NewNet Communication Technologies

FOUNDATIONS FOR NETWORK INNOVATION

AV Launch Guide (Standard)

TRADEMARK

COPYRIGHT INFORMATION

GOVERNMENT USE

PERFORMANCE SPECIFICATIONS

NewNet Communication Technologies, LLC, reserves all the rights to change the equipment performance specifications stated herein at any time without notice. For OEM components, NewNet relies on the specifications supplied by the OEM vendors.

SUCCESSOR IN INTEREST

NewNet Communication Technologies is the successor in interest to:

- EBS, Inc.
- NewNet
- Centigram Communications Corporation
- ADC ESD, Inc.
- ADC Enhanced Services Division
- SS8

Any rights or title to the marks or copyrights of these entities, unless otherwise disclosed, are the property of NewNet.

NewNet Communication Technologies, LLC

720 East Butterfield Road. Suite 250

Lombard, IL 60148
+1 224-795-5200

www.newnet.com

NewNet Communication Technologies
FOUNDATIONS FOR NETWORK INNOVATION

AccessView Launch Guide

Contents:

1 About Access View 4
2 Document Structure 5
3 Prerequisites 6
3.1 Skills Required 6
3.2 Accessing STC 6
3.3 Accessing AV Instance 6
3.4 Other requirements 6
3.5 Pre-Launch 6
3.5.1 Admin user key-pair generation 6
3.5.2 Creation of VPC and Subnets 7
3.6 Post-Launch 11
3.6.1 Assigning IAM Role to DB 12
4 Access View Cloud Edition Stack Creation 14
4.1 AV CE Cloud Launch 16
4.2 AV CE Stack Properties 21
5 Launching the AV CE