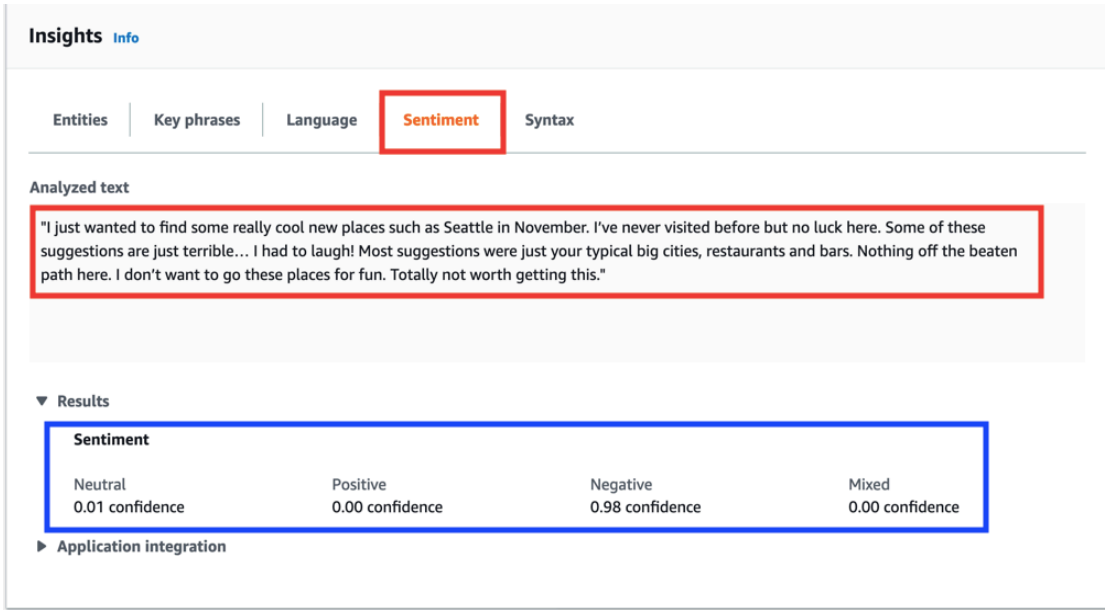
Review 3:
"As a traveler, I really appreciated reading about these great places to visit. The author takes you all over the world. Even with all the free information online these days, I find I'm taking this book with me wherever I go and using it to discover hidden gems."

Use Amazon Comprehend Insights to analyze the first review for positive, negative, or mixed sentiment, entities, key phrases, language, and syntax detection.



Screen 165

Copy and paste Review 1 on screen above and click ***Analyze*** button. Click ***Sentiment*** tab and you will see screen below



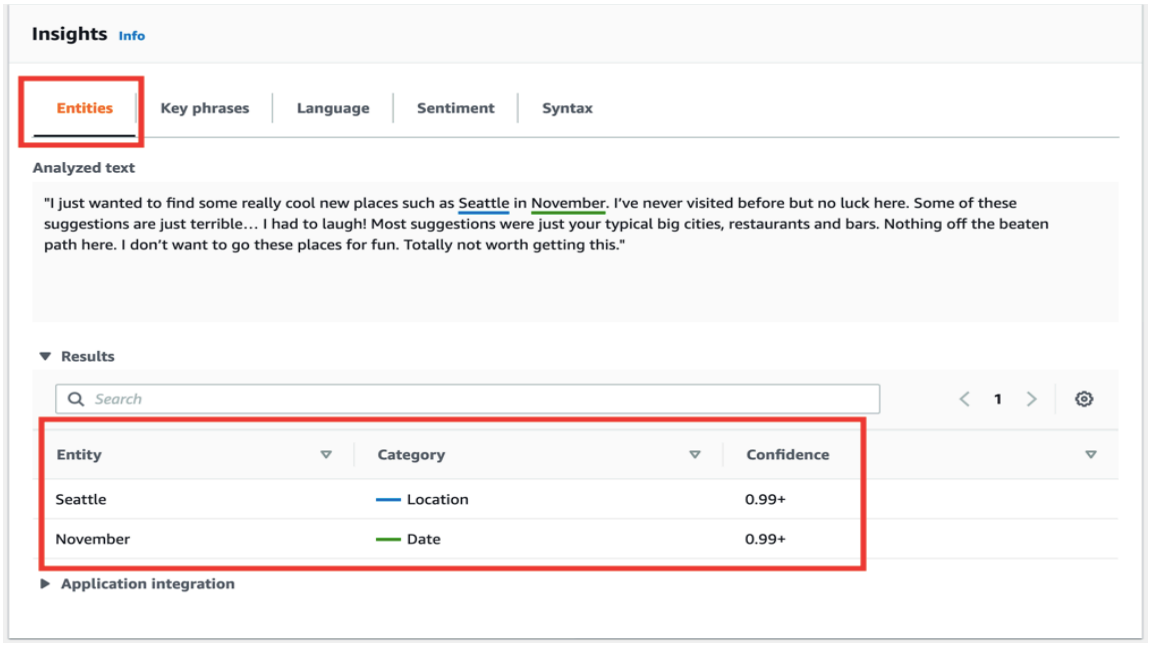
Screen 166

The ***Sentiment*** tab shows the overall emotional sentiment of the text. Sentiment can be rated *neutral, positive, negative, or mixed*. In this case, each emotional sentiment has a confidence rating, providing an estimate by Amazon Comprehend for that sentiment being dominant.

Use Amazon Comprehend to determine the sentiment of a document. You can determine if the sentiment is positive, negative, neutral, or mixed.

The results for sentiment can be neutral, positive, negative, and mixed. For this review, the results indicate that this is a negative review, and low scores for positive or mixed sentiment.

Click ***Entities*** tab and you will see screen below



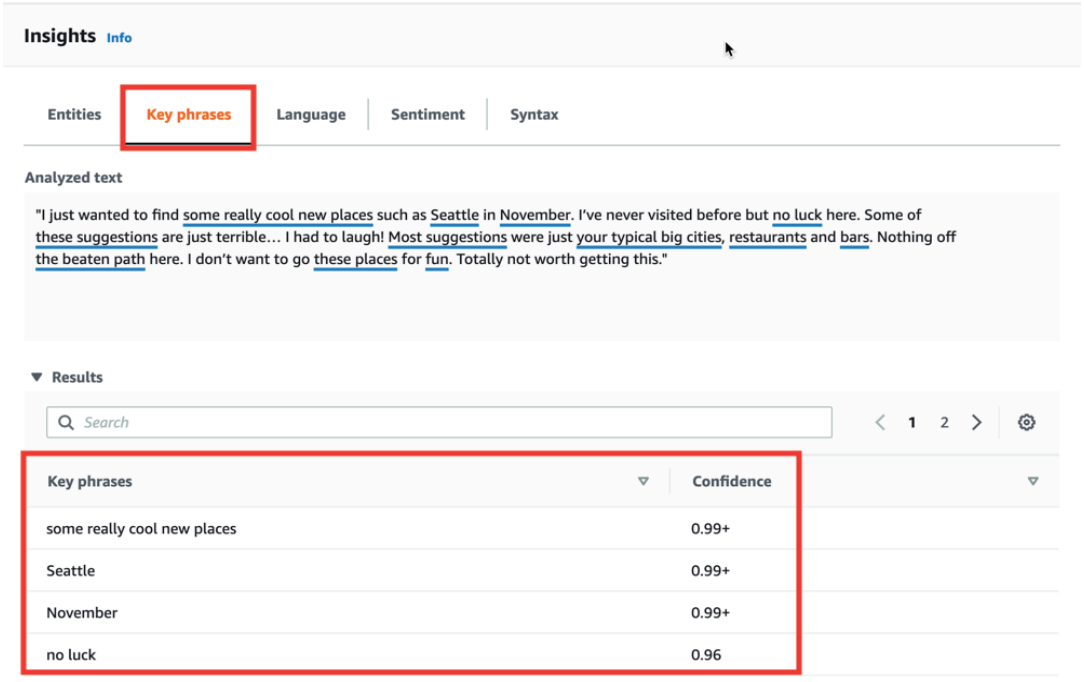
Screen 167

The ***Entities*** tab shows ***color-coded*** text to indicate different entity types such as organizations, locations, dates, and persons. The Results pane shows more information about the text.

Each entry shows the entity, its category, and the level of confidence Amazon Comprehend has in this analysis. In case you want to extract custom entities.

You can see the entities detected along with their confidence score. For this review, Seattle has been identified as a location with a confidence score & November has been identified as date with confidence score.

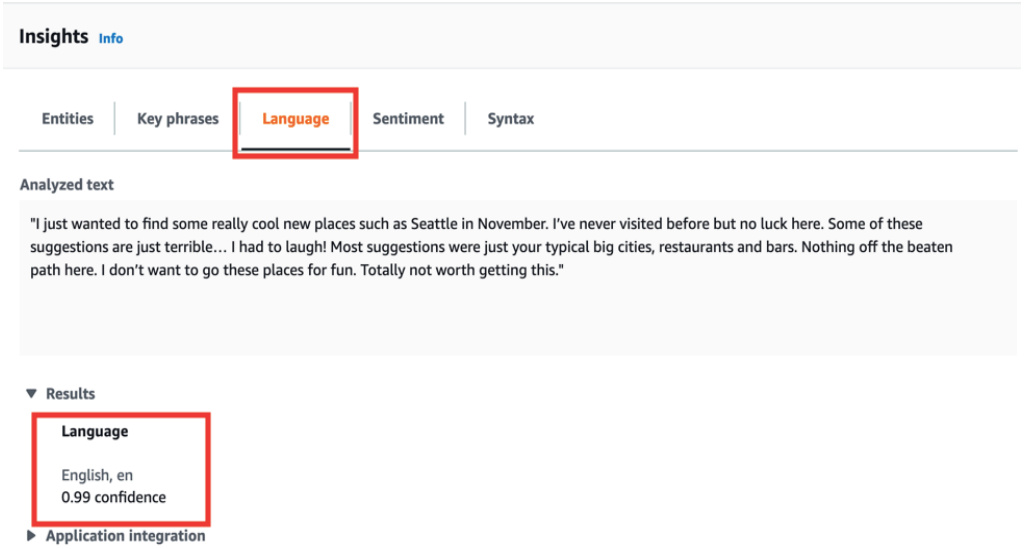
Click ***Key Phrases*** tab and you will see screen below



Screen 168

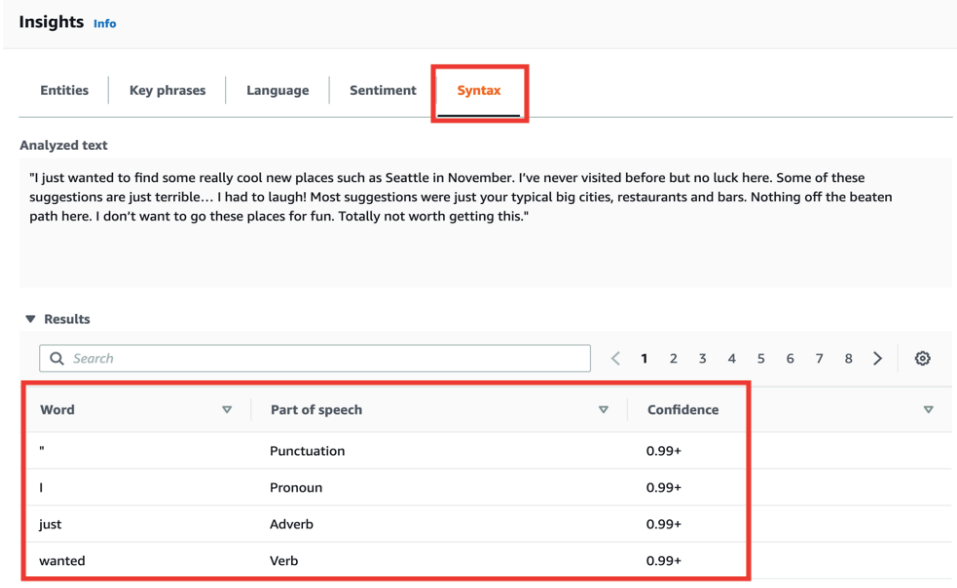
The ***Key phrases*** tab lists key noun phrases that Amazon Comprehend detected in the input text and the associated confidence level. In the Analyzed text box, key phrases are indicated by underlined text. The Results section lists key phrases with the respective confidence score.

Click ***Language*** tab and you will see screen below



Screen 169

The ***Language*** tab shows the dominant language of the text along with the confidence rating. Amazon Comprehend can recognize 100 languages. For this review, you can see that Amazon Comprehend detected the English language with a 0.99 confidence rating. Click ***Syntax*** tab and you will see screen below



Screen 170

The ***Syntax*** tab shows a breakdown of each element in the text, along with its part of speech, and the associated confidence score.

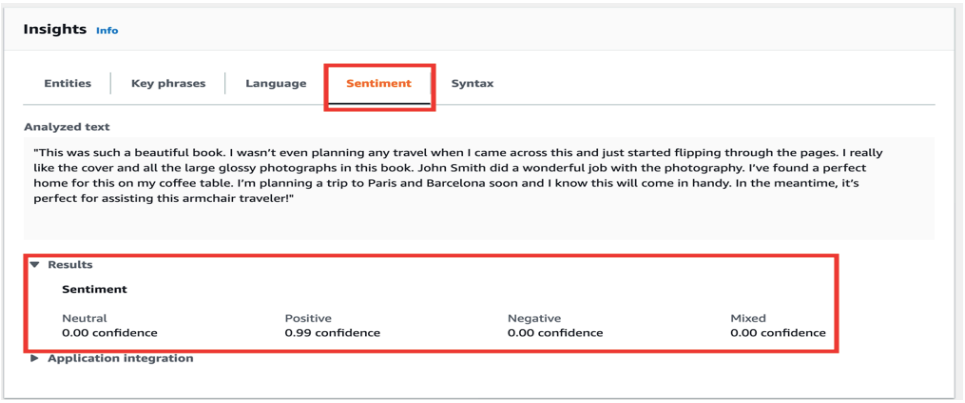
Repeat step screens 165 through 170 above to perform the second review below

Review 2:

"This was such a beautiful book. I wasn't even planning any travel when I came across this and just started

flipping through the pages. I really like the cover and all the large glossy photographs in this book. John Smith did a wonderful job with the photography. I've found a perfect home for this on my coffee table. I'm planning a trip to Paris and Barcelona soon and I know this will come in handy. In the meantime, it's perfect for assisting this armchair traveler!"

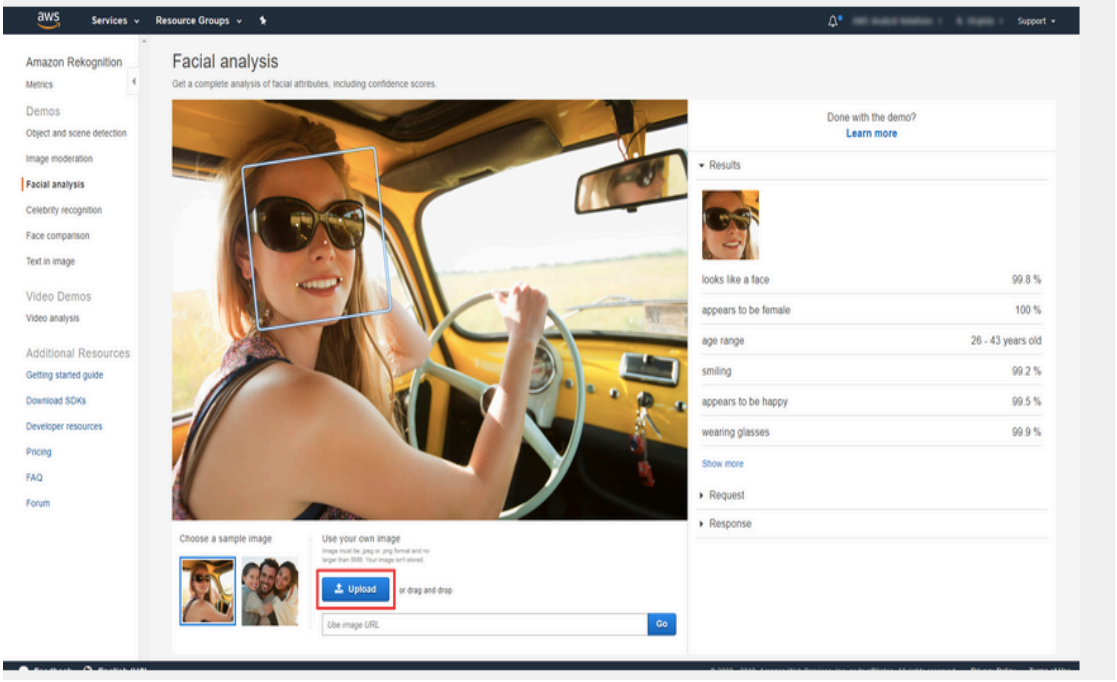
Make sure you go over every tab just like what you did with the first review: ***Entities, Key Phrases, Language, Sentiment*** and ***Syntax*** tabs. For example, compared Sentiment tab for Review 2 against Sentiment tab for Review 1 on screen XYZ above and you can see on screen below that the second review has ***0.99 Positive & 0.00 Negative*** while first review displayed on screen XYZ above has ***0.00 Positive & 0.98 Negative***. Based on this input, you might want to go with Review 2 instead of Review 1



Screen 171

14.3 Amazon Rekognition

Identify object, people, text, scene & activities I images & video as well as detect any inappropriate content. Easy to add image, video analysis to your APP using proven, highly scalable deep learning technology

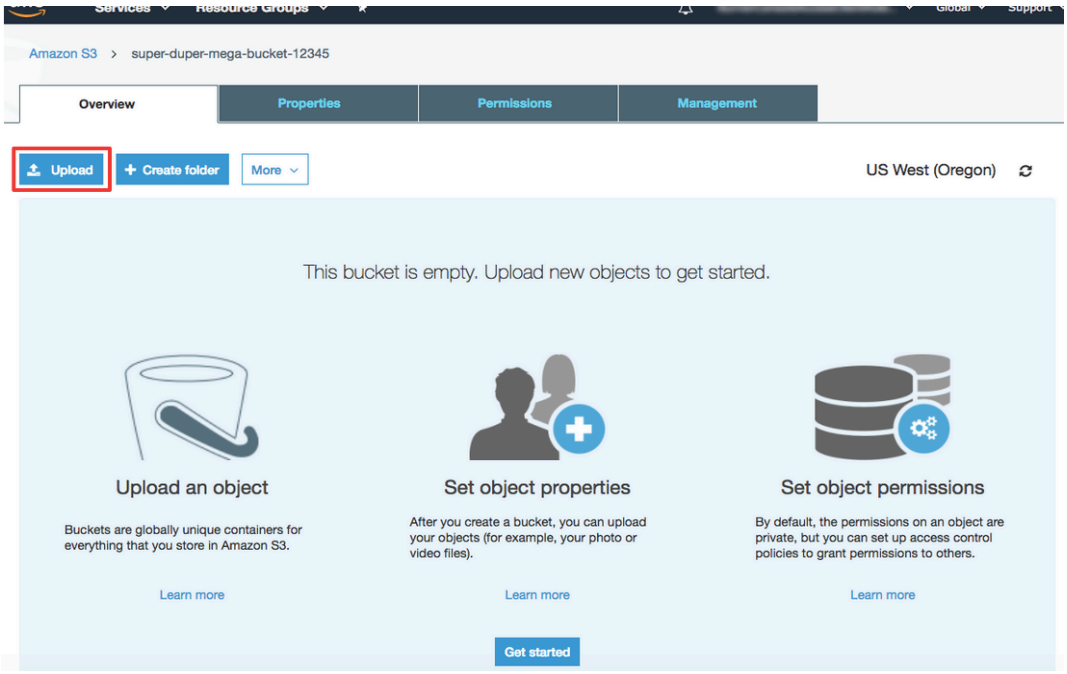


Screen 172

14.4 Amazon Transcribe

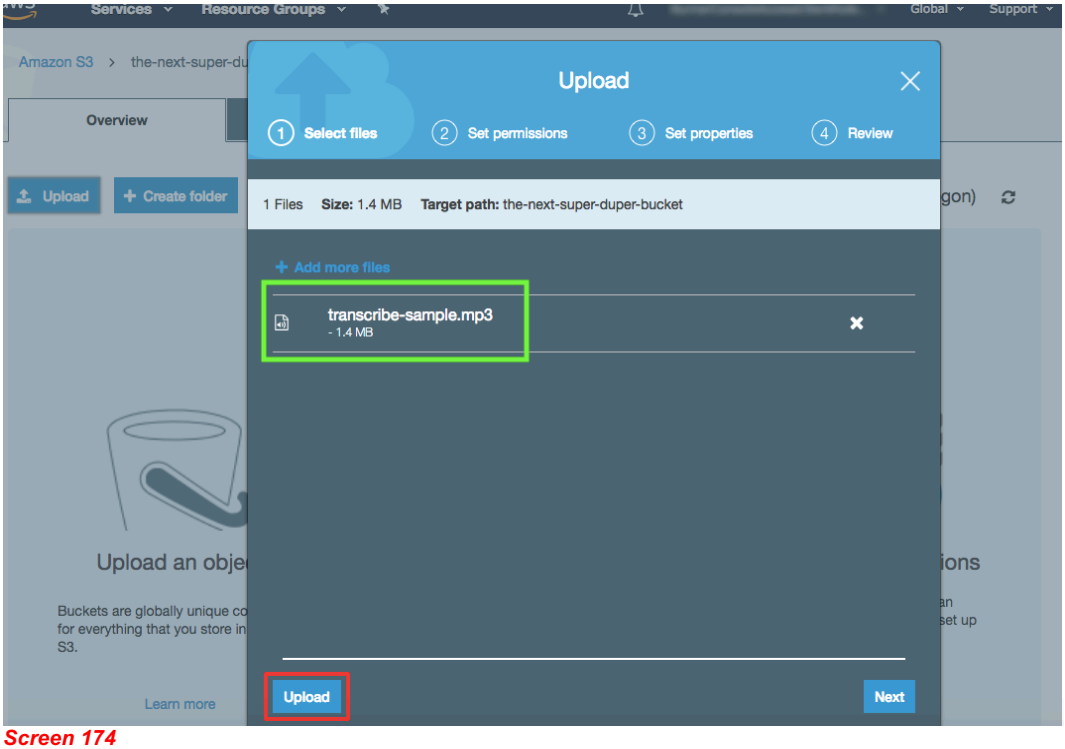
It is an Automated Speech Recognition (ASR). Uses deep learning process to convert SPEECH to TEXT quickly & accurately.

You need to do some preparation steps to use Amazon Transcribe. When you have done the preparation steps, you can click ***Upload*** button displayed below



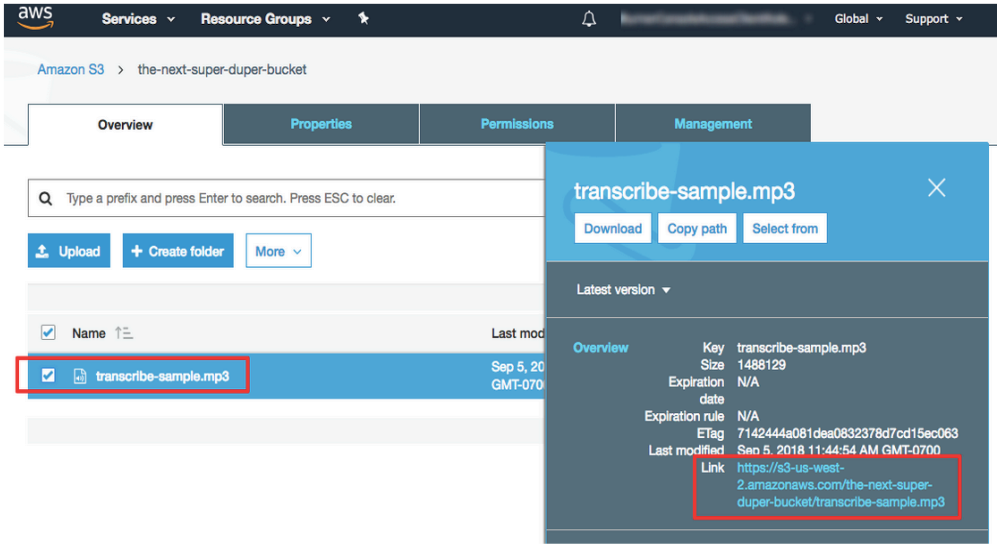
Screen 173

You will see screen below then you will need to upload the mp3 file consists of voices that you want to convert to text



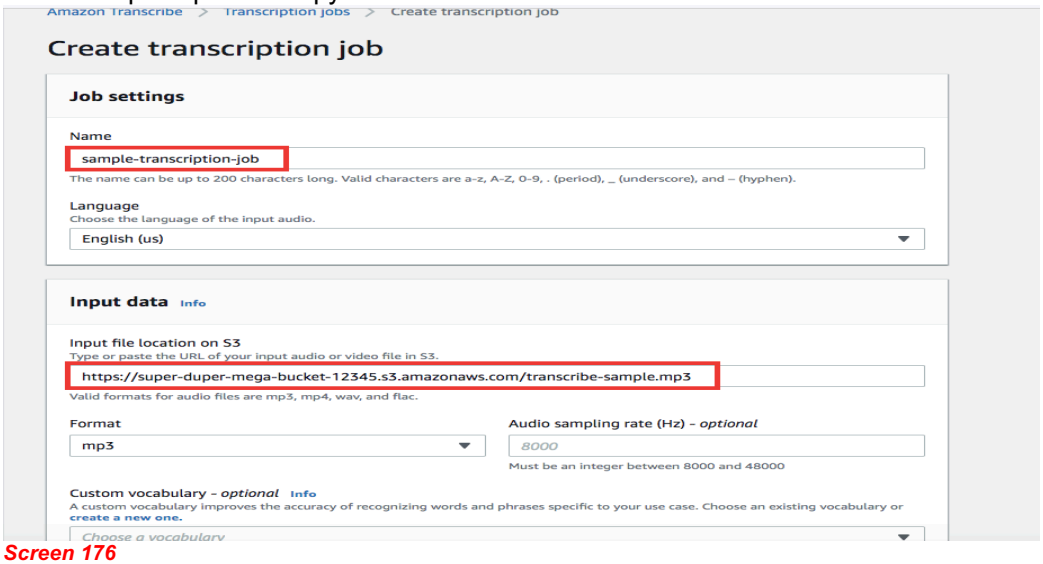
Screen 174

Click Upload from screen above and you will see screen below.



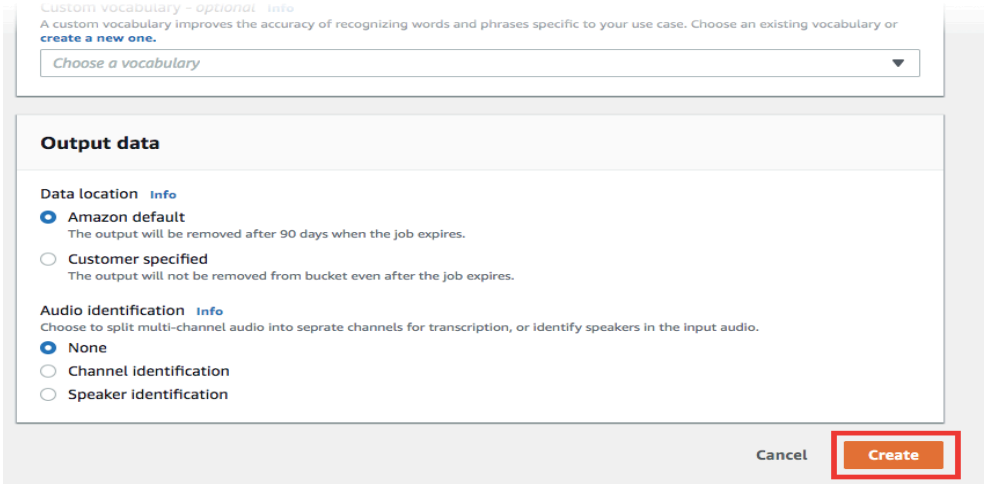
Screen 175

Select the checkbox next to the *transcribe-sample.mp3* file in your bucket. A file detail pane will be displayed for the transcribe-sample.mp3 file. Copy the link to the file and save it for use later in the tutorial.



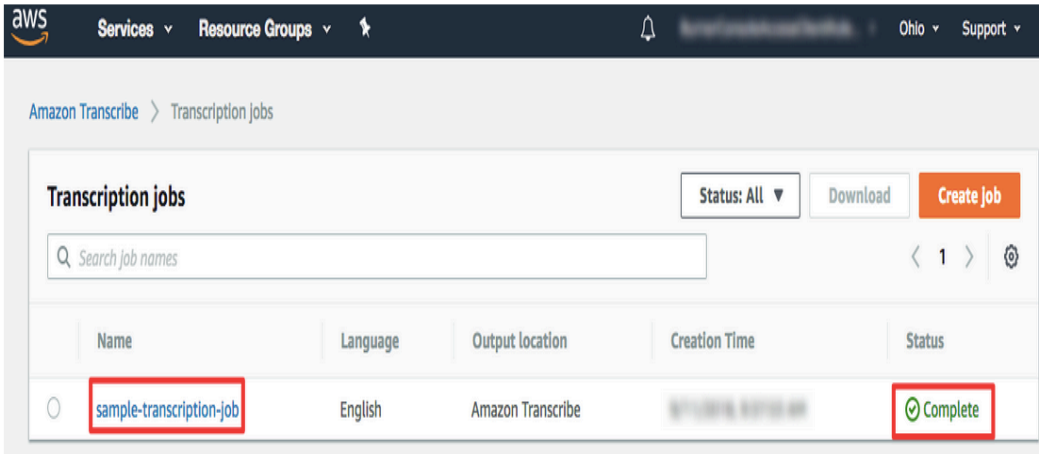
Screen 176

Now you have your input file (mp3 file – an audio file) and simply activate Amazon Transcribe to covert your audio file (mp3 file) into text (output)



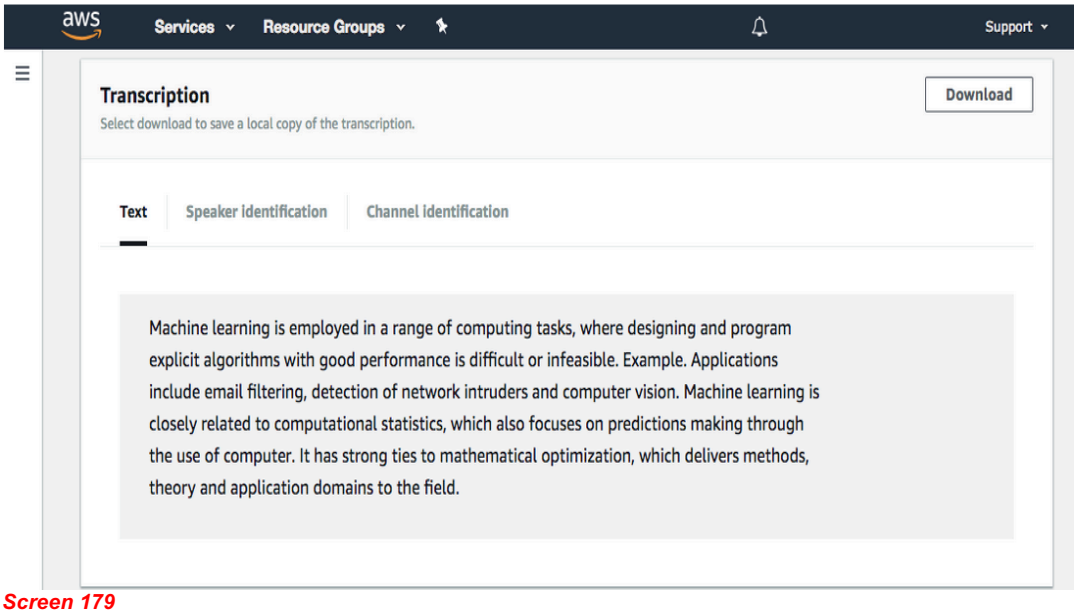
Screen 177

Click ***Create*** from screen above and after you click the ***Create*** button, you will be taken to the ***Transcription jobs*** screen below.



Screen 178

It will show the status of *sample-transcription-job*. The status can be ***In progress***, ***Complete***, or ***Failed***. When the status is ***Complete***, click on the *sample-transcription-job* link in the ***Name*** column to view the transcription results.

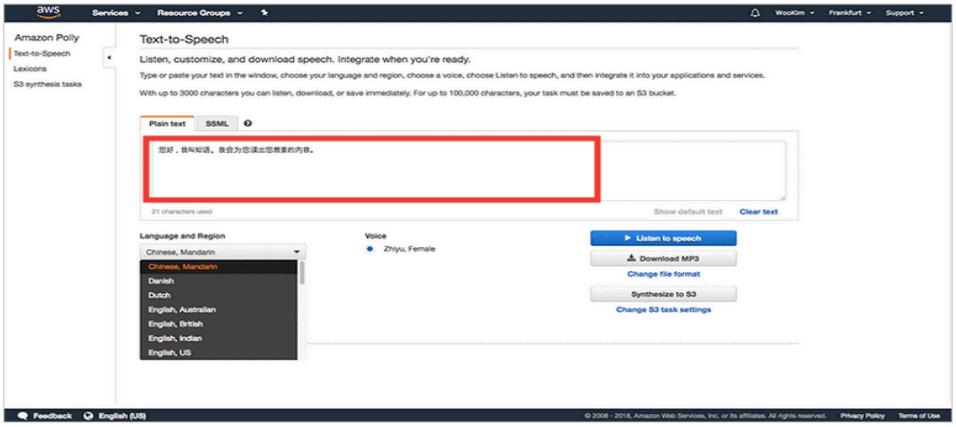


Screen 179

This is the end result; you have successfully converted an audio file as an input (mp3) into text-based output.

14.5 Amazon Polly

It turns TEXT into SPEECH – allowing you to create APP that talk *Create applications that TALK.*
Amazon Polly offers Neural Text-to-Speech (NTTS) voices that deliver advanced improvements in speech quality through a new machine learning approach. It's the opposite of Amazon Transcribe. Here on screen below, you can type your input (TEXT) and the output will be voice automated



Screen 180

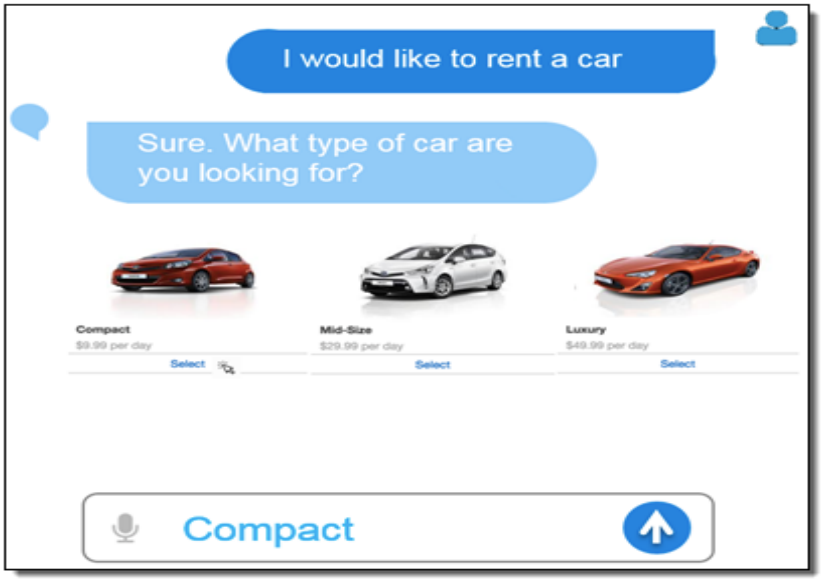
For example, Zhiyu introduces herself in Chinese Mandarin voice clipped on the Amazon Polly website:

https://aws.amazon.com/blogs/machine-learning/meet-zhiyu-the-first-mandarin-chinese-voice-for-amazon-polly/

"大家好，我叫知语，我是亚马逊 Polly 的中文女声，很高兴认识大家。." The English translation is "Hello, my name is Zhiyu. I'm the Chinese Mandarin voice of Amazon Polly. Very nice to meet you."

14.6 Amazon LEX

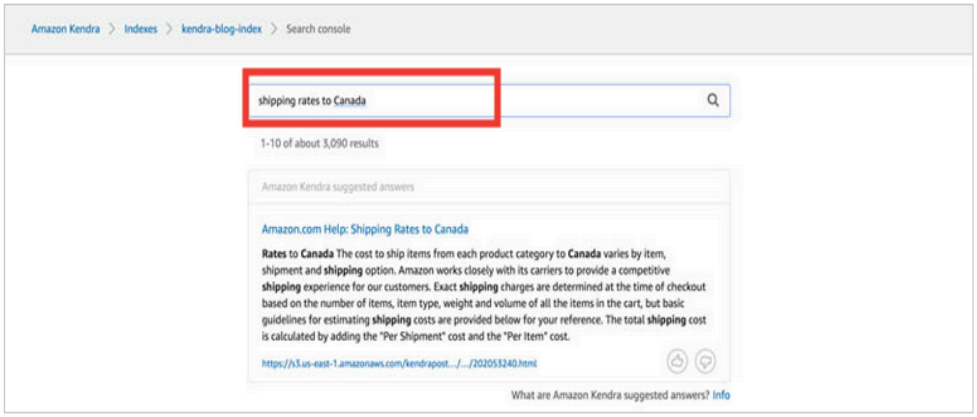
Building conversational interface into any application using voice and text. It provides high-quality *speech recognition* & language understanding capabilities, enabling the addition of sophisticated, natural language *Chatbots* to new existing applications. For example, let's say you are building an application for a rental car company, you can use Amazon LEX for to have Chatbots conversation like displayed on screen below with automated voice



Screen 181

14.7 Amazon Kendra

It is an Intelligent Search Service by Machine Learning. It is a Powerful Search tool that can dig into knowledge resources.



Screen 182

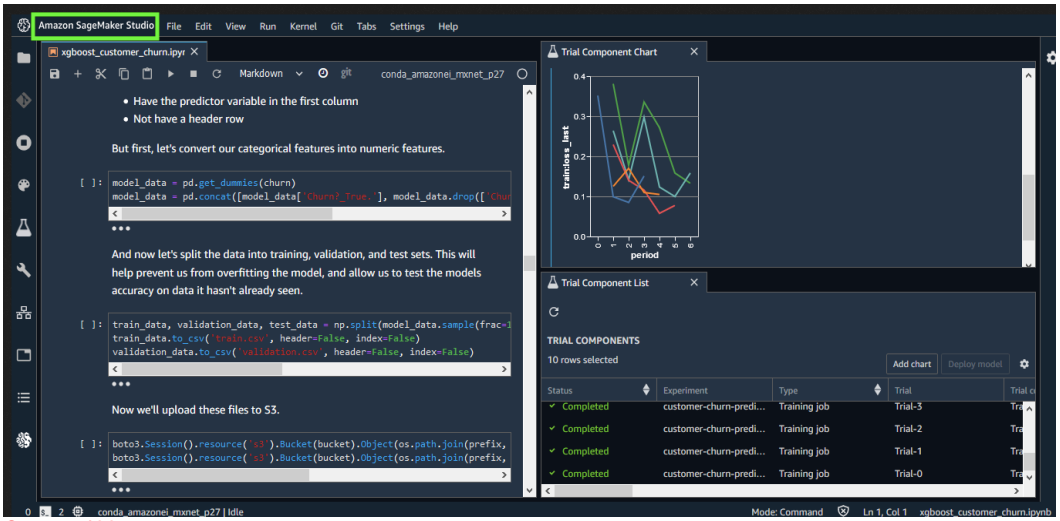
Amazon Kendra works like a Google search but way more efficient and more interactive. You need to do some setups before using Amazon Kendra. Once, everything is setup properly, you can use Amazon Kendra displayed on screen above. In this example, you would like to know about ***"Shipping rates to Canada"*** Amazon Kendra will give that information to you.

Amazon Kendra is an intelligent search service powered by machine learning. Kendra reimagines enterprise search for your websites and applications so your employees and customers can easily find the content they are looking for, even when it's scattered across multiple locations and content repositories within your organization.

Amazon Kendra can be used to document search service that can extract answers from text within documents.

14.8 Amazon SageMaker

Build, train, and *deploy Machine Learning models* at any scale quickly & easily. Remove **ALL** the barriers that typically slow down developers who want to use Machine Learning



Screen 183

Amazon SageMaker studio unifies at last all the tools needed for ML development. Developers can write code, track experiments, visualize data, and perform debugging and monitoring all within a single, integrated visual interface, which significantly boosts developer productivity.

In addition, since all these steps of the ML workflow are tracked within the environment, developers can quickly move back and forth between steps, and also clone, tweak, and replay them. This gives developers the ability to make changes quickly, observe outcomes, and iterate faster, reducing the time to market for high quality ML solutions.

Amazon SageMaker is a fully managed service that provides every developer and data scientist with the ability to build, train, and deploy machine learning (ML) models quickly. SageMaker removes the heavy lifting from each step of the machine learning process to make it easier to develop high-quality models.

Amazon SageMaker can be used to develop and test fully functional machine learning models

14.9 Amazon Personalize

It enables developers to build application with the same Machine Learning technology used by Amazon. It is a fully managed Machine Learning service that goes beyond rigid static rule-based recommendation systems and trains, tunes, and deploys custom ML models to deliver *highly customized recommendations to customers* across industries such as retail and media and entertainment.

Amazon Personalize is useful in creating recommendations. Amazon Personalize makes it easy for developers to build applications capable of delivering a wide array of personalization experiences, including specific product recommendations, personalized product re-ranking, and customized direct marketing.

Amazon Personalize can be used to recommend personalized products for users based on their previous purchases.

14.10 Amazon Forecast

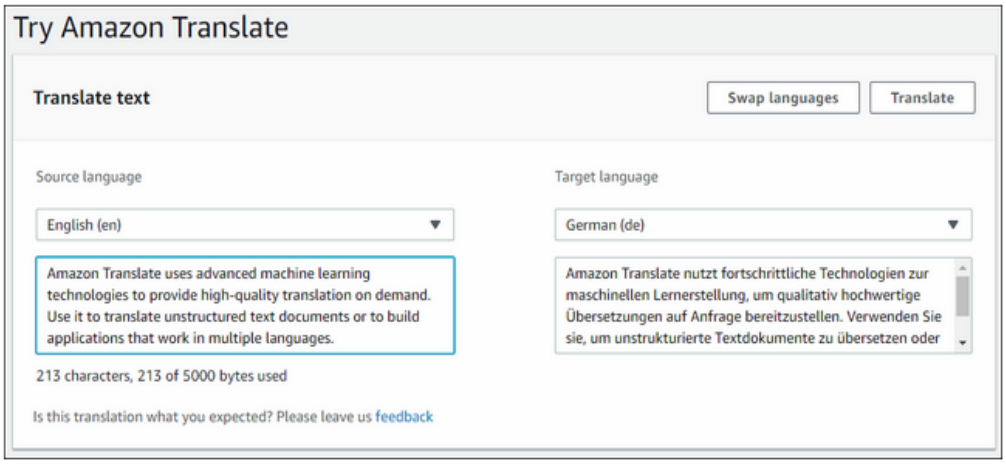
Amazon Forecast is a fully managed service that uses machine learning to deliver highly accurate forecasts. Based on the same technology used at Amazon.com, Amazon Forecast uses machine learning to combine time series data with additional variables to build forecasts. Amazon Forecast requires no machine learning experience to get started. You only need to provide historical data, plus any additional data that you believe may impact your forecasts.

Amazon Forecast can be used to forecast any time-series data, such as retail demand, manufacturing demand, travel demand, revenue, IT capacity, logistics, and web traffic.

It can be used to predict the web traffic of a website for the next few weeks.

14.11 Amazon Translate

It's **a neural machine translation service** that delivers fast, high-quality, affordable, and customizable language translation.

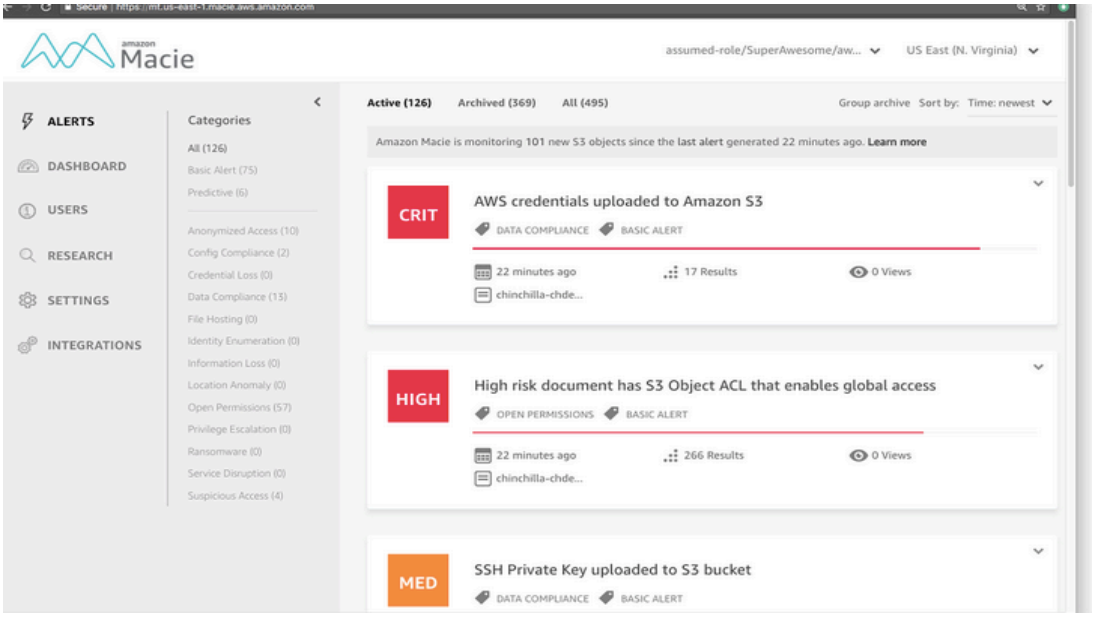


Screen 184

Screen above displays English to German translation performed by Amazon Translate

14.12 Amazon Macie

It is a fully managed data security and data privacy service that uses Machine Learning and pattern matching to discover and protect your sensitive data in Amazon S3



Screen 185

14.13 Amazon QuickSight

It is a scalable, serverless, embeddable, Machine Learning powered Business Intelligence (BI) Service built for the cloud.

Amazon QuickSight lets you easily create and publish interactive BI Dashboard and receive answer in seconds through Natural Language queries.

Screen 186

15 ELB, AWS Auto Scaling & AWS Global Accelerator

WARNING: Your Credit Card will be charged if you decide to active ELB Resources & AWS Global Accelerator, but AWS Auto Scaling is always FREE

15.1 Elastic Load Balance (ELB)

ELB distributes traffic load evenly across the availability EC2 instances, routes to heathy instances and STOP sending to unhealthy instances.

ELB has the following benefits:

- High availability
- Automatic scaling
- Fault Tolerant (uninterrupted service)

There are three types of Load Balancers in AWS

15.1.1 Application Load Balance (ALB)

ALB is used to balance Layer 7 (Application). It supports HTTP & HTTPS protocols, and it is good for Web Applications, Microservices and Containers

15.1.2 Network Load Balance (NLB)

NLB is used to balance Layer 4 (Transport). It supports TCP, TLS & UDP protocols, and it is good for Extreme Performance.

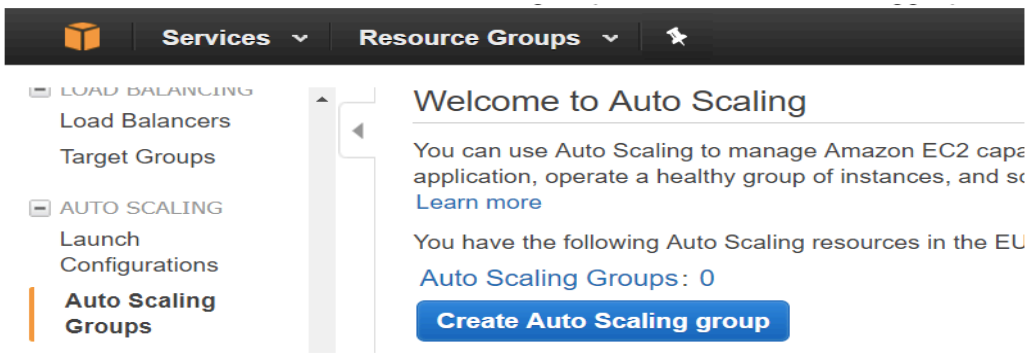
15.1.3 Classic Load Balance

CLB is used to balance Layer 4 (Transport) and Layer 7 (Application). It supports TCP, TLS, UDP, HTTP & HTTPS protocols. Please AVOID if possible – it's not recommended by AWS.

15.2 AWS Auto Scaling

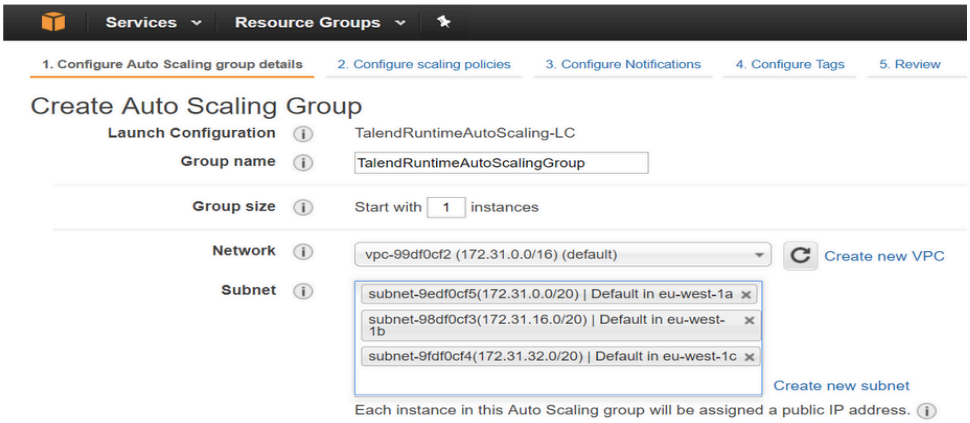
AWS Auto Scaling is always ***FREE*** to use. It automatically adjusts capacity by provisioning new EC2 Instances in case if the traffic increases, but it does not distribute compute capacity across EC2 instances.

From AWS Management Console type Auto Scaling and you will see screen below



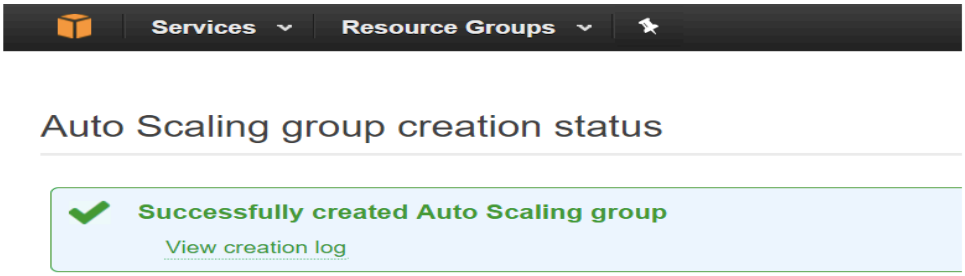
Screen 187

Click Create Auto Scaling group and follow instruction until you see screen below



Screen 188

Once you have successfully created your auto scaling, you will see a conformation screen below



Screen 189

Just keep in mind about Auto Scaling:

- Auto Scaling increases the instance when threshold value is exceeded
- Auto Scaling removes the instance when it is not being utilized

15.2.1 Predictive Auto Scaling

Predictive Auto Scaling uses machine learning to predict capacity requirements based on historical data from CloudWatch. The machine learning algorithm consumes the available historical data and calculates capacity that best fits the historical load pattern, and then continuously learns based on new data to make future forecasts more accurate.

Predictive Auto Scaling can be used to manage a workload that exhibits recurring load patterns that are specific to the day of the week or the time of day**.**

Use predictive scaling to increase the number of EC2 instances in your Auto Scaling group in advance of daily and weekly patterns in traffic flows.

Predictive scaling is well suited for situations where you have:

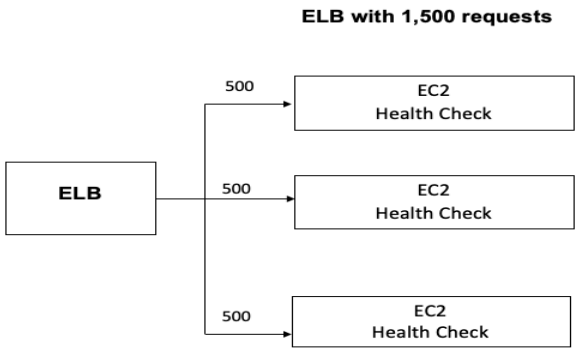
- Cyclical traffic, such as high use of resources during regular business hours and low use of resources during evenings and weekends
- Recurring on-and-off workload patterns, such as batch processing, testing, or periodic data analysis
- Applications that take a long time to initialize, causing a noticeable latency impact on application performance during scale-out events

15.3 ELB vs. AWS Auto Scaling

Understand the differences between ELB vs. Auto Scaling.

15.3.1 ELB Scenario 1

How ELB handles 1,500 requests.

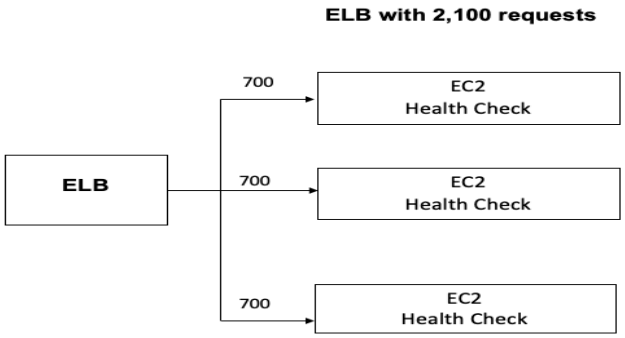


Screen 190

ELB evenly distributes traffic – 500 to each healthy EC2

15.3.2 ELB Scenario 2

How ELB handles 2,100 requests.

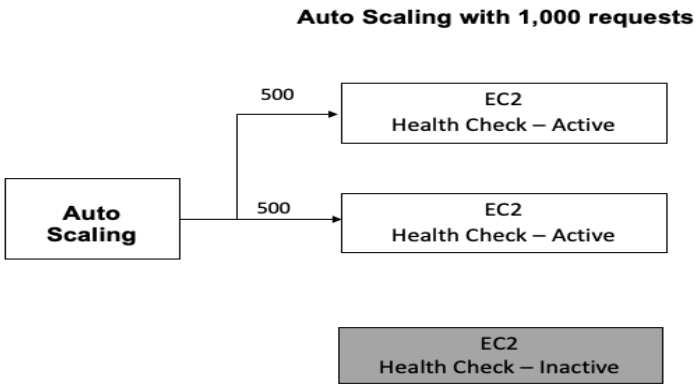


Screen 191

ELB evenly distributes traffic – 700 to each healthy EC2

15.3.3 Auto Scaling Scenario 1

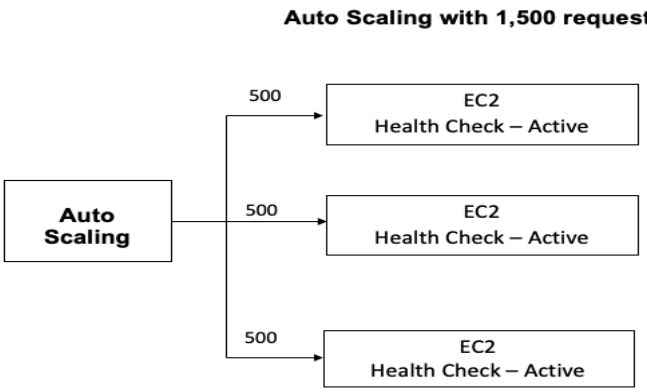
How Auto Scaling handles 1,000 requests.



Screen 192

15.3.4 Auto Scaling Scenario 2

How Auto Scaling handles 1,500 requests.



Screen 193

15.4 AWS Global Accelerator

AWS Global Accelerator is ***a networking service that improves the performance of your users' traffic*** *by up to 60%* using Amazon Web Services' global network infrastructure. Global Accelerator automatically re-routes your traffic to your nearest healthy available endpoint to mitigate endpoint failure.

ELB provides load balancing within one Region, AWS Global Accelerator provides traffic management across multiple Regions.

It improves the availability and performance of your applications with Local or Global Users. AWS Global Accelerator is one of the 5 resources used to provides expanded DDoS attack protection.

Here are the five resources that provides DDoS attack protection for web applications running on the following resources:

1. Amazon Elastic Compute Cloud (EC2)
2. Elastic Load Balancer (ELB)
3. Amazon CloudFront
4. Amazon Route 53
5. AWS Global Accelerator

Benefits of AWS Global Accelerator

- Global Accelerator is a good fit for non-HTTP use case such as gaming, IOT, voice over IP
- Global Accelerator provides static IP addresses that acts as a fixed entry point to your application
- Global Accelerator & Amazon CloudFront use the same edge locations

15.4.1 AWS Global Accelerator vs. S3 Transfer Acceleration

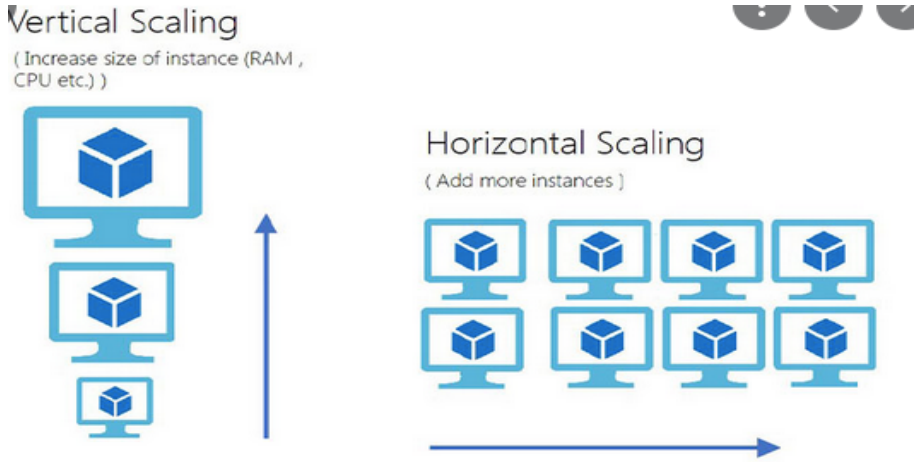
AWS Global Accelerator	***S3 Transfer Acceleration***
Improve the ability and performance of your applications with Local or Global User	*Move data faster over long distance – optimize transfer speed*
Automatically re-routes your traffic to your nearest healthy available endpoint to mitigate endpoint failure	*Fast, easy, secure long distance file transfer*

Screen 194

15.5 Horizontal Scaling vs. Vertical Scaling

Horizontal Scaling	***Vertical Scaling***
Increase capacity by adding more computers/instances to the system	*Increase capacity by adding more CPUs, memory, store to a SINGLE computer*
Fault Tolerance achieved by horizontal scaling	*Running its process on only one computer*

Screen 195


Vertical Scaling
(Increase size of instance (RAM , CPU etc.))
Horizontal Scaling
(Add more instances)

Screen 196

16 AWS Account Types & EC2 Pricing Model

16.1 AWS Account Type: Basic

- Provides access to ONLY 7 core checks
- Does not provide 24x7 phone based technical support
- Included FREE AWS Personal Health Dashboard

Please note that with Basic Plan you have the option with the AWS Free Tier which provides customers the ability to explore and try out AWS services free of charge up to specified limits for each service.

*The Free Tier is comprised of three different types of offerings, a **12-month Free Tier**, an Always Free offer, and short-term trials.*

16.2 AWS Account Type: Developer

WARNING: Your Credit Card will be charged if you decide to select DEVELOPER account type

- Provides access to ONLY 7 core checks
- Does not provide 24x7 phone based technical support
- Included FREE AWS Personal Health Dashboard
- Provides general architecture guidance
- Only allow one contact to open unlimited cases

16.3 AWS Account Type: Business

WARNING: Your Credit Card will be charged if you decide to select BUSINESS account type

- Included FREE AWS Personal Health Dashboard
- Provides 24x7 phone based technical support
- Provides contextual architecture guidance
- Unlimited case with unlimited contacts (IAM Supported)
- Guidance, configuration and troubleshooting of AWS interoperability with third-party software
- AWS Support API provide programmatic access (API Access) to AWS Support Center features to create, manage and close your support cases
- Infrastructure Event Management for additional fee

16.4 AWS Account Type: Enterprise

WARNING: Your Credit Card will be charged if you decide to select ENTERPRISE account type

- Included FREE AWS Personal Health Dashboard
- Provides 24x7 phone based technical support
- Provides consultative review & architecture guidance based on your applications
- Unlimited case with unlimited contacts (IAM Supported)
- Guidance, configuration and troubleshooting of AWS interoperability with third-party software
- AWS Support API provide programmatic access (API Access) to AWS Support Center features to create, manage and close your support cases
- Infrastructure Event Management Well-architected reviews operational reviews

- Provides Technical Account Manager (TAM)
- Provides Access to Online self-paced labs
- Provides Concierge Support Team

16.5 AWS Account Type: Summary Table

	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
Available in ALL Support plan for FREE	*YES Included for FREE AWS Personal Health Dashboard*	*YES Included for FREE AWS Personal Health Dashboard*	*YES Included for FREE AWS Personal Health Dashboard*	*YES Included for FREE AWS Personal Health Dashboard*
Architecture Guidance	*NO*	*YES General Architecture Guidance*	*YES Contextual Architecture Guidance*	*YES Consultative Review & Architecture Guidance based on your applications*
Contact	*NO*	*YES, BUT Only allow ONE contact to open unlimited cases*	*YES Unlimited case with unlimited contacts (IAM Supported)*	*YES Unlimited case with unlimited contacts (IAM Supported)*
AWS Trusted Advisor Best Practices	*NO Full set of checks ONLY 7 core checks ONLY*	*NO Full set of checks ONLY 7 core checks ONLY*	*YES, Ful set of checks*	*YES, Ful set of checks*
24x7 Phone Based-Technical Support	*NO DOES NOT Provide 24X7 Phone based technical support*	*NO DOES NOT Provide 24X7 Phone based technical support*	*YES 24x7 Phone based technical support included*	*YES 24x7 Phone based technical support included*
Third-Party Software Support	*NO*	*NO*	*YES Guidance, configuration & trouble shooting of AWS Interoperability with third party software*	*YES Guidance, configuration & trouble shooting of AWS Interoperability with third party software*
Programmatic access to AWS support center	*NO*	*NO*	*YES AWS Support API Provide Programmatic access (API Access) to AWS Support Center features to create, manage and close your support cases*	*YES AWS Support API Provide Programmatic access (API Access) to AWS Support Center features to create, manage and close your support cases*
Infrastructure Event Management	*NO*	*NO*	*YES, BUT Infrastructure Event Management for additional fee*	*YES Infrastructure Event Management Well-architected reviews operational reviews*
Technical Account Management	*NO*	*NO*	*NO*	*YES*
Access to online self-paced lab	*NO*	*NO*	*NO*	*YES*
Concierge support team	*NO*	*NO*	*NO*	*YES*

Screen 197

16.6 EC2 Pricing Model: On-Demand

WARNING: Your Credit Card will be charged if you decide to select ON-DEMAND – EC2 Pricing Model

- Short-term application
- No upfront commitment
- No long-term commitment
- Pay for compute capacity by hour/second whatever you use

- Cannot be interrupted

16.7 EC2 Pricing Model: Reserved-Instance

WARNING: Your Credit Card will be charged if you decide to select RESERVED-INSTANCE – EC2 Pricing Model

- Long-term application
- With commitment – minimum one year
- Available for Amazon RDS & Amazon EC2
- Cannot be interrupted
- Discount up to 70% from on-Demand
- For more flexibilities – select Convertible Reserved Instance

You can optimize EC2 cost by performing the following actions:

- Purchase EC2 Reserved Instance
- Set up auto scaling groups to align number of instances in demand

16.8 EC2 Pricing Model: Spot-Instance

WARNING: Your Credit Card will be charged if you decide to select SPOT-INSTANCE – EC2 Pricing Model

- Applications that have flexible start & end dates
- Not suitable for critical workloads that need to run at a specific point of time
- *Can be interrupted (The only instance that can be interrupted)*
- Discount up to 90% from on-Demand

Please note that if your Spot-Instance is terminated by Amazon in the first hour, you will not be charged for that usage. For any subsequent hour (after the first hour), if you are running on windows and you terminate the instance yourself, you will be charged for the entire hour

16.9 EC2 Pricing Model: Dedicated-Host

WARNING: Your Credit Card will be charged if you decide to select DEDICATED-HOST – EC2 Pricing Model

- Not sharing with other AWS customers
- You will have a dedicated physical server and it will be fully dedicated for your own use
- It allows you to use your own eligible software licenses from any vendors of your choice
- Cannot be interrupted
- The most expensive option

16.10 AWS Savings Plans

AWS offers two types of Savings Plans:

1. **Compute Savings Plans** provide the most flexibility and help to reduce your costs by up to 66%. These plans automatically apply to EC2 instance usage regardless of instance family, size, AZ, region, OS or tenancy, and also apply to Fargate and Lambda usage. For example, with Compute Savings Plans, you can change from C4 to M5 instances, shift a workload from EU (Ireland) to EU (London), or move a workload from EC2 to Fargate or Lambda at any time and automatically continue to pay the Savings Plans price.

2. **EC2 Instance Savings Plans** provide the lowest prices, offering savings up to 72% in exchange for a commitment to the usage of individual instance families in a region (e.g. M5 usage in N. Virginia). This automatically reduces your cost on the selected instance family in that region regardless of AZ, size, OS or tenancy. EC2 Instance Savings Plans give you the flexibility to change your usage between instances within a family in that region. For example, you can move from c5.xlarge running Windows to c5.2xlarge running Linux and automatically benefit from the Savings Plans prices.

17 IaaS vs. PaaS vs. SaaS

17.1 Infrastructure as a Service (IaaS)

IaaS (Infrastructure as a Service), as the name suggests, provides you the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, servers, firewalls, load balancers, IP addresses, virtual local area networks etc.

17.1.1 IaaS: AWS CloudFormation

It is an infrastructure as a code service that allows you easily model, provision, and manage AWS third-party resources. AWS CloudFormation is a great tool for regional expansion, great for code review infrastructure changes. You write a template which contains resources (S3, Lambda, DynamoDB, etc) and upload into CloudFormation

17.1.2 IaaS: Amazon Elastic Compute Cloud (EC2)

EC2 provides scalable infrastructure for companies who want to host cloud-based applications. Hence, EC2 is considered as IaaS. Amazon is responsible for networking, storage, and server utilization EC2 gives you full control over managing the underlying OS, virtual network configurations, storage, data and applications. So EC2 is an example of an IaaS service.

17.2 Platform as a Service (PaaS)

PaaS (Platform as a Service), as the name suggests, provides you computing platforms which typically includes operating system, programming language execution environment, database, web server etc.

17.2.1 PaaS: Amazon RDS

Amazon RDS is a PaaS as it only provides a platform or a set of tools to manage your database instances. AWS is IaaS, but the RDS provided by the AWS is PaaS.

17.2.2 PaaS: Amazon DynamoDB

Services like DynamoDB, Lambda and Kinesis are all in the PaaS category

17.2.3 PaaS: AWS Lambda

AWS Lambda is the most robust service that positions as a strong PaaS, enabling developers to utilize all AWS platform services. Services like DynamoDB, Lambda and Kinesis are all in the PaaS category

17.2.4 PaaS: AWS Fargate

AWS Fargate is a PaaS-like layer on top of ECS that abstracts the infrastructure which enables users to focus on the desired state of the application.

17.2.5 PaaS: AWS Elastic Beanstalk

AWS Elastic Beanstalk is a PaaS offering from AWS, which helps developers deploy applications on the AWS cloud.

17.2.6 PaaS: AWS LightSail

AWS LightSail is a platform as a service (PaaS) mainly targeted for web hosting with Virtual Private Servers (VPS) for lower cost. It’s intended to provide a simple web user interface to Manage the Servers and basic configuration around it.

17.2.7 PaaS: Amazon Kinesis

Services like DynamoDB, Lambda and Kinesis are all in the PaaS category

17.3 Software as a Service (SaaS)

While in SaaS (Software as a Service) model you are provided with access to application software often referred to as "on-demand software". You don't have to worry about the installation, setup and running of the application. Service provider will do that for you. You just must pay and use it through some client.

17.3.1 SaaS: Amazon Rekognition

Amazon Rekognition is a **cloud-based software as a service (SaaS) computer vision platform** that was launched in 2016.

17.3.2 SaaS: Amazon Redshift

AWS **Redshift** are the popular **SaaS** options that offer a complete data warehouse solution in the cloud. Their stack integrates all the four layers and is designed to be highly scalable.

17.3.3 SaaS: AWS Marketplace

AWS Marketplace enables you to discover, buy, and launch dozens of SaaS and API products. Procure on AWS Marketplace and consume directly through the seller's website or API. AWS Marketplace enables you to easily manage your subscriptions in one place, with all charges coming from AWS. AWS Marketplace supports two options for purchasing SaaS and API products

17.4 IaaS, PaaS, SaaS – Summary Table

Category	Description	AWS Resources
Infrastructure as a Service (IaaS)	*The Infrastructure-as-a-Service (IaaS) cloud model has transformed the way cloud computing and storage inf restructure services are attained and administered. Because of this, most organizations have migrated their legacy on-premises processes and applications to the public cloud, avoiding the costs and effort that goes into tasks like backup, archiving, and so on.*	*Amazon EC2* *AWS CloudFormation*
Platform as a Service (PaaS)	*Platforms as a Service (PaaS) removes the need for organizations to manage the underlying inf restructure (usually hardware and operating systems) and allows you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other heavy lifting involved in running your application. PaaS provides the inf restructure and application development platform to easily develop applications over a cloud platform.*	*Amazon RDS* *Amazon DynamoDB* *AWS Lambda* *AWS Fargate* *AWS Elastic Beanstalk* *AWS LightSail* *Amazon Kinesis*
Software as a Service (PaaS)	***Software as a service (SaaS)** is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. SaaS is also known as "on-demand software" and Web-based/Web-hosted software. SaaS is considered to be part of cloud-computing along with Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)*	*Amazon Rekognition* *Amazon Redshift* *AWS Aurora* *AWS Marketplace*

Screen 198

18 Shared Responsibilities: AWS & Customers

18.1 Shared Responsibilities: AWS (Security OF the Cloud)

AWS is responsible for ***"Security OF the Cloud"*** which consists of the following activities below:

- Responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud
- The infrastructure is composed of the hardware, software, networking, and facilities at run AWS cloud services
- Maintaining physical security and anything to do with hardware (storage device decommissioning, disk disposal, hardware patching)
- Maintaining physical & environment control/global infrastructure (Regions, Availability Zones and Edge Location managements)
- Responsible for patch management within infrastructure and maintaining configuration of infrastructure
- Protecting the infrastructure (hardware, software, network)
- Keeping data infrastructure sage from failures
- Replacing fault hardware on Amazon EC2 Instance
- Maintaining Amazon S3 data in different Availability Zones to keep it durable

18.2 Shared Responsibilities: Customers (Security IN the Cloud)

Customer is responsible for ***"Security IN the Cloud"*** which consists of the following activities below:

- Responsible for client site data encryption & data integrity authentication
- Anything to do with data & access management
- Customer assumes responsibility & management of the guest Operating System (OS) – including udates and security patches
- Enabling Data Encryption of data stored in S3 bucket
- Patch & configure their guest OS
- OS, Network, Firewall Configuration Data Encryption
- Managing patches of the guest OS on Amazon EC2
- Identify and Access Management (IAM) – enabled MFA on all accounts & analyze user access patterns & review IAM permissions
- Application software licenses costs

18.3 Shared Responsibilities: AWS & Customers

18.3.1 Configuration Management

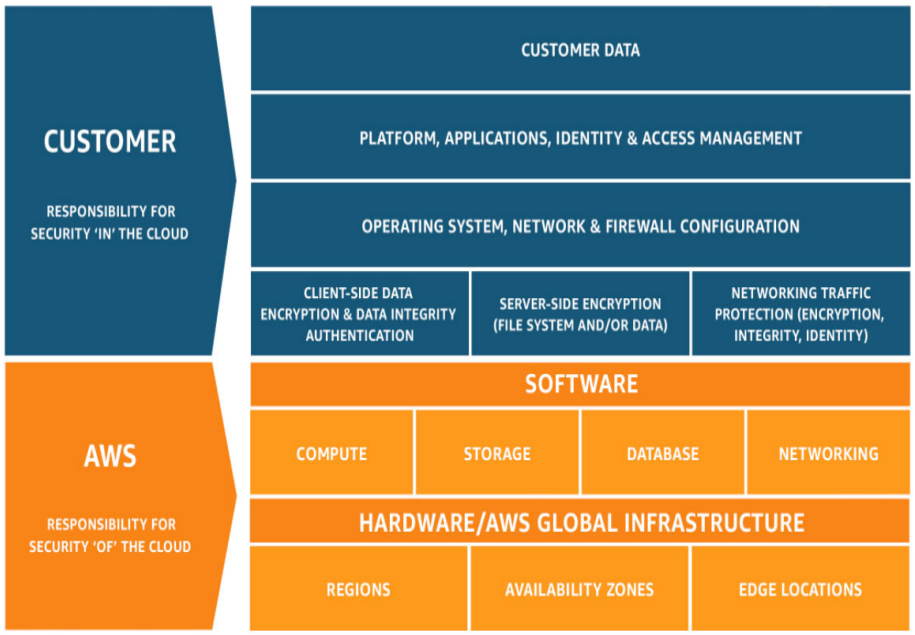
- AWS Maintains the configuration of its infrastructure
- Customers configuring their own OS, Database & application

18.3.2 Patch Management

- AWS patching & fixing flaws in infrastructure
- Customers patching OS & applications

18.3.3 Training

- AWS trains AWS employees
- Customers train their own employees


CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

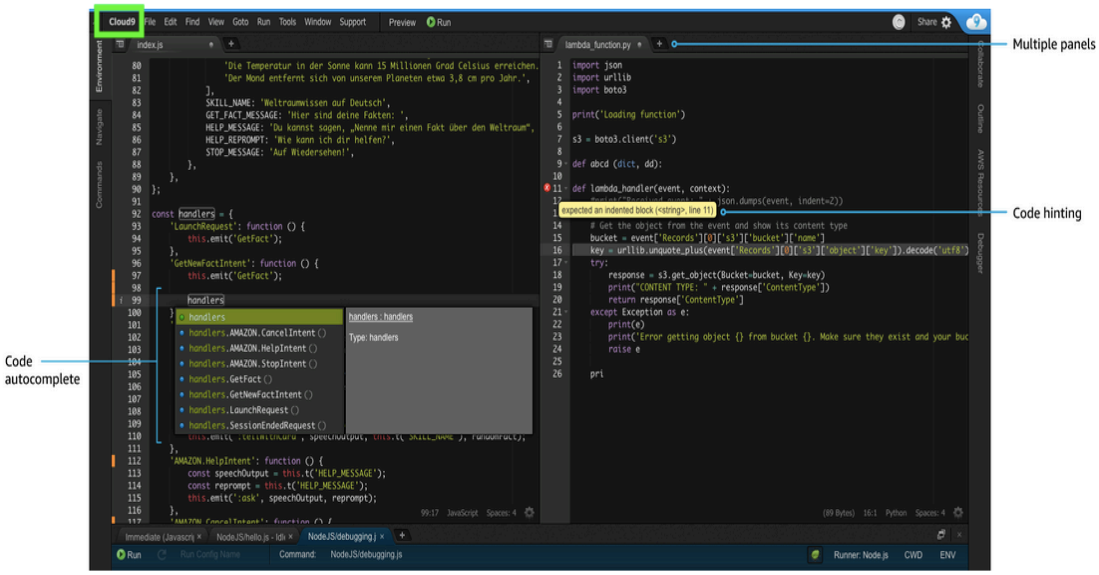
Screen 199

19 Other Services

19.1 Debug Tools

19.1.1 AWS Cloud9

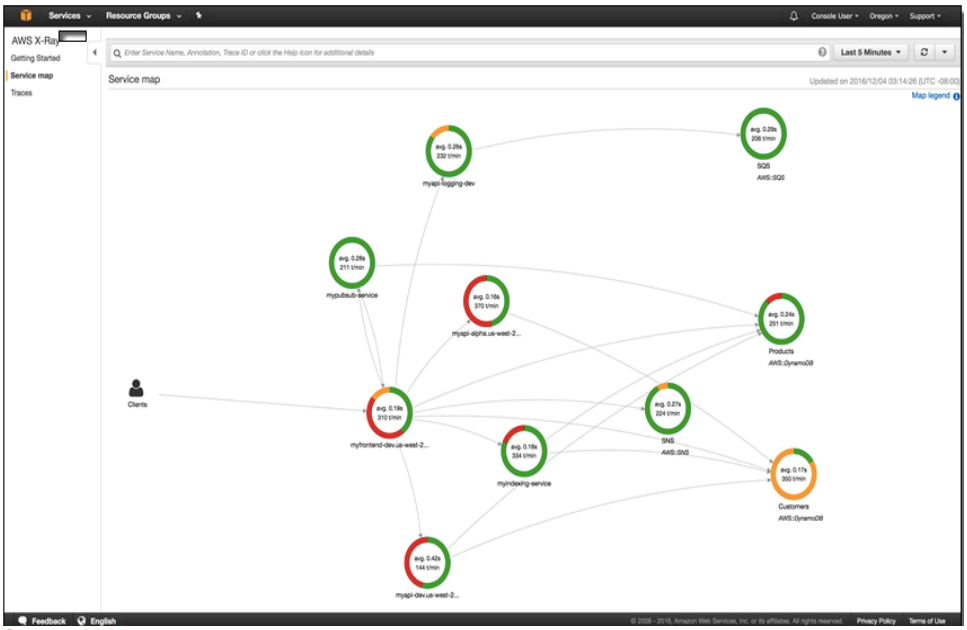
It's an Integrated Development Environment (IDE) that lets you write, run & debug your code with a browser.



Screen 200

19.1.2 AWS X-Ray

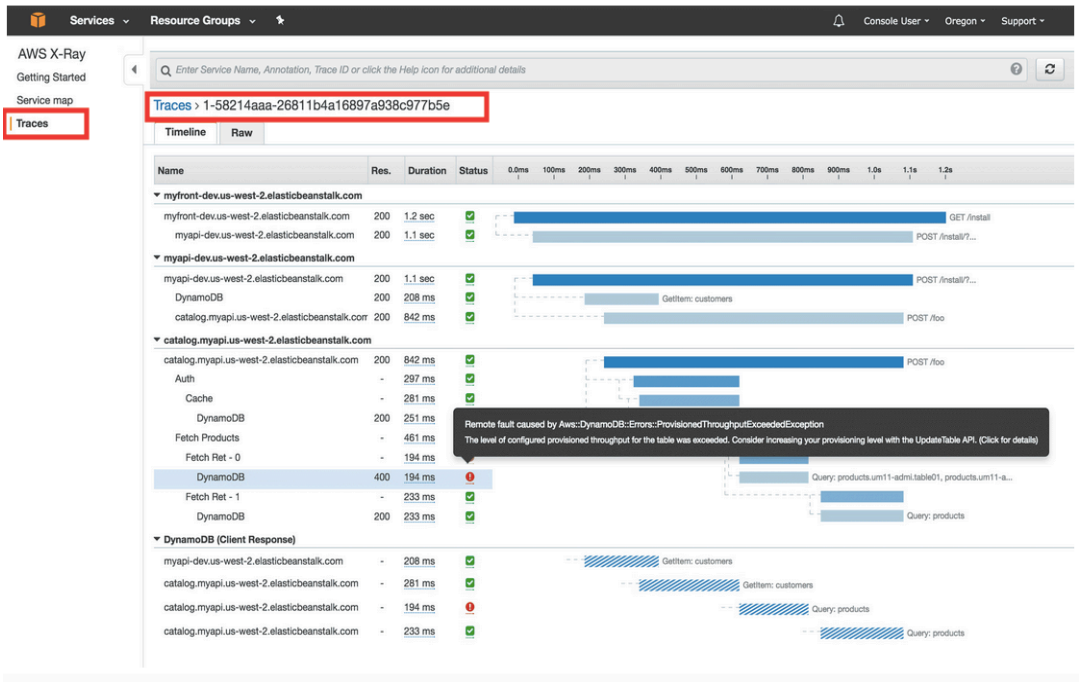
AWS X-Ray is used to analyze and DEBUG production distributed applications, such as those built using a microservices architecture.



Screen 201

AWS X-Ray allows you to trace requests made to your application as execution traverses Amazon EC2 instances, Amazon ECS containers, microservices, AWS database services, and AWS messaging services. It is designed for development and production use and can handle simple three-tier applications as well as applications composed of thousands of microservices.

As I showed you last year, X-Ray helps you to perform end-to-end tracing of requests, record a representative sample of the traces, see a map of the services and the trace data, and to analyze performance issues and errors. This helps you understand how your application and its underlying services are performing so you can identify and address the root cause of issues.



Screen 202

AWS X-Ray creates a map of services used by your application with trace data that you can use to drill into specific services or issues. This provides a view of connections between services in your application and aggregated data for each service, including average latency and failure rates. You can create dependency trees, perform cross-availability zone or region call detections, and more.

19.2 Integration Services

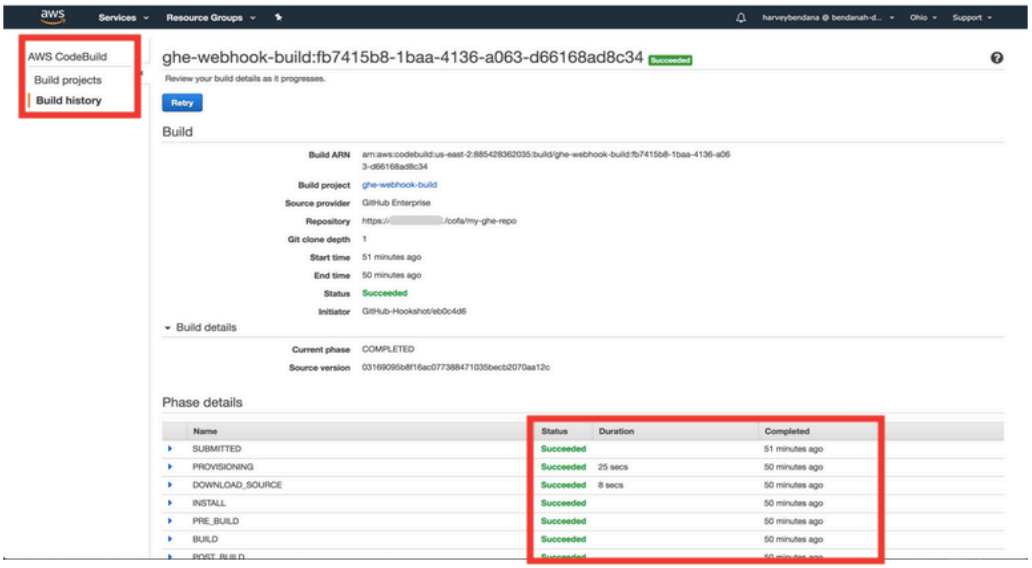
19.2.1 AWS CodeBuild

AWS CodeBuild is a Fully Managed *continuous integration service* that compiles source code, run, tests, and produces software packages that are ready to deploy. AWS CodeBuild scales continuously and process multiple builds concurrently, so your builds are not left waiting in a queue.

Proper set up is required to have AWS CodeBuild running. You would need the following:

- You'll need an AWS account.
- You'll need a GitHub Enterprise implementation with a repo. If you'd like to deploy one inside your own Amazon VPC.
- You'll need an S3 bucket to store your GitHub Enterprise self-signed SSL certificate.

Once you have setup everything properly, you will see screen below displayed AWS CodeBuild. The screen gives you the current status and when you completed the deployment under ***Build History*** tab on the left side of the screen.



Screen 203

19.2.2 AWS Glue

AWS Glue is a Fully Managed ETL service that makes it easy for customers to prepare & load their data for Analytics. It is a *SERVERLESS Data Integration Service*. ETL Load for Analytics

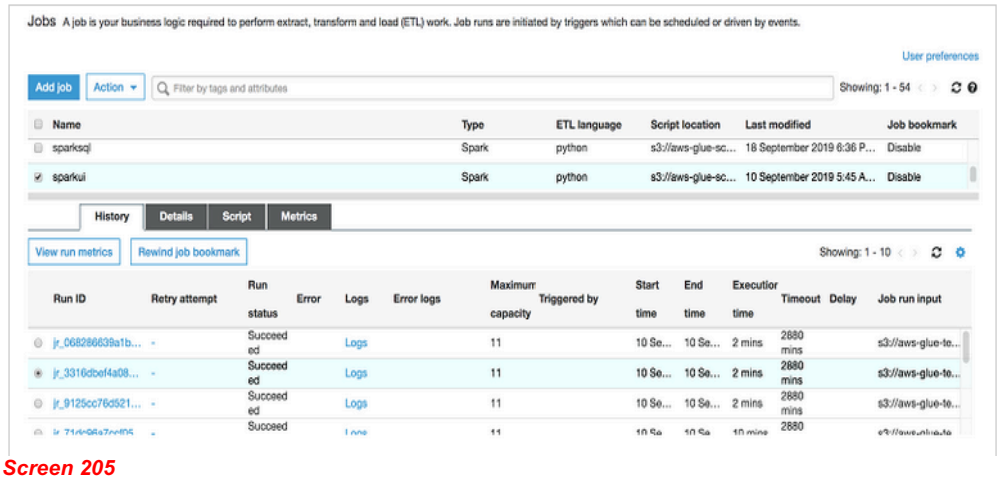
```
import sys
from awsglue.transforms import *
from awsglue.utils import getResolvedOptions
from pyspark.context import SparkContext
from awsglue.context import GlueContext
from awsglue.job import Job

## @params: [JOB_NAME]
args = getResolvedOptions(sys.argv, ['JOB_NAME'])
sc = SparkContext()
glueContext = GlueContext(sc)
spark = glueContext.spark_session

job = Job(glueContext)
job.init(args['JOB_NAME'], args)
datasource0 = glueContext.create_dynamic_frame.from_catalog(database = "firehose_s3_db",
                table_name = "firehose_s3_raw_table",
                transformation_ctx = "datasource0")
```

Screen 204

The following code example displayed above is how to use job bookmarks in a Glue ETL job that reads from a AWS Glue table backed by a Amazon S3 location. The job receives new files from a Kinesis Firehose event stream in JSON format, transforms to rename two columns, converts and writes it out to Amazon Redshift. `transformation_ctx` is the identifier for the job bookmark associated with this data source. For proper operation, you need `job.init` & `job.commit` to initialize and persist the bookmark state.

AWS Glue's Spark runtime has a mechanism to store state. This mechanism is used to track data processed by a particular run of an ETL job. The persisted state information is called *job bookmark*.

The snapshot above shows a view of the Glue Console with multiple job runs at different time instances of the same ETL job. Job bookmarks are used by AWS Glue jobs to process incremental data since the last job run. A job bookmark is composed of the states of various job elements, such as sources, transformations, and targets. For example, your AWS Glue job might read new partitions in an S3-backed table. AWS Glue tracks the partitions that the job has processed successfully to prevent duplicate processing and writing the same data to the target data store multiple times.

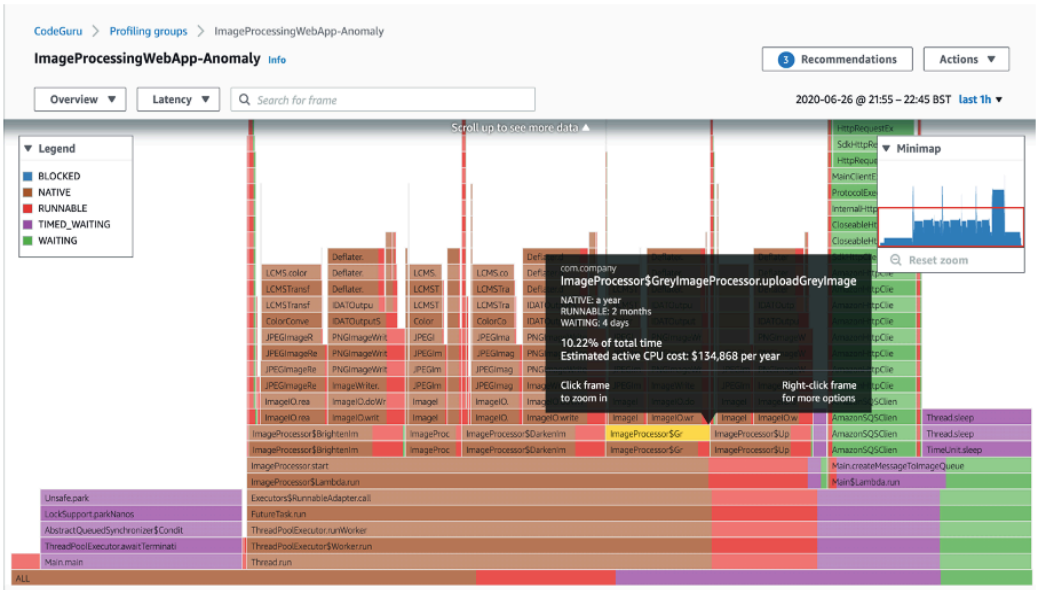


Screen 205

19.3 Code Review – Developer Tool

19.3.1 Amazon CodeGuru

Amazon CodeGuru is a developer tool that provides intelligent recommendations to *improve code quality* and identity an application's *most expensive line of code*



Screen 206

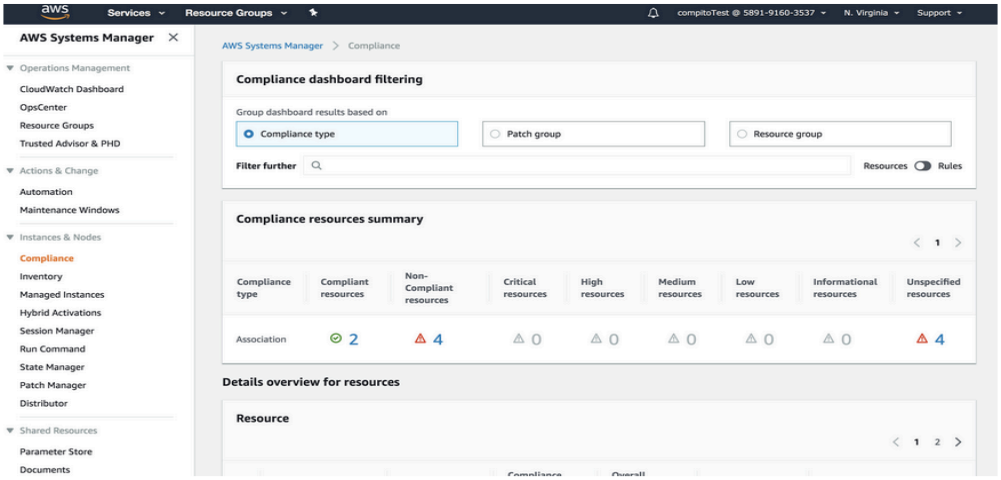
19.4 Visibility, Control, Govern, Organize & Resource Management

19.4.1 AWS System Manager

AWS System Manager is used for Visibility & Control of your Infrastructure on AWS Cloud
It used to automate *Operational Tasks* – collecting software inventory, running command, and *managing patches*

AWS System Manager allows you to *CENTRALIZE* operational data from multiple AWS services
AWS System Manager is also used for Operational Insights – quickly identify and issue that might impact APP using the resources.

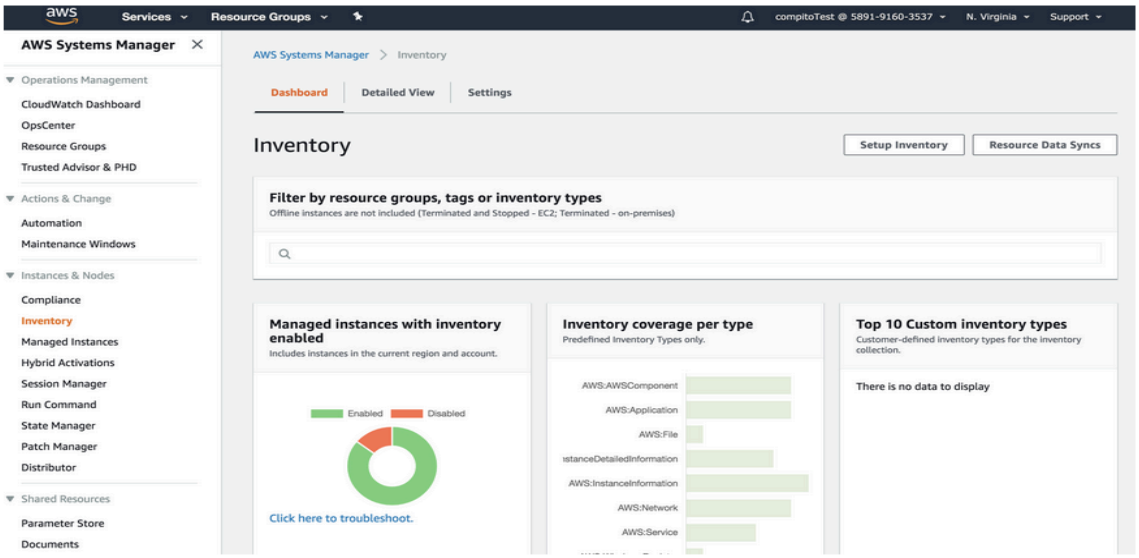
Finally, AWS System Manager also used to automatically collect software Inventory, *apply OS patches*, create system images.



Screen 207

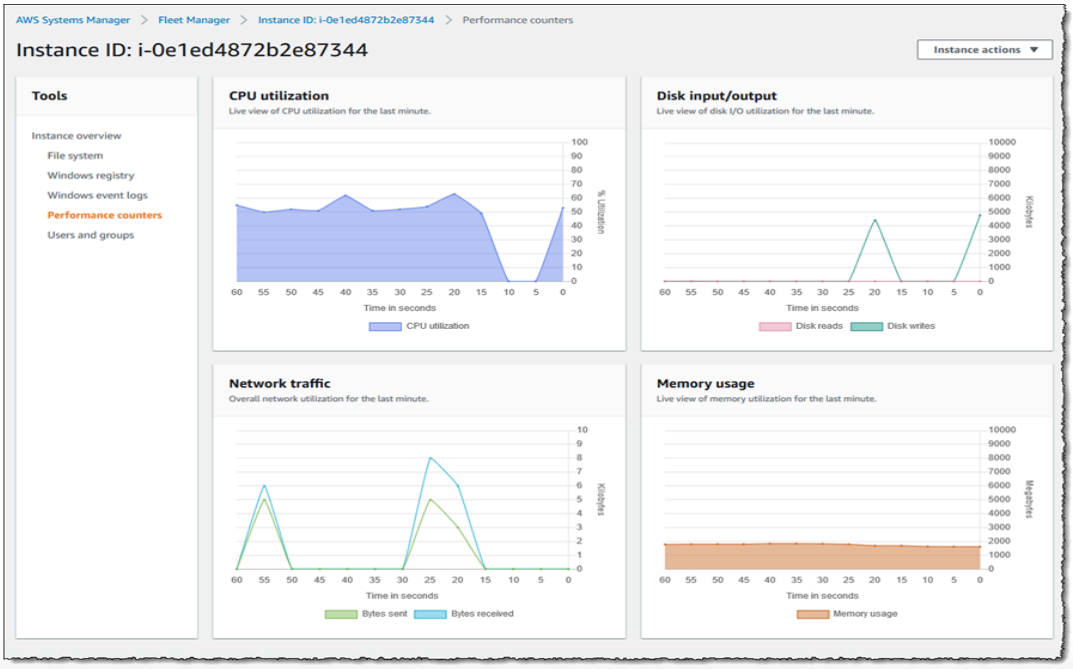
In other words, you can say that AWS Systems Manager allows you to centralize operational data from multiple AWS services and automate tasks across your AWS resources. You can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments.

With Systems Manager, you can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status.



Screen 208

You can also take action on each resource group depending on your operational needs. Systems Manager provides a central place to view and manage your AWS resources, so you can have complete visibility and control over your operations.



Screen 209

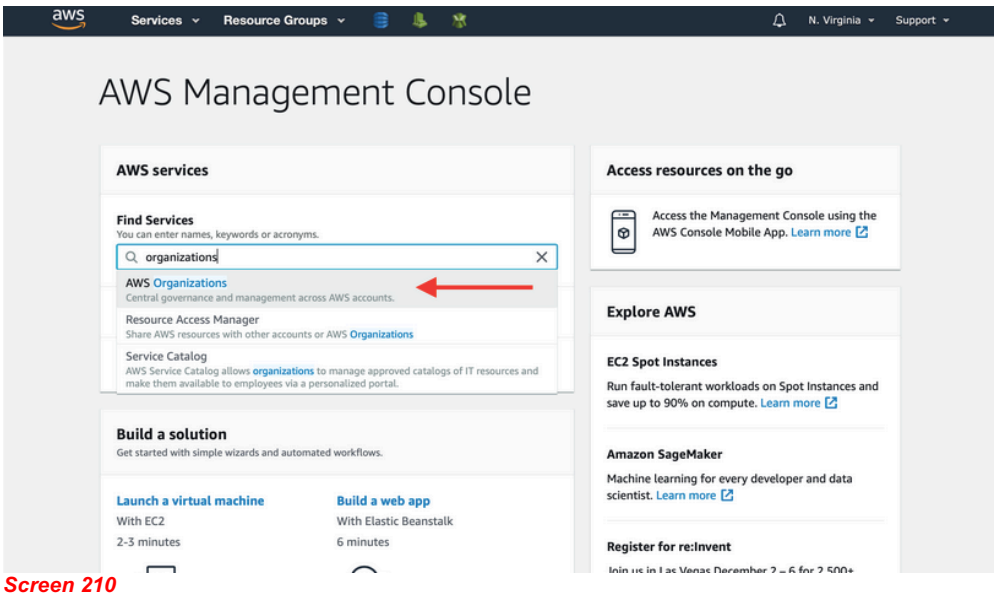
19.4.2 AWS Organizations

AWS Organizations helps you *centrally manage and govern your environment* as you grow and scale your AWS resources.

By using AWS Organizations, you can programmatically *create new AWS accounts, allocate resources, group accounts to organize your workloads*, and apply policies to accounts or groups of accounts for governance.

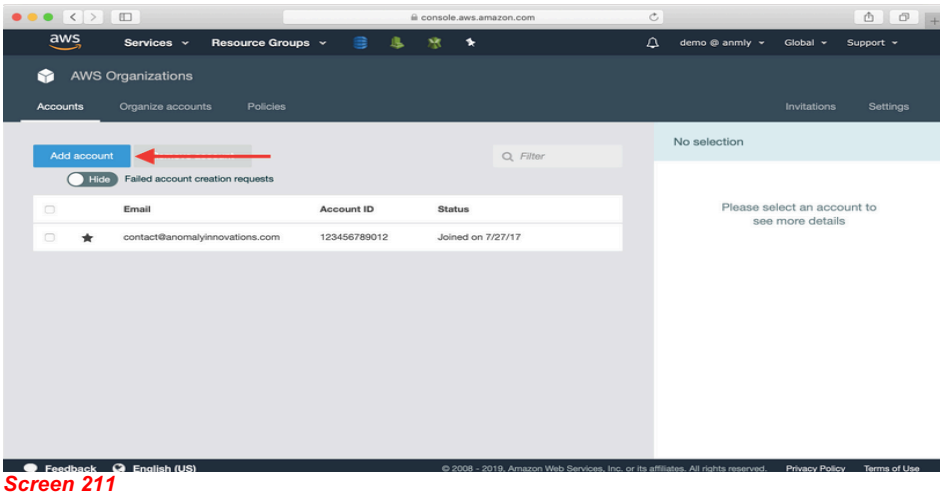
AWS organization *consolidates your AWS accounts so that you can administer them as a single unit.*

From AWS Management Console type ***Organizations*** – refer to screen below



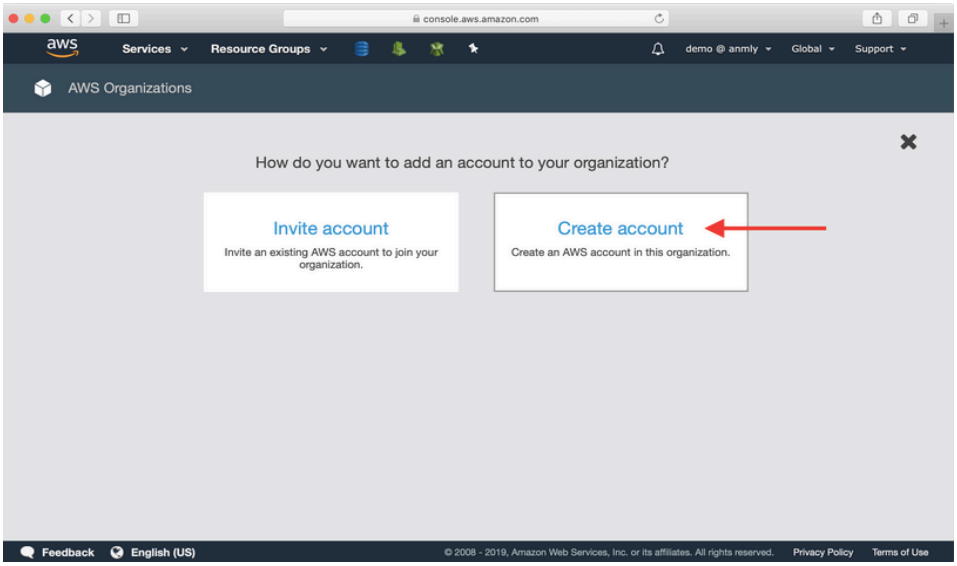
Screen 210

You will see screen below



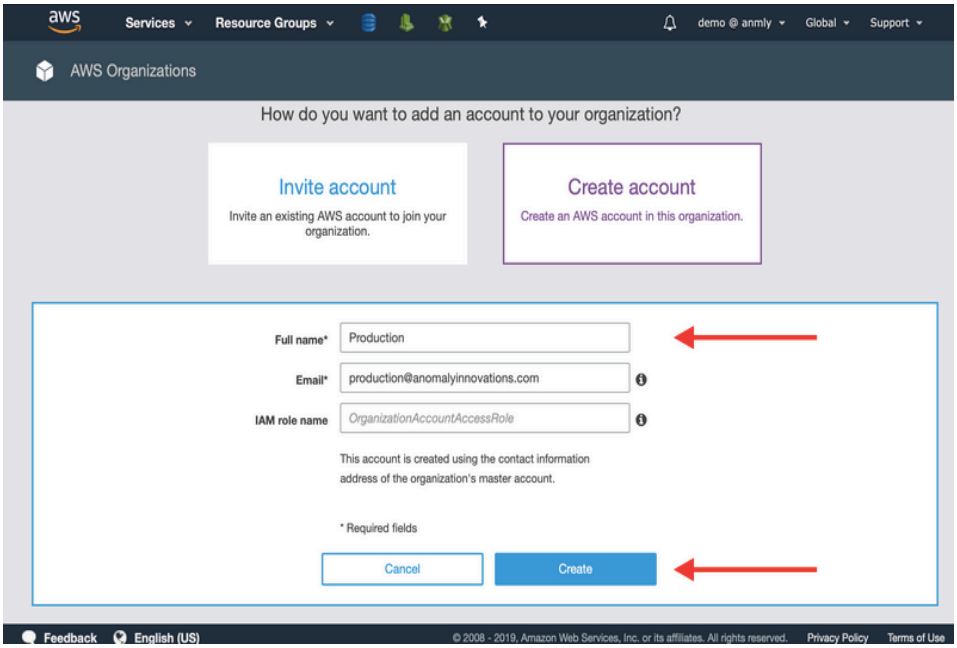
Screen 211

On screen below select Create account



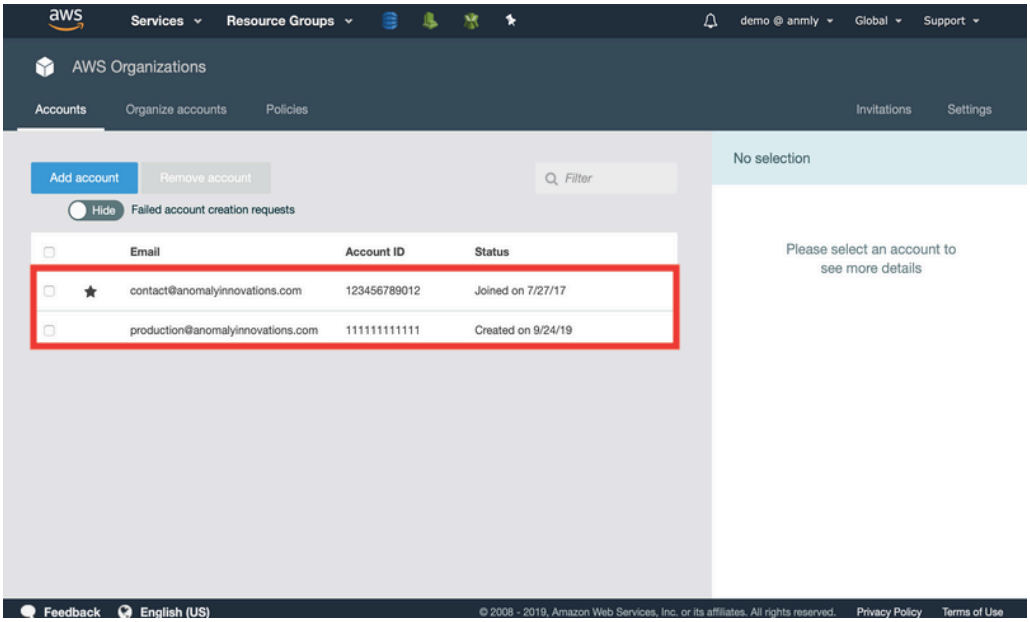
Screen 212

- ***Full name****: Enter Prod, Production or what you would like to call this account. It is used for display purposes only.*
- ***Email****: Each account requires a unique email address. Emails with the '+' sign are allowed.*
- ***IAM role name****: Leave this empty. When creating a new account, AWS Organizations automatically creates an IAM role in the new account that allows the master account to be able to assume into it. Actually, it's the only way to access a newly created account. By default, the IAM role is named* ***OrganizationAccountAccessRole****, you can give it another name.*



Screen 213

Now, you have 2 AWS accounts in your organization.



Screen 214

AWS Also can be used for

- Centrally manage policies on multiple AWS accounts
- Consolidated billing & single payment method
- Create new accounts, grouped accounts into organizations unit, allocate resources & apply organization wide policy
- Suitable for managing many accounts within big organization

Best practices on AWS Organizations

- ***Create Account per department*** – you should crate accounts per department based on Regulatory Restriction using SCP for better resources isolation, and to have separate per-account service limits
- ***Restrict account privileges*** using Service Control Policies (SCP)

19.4.3 AWS Control Tower

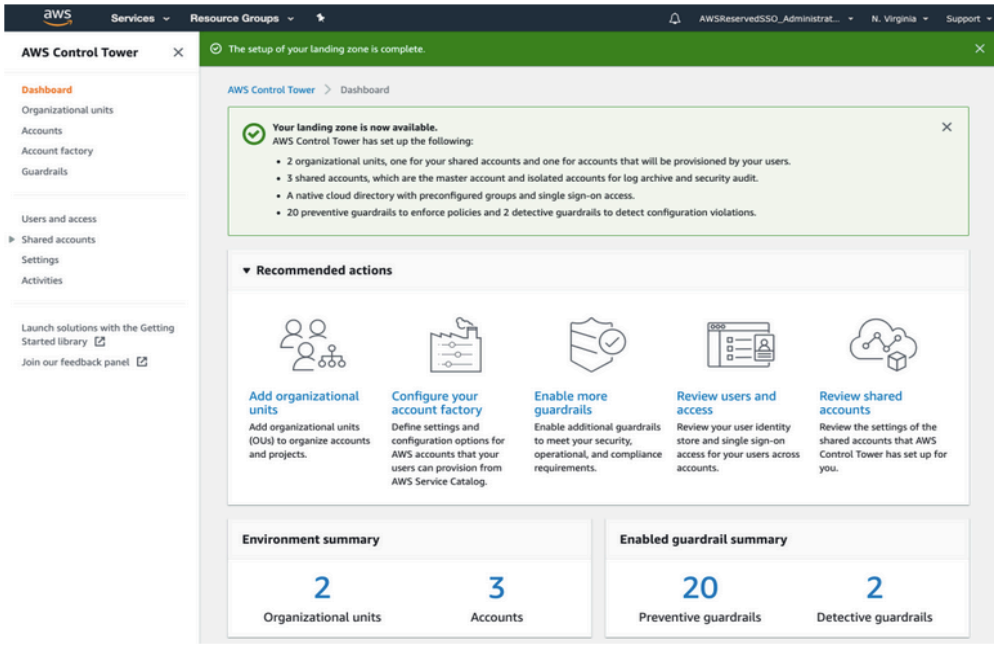
AWS Control Tower provides the easiest way to setup and govern a secured compliance multi-account in AWS Environments, called a landing zone.

There are 3 steps to follow:

- Setup – automated setup
- Apply Guardrails – apply security & compliant policy, detect mon compliance accounts/resources
- Get Visibility – Monitor compliance with various dashboard

AWS Control Tower creates your landing zone using AWS Organizations, bringing ongoing account management and governance as well as implementation best practices based on AWS's experience working with thousands of customers as they move to the cloud.

With AWS Control Tower, builders can provision new AWS accounts in a few clicks, while you have peace of mind knowing that your accounts conform to company-wide policies. AWS customers can implement AWS Control Tower, extend governance into new or existing accounts, and gain visibility into their compliance status quickly. If you are building a new AWS environment, starting out on your journey to AWS or starting a new cloud initiative, Control Tower will help you get started quickly with governance and best practices built in.

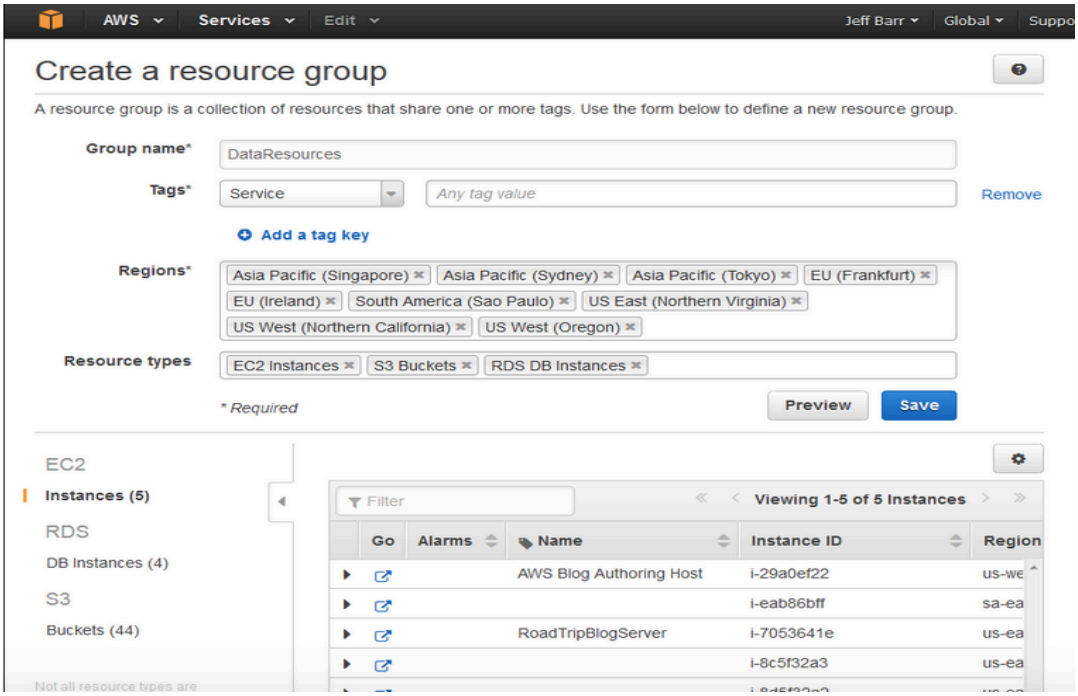


Screen 215

AWS Control Tower provides a pre-defined set of blueprints and guardrails to help customers implement a landing zone for new AWS accounts.

19.4.4 AWS Resource Group

AWS Resource Group is a collection of AWS Resources in the same AWS Region that match tag-based criteria provided in a search query. It is a collection of resources that are share one or more tags. It is used to organize your AWS Resources, manage, and automate tasks on large numbers of resources at a time.

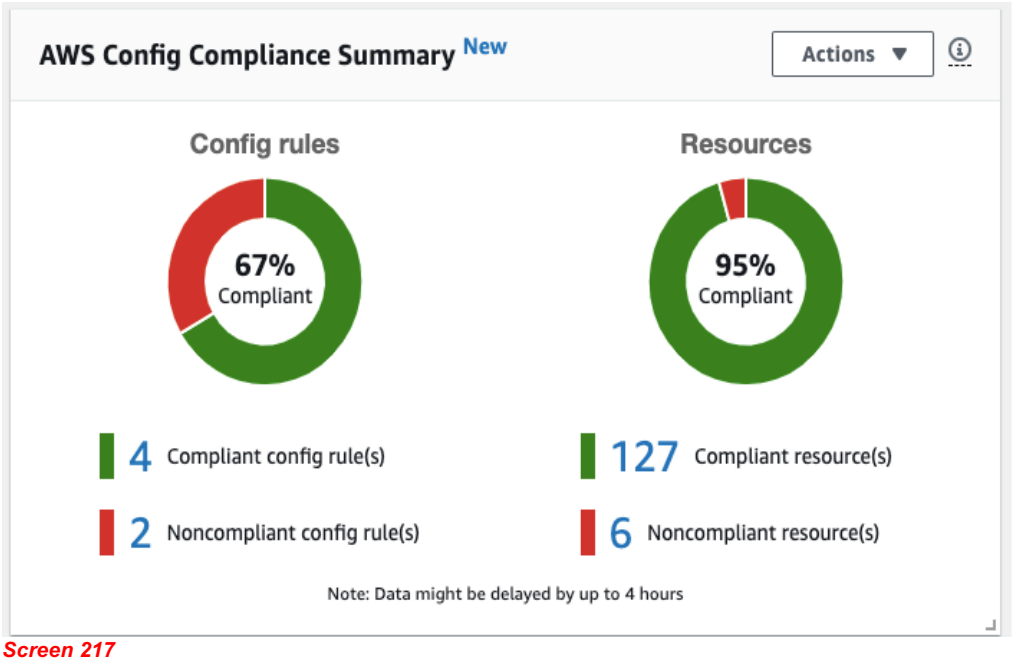


Screen 216

19.5 Configuration Changes

19.5.1 AWS Config

AWS Config is used to track history of *configuration changes* for all resources and provides a details view of the configuration of AWS Resources in your Account. It also helps with Auditing & Compliance of your AWS Resources. It is used for *Configuration change* for security & compliance reasons.



Screen 217

19.6 AWS CloudFront vs. AWS Cloud Formation

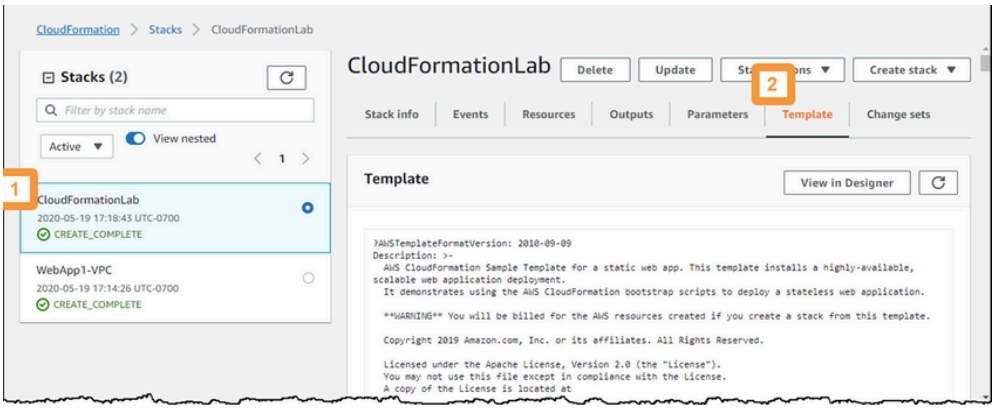
It's completely two different things, it's apple and orange. Please don't get mixed up between these two resources!

19.6.1 AWS Cloud Formation

AWS Cloud Formation allows you to use programming language or a simple text file to model and provision in an automated and secure manner. You can write a template which contain resources such as Amazon S3, AWS Lambda, Amazon DynamoDB, etc and upload into Cloud Formation.

It is great for a regional expansion – great for code review infrastructure changes and it helps you define your infrastructure as a code.

You can use Cloud Formation template as displayed on screen 168 below and write your code here and save them and can be used for future expansion.



Screen 218

19.6.2 AWS CloudFront

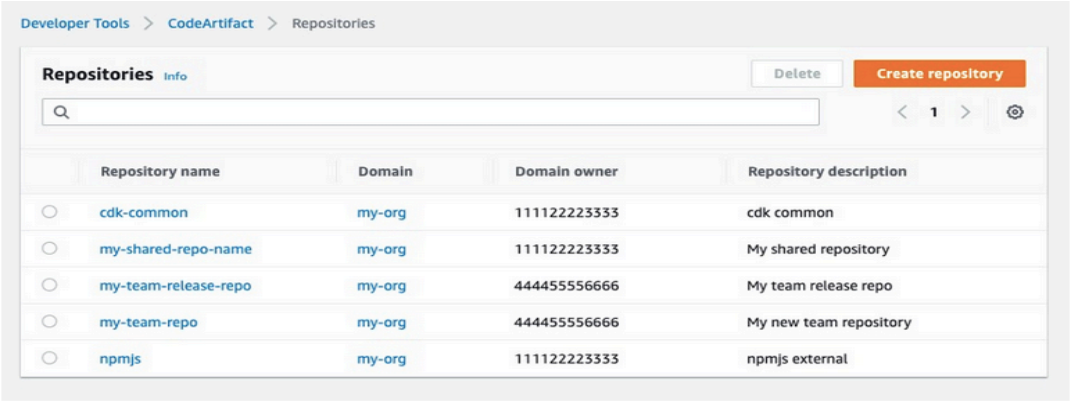
AWS CloudFront is a fast Content Delivery Network (CDN) service, and it securely delivers data, videos, applications and APIs to customer globally with low-latency, high transfer speeds.

19.7 Repository

19.7.1 AWS CodeArtifact

AWS CodeArtifact is a fully managed *artifact repository service* that makes it easy for organizations of any size to securely store, publish, and share software packages used in their software development process.

AWS CodeArtifact can be configured to automatically fetch software packages and dependencies from public artifact repositories, so developers have access to the latest versions. CodeArtifact works with commonly used package managers and build tools like Maven, Gradle, npm, yarn, twine, pip, and NuGet making it easy to integrate into existing development workflows.

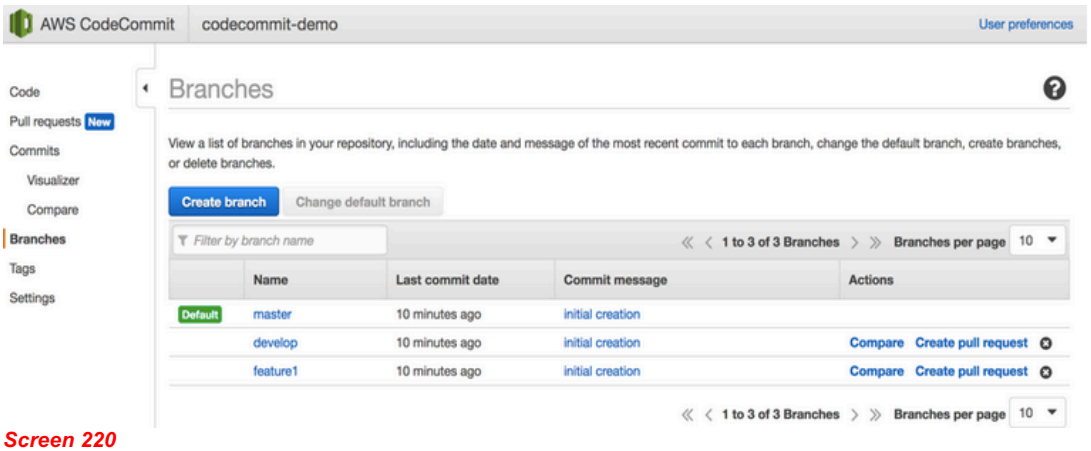


Screen 219

19.7.2 AWS CodeCommit

AWS CodeCommit is a fully managed source control service that hosts secure Git-based *repositories*. It makes it easy for teams to collaborate on code in a secure and highly scalable ecosystem.

AWS CodeCommit eliminates the need to operate your own source control system or worry about scaling its infrastructure. You can use CodeCommit to securely store anything from source code to binaries, and it works seamlessly with your existing Git tools.
AWS CodeCommit offers feature for version control and commits code privately.

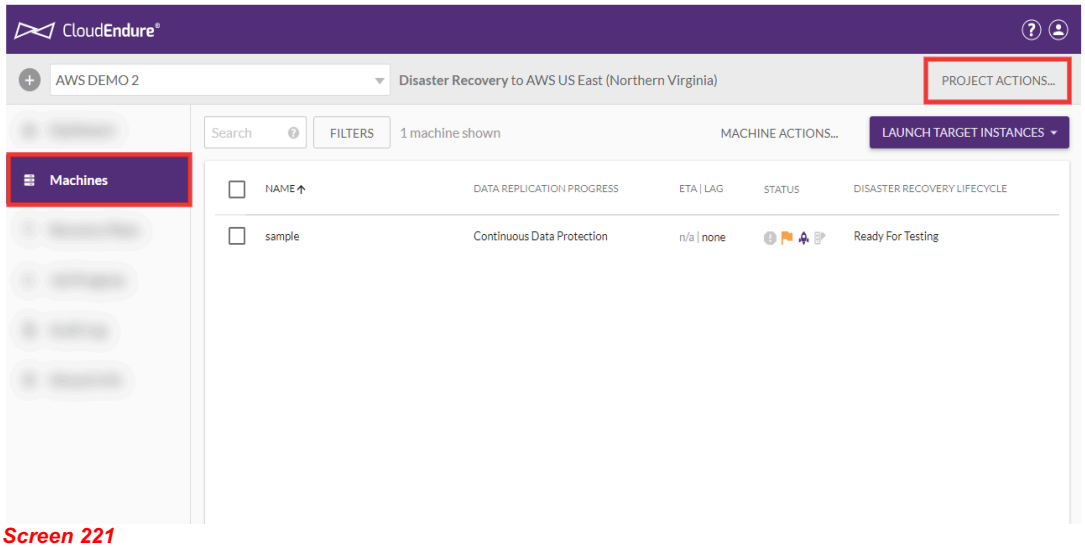


Screen 220

19.8 CloudEndure Disaster Recovery

CloudEndure Disaster Recovery continuously replicates your machines (including operating system, system state configuration, databases, applications, and files) into a low-cost staging area in your target AWS account and preferred Region. In the case of a disaster, you can instruct CloudEndure Disaster Recovery to automatically launch thousands of your machines in their fully provisioned state in minutes.

By replicating your machines into a low-cost staging area while still being able to launch fully provisioned machines within minutes, CloudEndure Disaster Recovery can significantly reduce the cost of your disaster recovery infrastructure.



Screen 221

Please don't get mixed up between CloudEndure Disaster Recovery vs. CloudCover Disaster Recovery. There NO such thing as ***CloudCover Disaster Recovery!***

19.9 Streaming Options

19.9.1 Amazon AppStream 2.0 (Desktop Service – Individual Application)

Amazon AppStream 2.0 is a fully managed non-persistent application and desktop streaming service. You centrally manage your desktop applications on AppStream 2.0 and securely deliver them to any computer. You can easily scale to any number of users across the globe without acquiring, provisioning, and operating hardware or infrastructure.

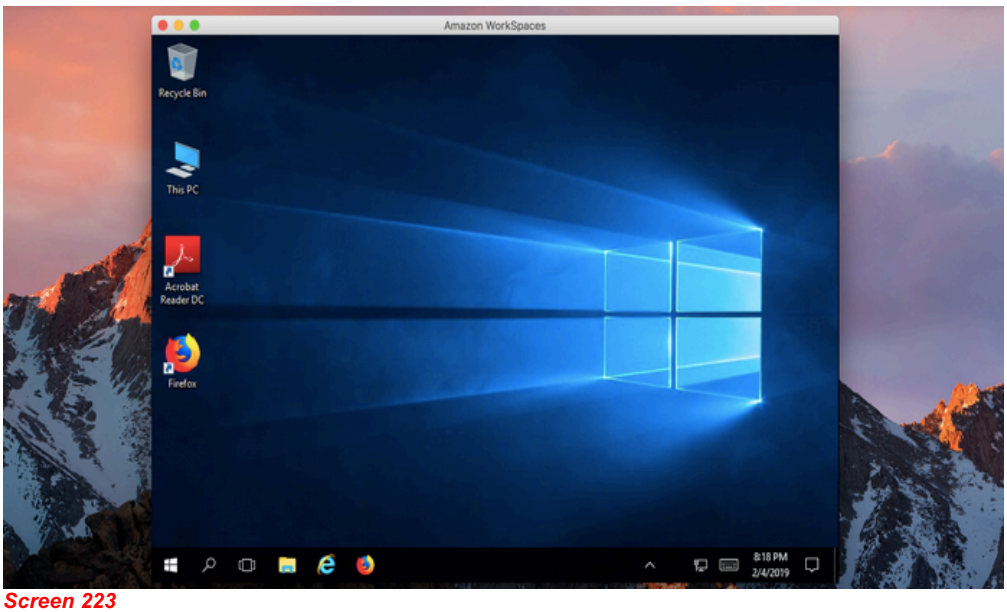
Amazon AppStream 2.0 is a fully managed non-persistent desktop and application service for remotely accessing your work.

Screen 222

19.9.2 Amazon WorkSpaces (Desktop Streaming Service/Virtualization – DaaS Solution)

Amazon WorkSpaces is a fully managed desktop virtualization service for Windows and Linux that enables you to access resources from any supported device.

Amazon WorkSpaces is a managed, secure ***Desktop-as-a-Service (DaaS)*** solution. You can use Amazon WorkSpaces to provision either Windows or Linux desktops in just a few minutes and quickly scale to provide thousands of desktops to workers across the globe.



Screen 223

19.9.3 AppStream 2.0 vs. Workspaces

While the two AWS services are somewhat similar, it's important to remember that Amazon AppStream 2.0 is focused on hosting individual applications on AWS, while Amazon WorkSpaces creates virtual desktops that can be used to create entire working environments for you and your team

Considered these scenarios below:

- AWS AppStream 2.0 allows you to access one of your applications virtually from anywhere such as Power Point, MS Mail (Email), or Spreadsheet, but you don't have access to your desktop
- AWS Workspaces allows you to have access to your desktop virtually by using Desktop as a Service (DaaS) concept

19.9.4 Amazon Kinesis

Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so you can get timely insights and react quickly to new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of your application.

With Amazon Kinesis, you can ingest real-time data such as video, audio, application logs, website clickstreams, and IoT telemetry data for machine learning, analytics, and other applications. Amazon Kinesis enables you to process and analyze data as it arrives and respond instantly instead of having to wait until all your data is collected before the processing can begin.

19.10 3D and Virtual Reality – Amazon Sumerian

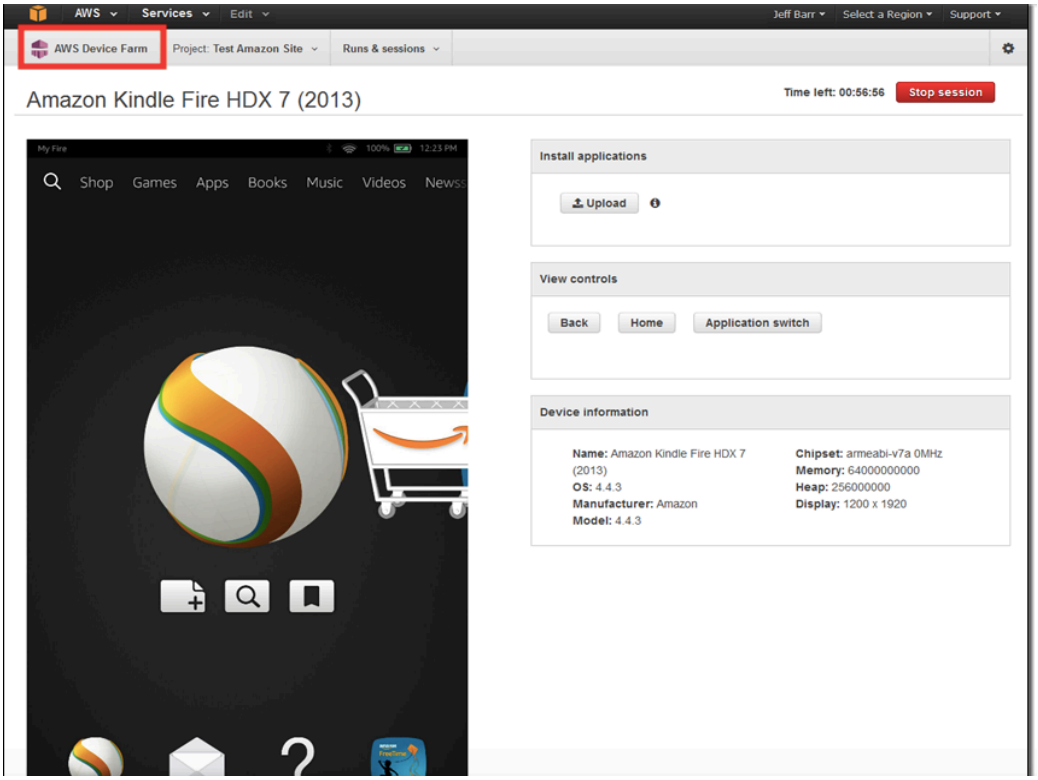
Amazon Sumerian is *a managed service that lets you create and run 3D, Augmented Reality (AR) and Virtual Reality (VR) applications*. You can build immersive and interactive scenes that run on AR and VR, mobile devices, and your web browser.

Screen 224

19.11 Mobility

19.11.1 AWS Device Farm

It's an application testing lets you to improve the quality of your web and *mobile applications* by testing them across an extensive range of desktop browsers and real *mobile devices*.



Screen 225

It is designed for developers, QA, and customer support representatives who are building, testing and supporting *mobile* applications to increase the quality of their applications.

19.11.2 AWS Wavelength

It is storage services with 5G Networks providing *Mobile Edge Computing Infrastructure* for developing, deploying, and scaling ultra-low latency applications.

19.12 Media Conversion – Amazon Elastic Transcoder

Amazon Elastic Transcoder is used to convert media files that you have stored in Amazon S3 into media files in the format required by customer playback devices.

It can convert large, high quality digital media files into formats that users can playback on mobile devices such as tablet.

19.13 IoT Device Connectivity – AWS IoT Core

AWS IoT Core connects IoT devices to the AWS Cloud without the need to provision or manage server. It can support billions of devices

19.14 AWS OpsWorks vs. AWS OpsHub

Although both names are very similar, but they have nothing to do with one each other.

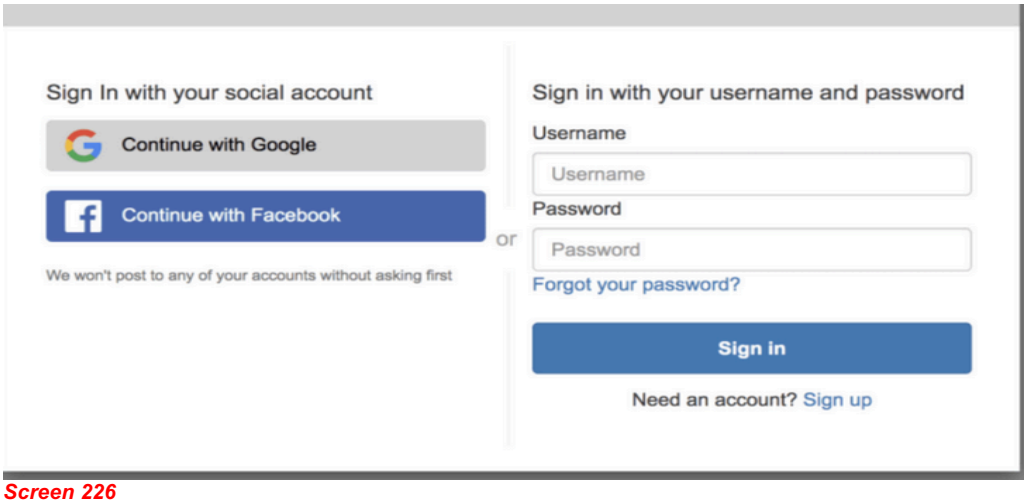
AWS OpsWorks is an infrastructure deployment for cloud admin. It is also Configuration Management service that provides managed instances for Chef and Puppet. Please refer to section 13.6 above.

On the other hands, AWS OpsHub is a graphical user interface you can use to manage your AWS Snowball devices, enabling you to rapidly deploy edge computing workloads and simplify data migration to the cloud. Please refer to section 11.2.5 above.

20 AWS Temporary Limited-Privilege Credentials

20.1 AWS Cognito

Amazon Cognito lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0 and OpenID Connect.



Screen 226

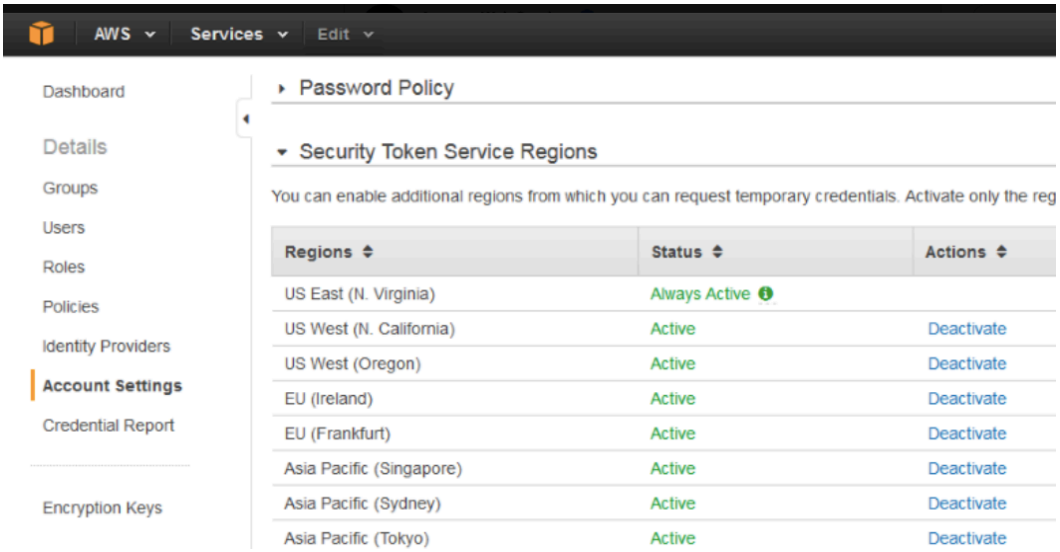
Screen 227

AWS Cognito makes it easy to add user signup and login to your web and mobile apps by abstracting out all of the functionality necessary including authentication and storage of credentials.

By leveraging AWS Cognito, we can take advantage of built-in security features such as multi factor authentication and password encryption/storage.

20.2 AWS Security Token Service (STS)

AWS provides AWS Security Token Service (AWS STS) as a web service that enables you to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for users you authenticate (federated users).



Screen 228

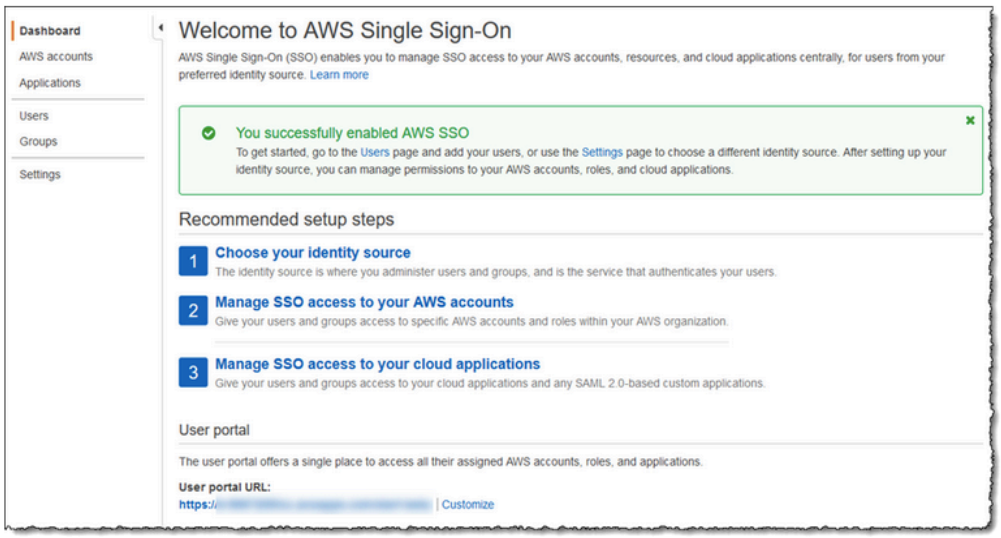
You can use the AWS Security Token Service (AWS STS) to create and provide trusted users with temporary security credentials that can control access to your AWS resources. Temporary security credentials work almost identically to the long-term access key credentials that your IAM users can use, with the following differences:

- Temporary security credentials are *short-term*, as the name implies. They can be configured to last for anywhere from a few minutes to several hours. After the credentials expire, AWS no longer recognizes them or allows any kind of access from API requests made with them.
- Temporary security credentials are not stored with the user but are generated dynamically and provided to the user when requested. When (or even before) the temporary security credentials expire, the user can request new credentials, as long as the user requesting them still has permissions to do so.

20.3 AWS Single Sign On (SSO)

AWS Single Sign-On (AWS SSO) is where you create, or connect, your workforce identities in AWS once and manage access centrally across your AWS organization.

You can choose to manage access just to your AWS accounts or cloud applications. You can create user identities directly in AWS SSO.



Screen 229

With AWS SSO, you get a unified administration experience to define, customize, and assign fine-grained access. Your workforce users get a user portal to access all of their assigned AWS accounts or cloud applications. AWS SSO can be flexibly configured to run alongside or replace AWS account access management via AWS IAM.

21 AWS Global vs. Regional Services

21.1 AWS Regional Services

Most of the AWS Services are Regional such as; AWS Lambda, Amazon S3, EFS, EBS, AWS Shield, Amazon Rekognition, AWS Aurora, AWS Athena, Amazon RDS, and everything else.

Please refer to the complete list below.

https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/

21.2 AWS Global Services

However, the following AWS Services are Global

21.2.1 Global – Identity and Access Management (IAM)

AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. It is a GLOBAL service instead of REGIONAL service.

21.2.2 Global – AWS CloudFront (CDN)

Amazon CloudFront is a content delivery network (CDN) service built for high performance, security, and developer convenience. It is a GLOBAL service instead of REGIONAL service.

21.2.3 Global – AWS Web Application Firewall (WAF)

AWS WAF is a web application firewall that helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. It is a GLOBAL service instead of REGIONAL service.

21.2.4 Global – Amazon Route 53

Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is a GLOBAL service instead of REGIONAL service.

21.2.5 Global – AWS Organizations

AWS Organizations helps you centrally manage and govern your environment as you grow and scale your AWS resources. It is a GLOBAL service instead of REGIONAL service.

21.2.6 Global – AWS Global Accelerator

AWS Global Accelerator is a networking service that improves the performance of your users' traffic by up to 60%. It is a GLOBAL service instead of REGIONAL service.

21.2.7 Global – Amazon Workspaces

An Amazon WorkSpace is a cloud-based virtual desktop that can act as a replacement for a traditional desktop. It is a GLOBAL service instead of REGIONAL service.

21.2.8 Global – Amazon WorkDocs

Amazon WorkDocs is an Amazon Web Services online collaboration tool that allows a business to store, share and update files from different devices. It is a GLOBAL service instead of REGIONAL service.

21.2.9 Global – Amazon WorkMail

Amazon WorkMail is a secure, managed business email and calendaring service with support for existing desktop and mobile email clients. You can create an Amazon WorkMail organization and assign to it one or more email domains that you own. It is a GLOBAL service instead of REGIONAL service.

21.2.10 Global – Amazon WorkLink

Amazon WorkLink is **a fully managed service** that lets you provide your employees with secure, easy access to your internal corporate websites and web apps using their mobile phones. It is a GLOBAL service instead of REGIONAL service.

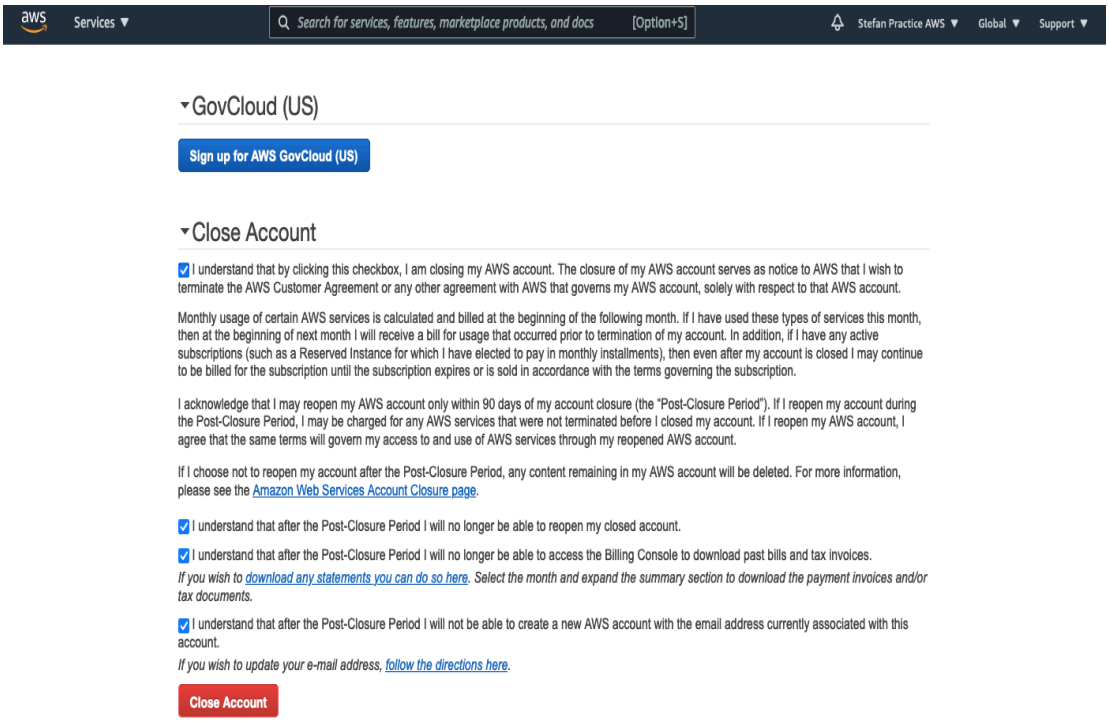
21.2.11 Global – Amazon Chime

Amazon Chime is a communications service that lets you meet, chat, and place business calls inside and outside your organization, all using a single application. It is a GLOBAL service instead of REGIONAL service.

22 AWS Account Termination & Support Group

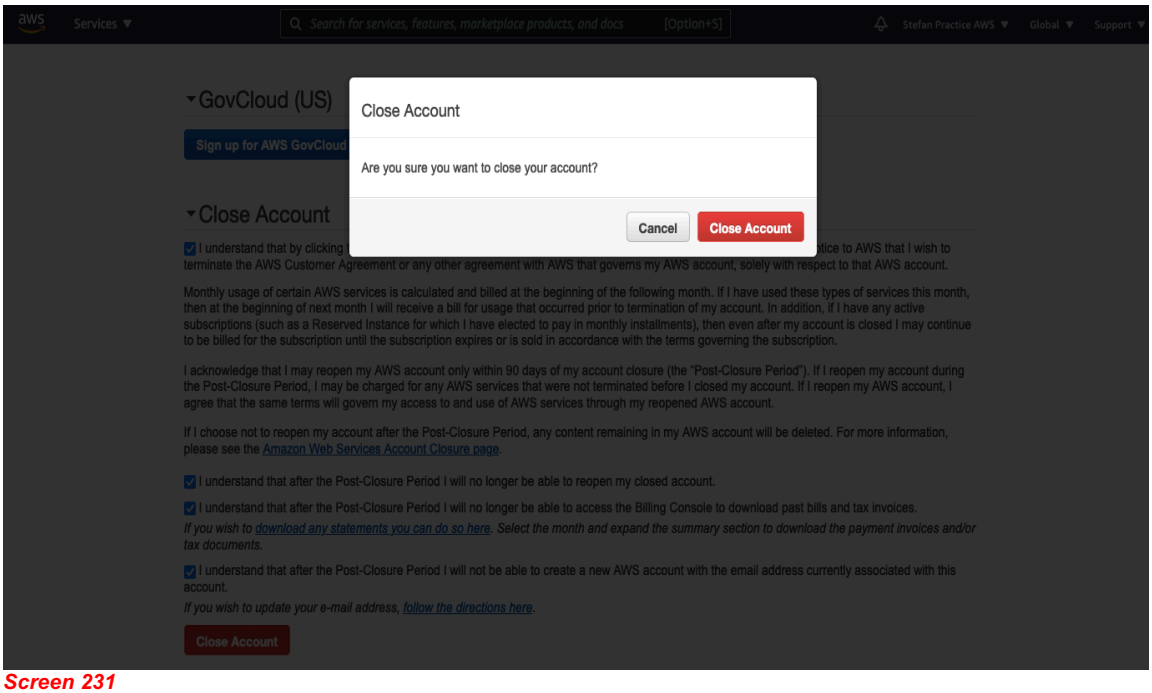
22.1 Closing AWS Account

You can close your AWS Account at any time. From AWS Management Console type close account and you will see screen below



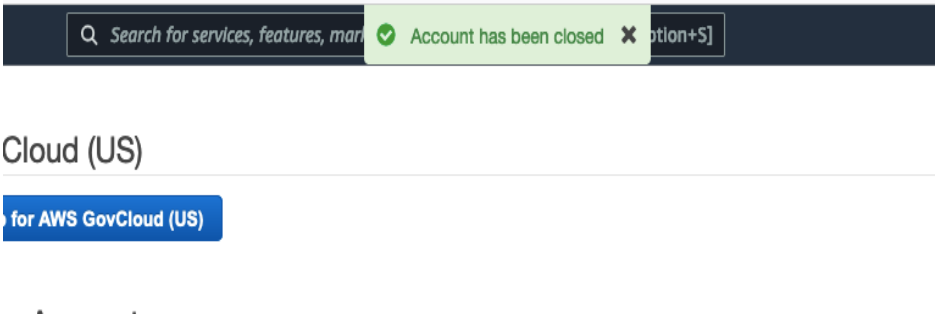
Screen 230

Make sure you click all the check boxes and click ***Close Account*** and you will see screen below



Screen 231

Click ***Close Account*** from screen above and you will see confirmation screen below.



Screen 232

22.2 Why Am I still being billed after closing my account?

Closing your account might not automatically terminate all your active resources. You might continue to incur charges for some of your active resources even after you close your account. You're charged for any usage fees incurred before closure.

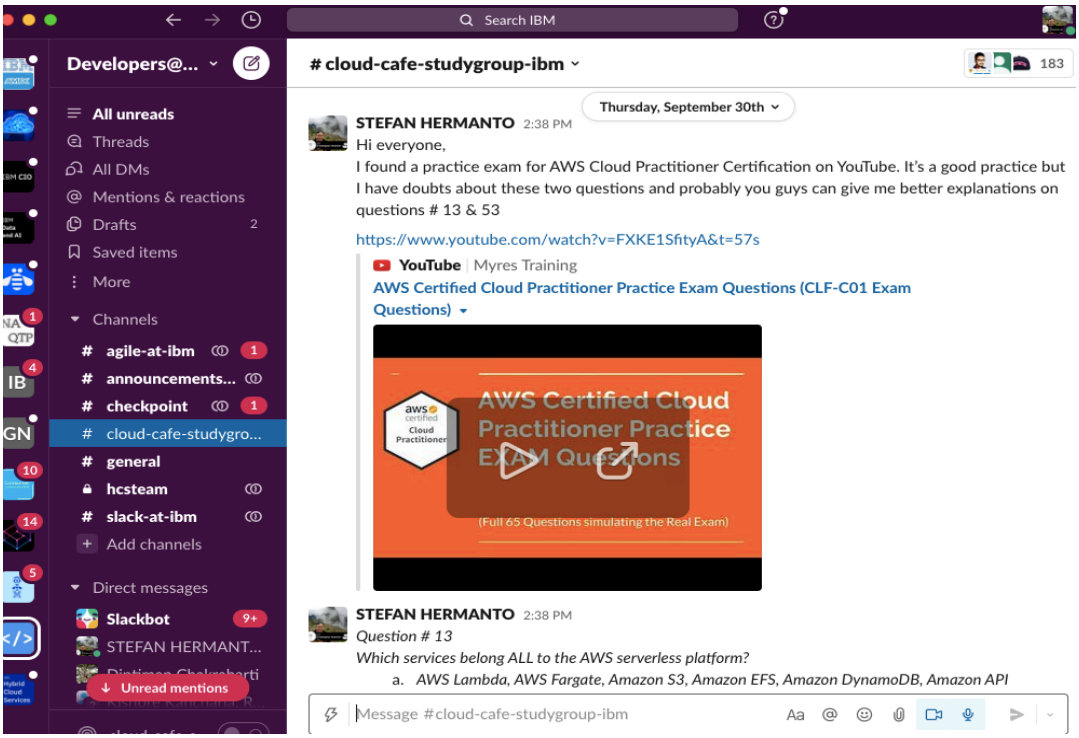
To avoid incurring unexpected charges, it's a best practice to routinely check if you have active resources that you no longer need. Then, terminate these unneeded resources.

22.3 Study/Support Group

Should you have any questions about Cloud in general or AWS Cloud in particular, you can join this Slack Channel:

#cloud-cafe-studygroup-ibm

https://developers-at-ibm.slack.com/archives/CSBNB6GG6



Screen 234

It’s a very good Slack community and most of the members are IBMers that are working on the cloud projects as cloud architects, cloud infrastructure engineers and cloud partitioners. They are very helpful with all the cloud questions that you have and it’s a very good community that are willing to help you especially if you are just started your journey to the cloud.

****** End of Document ******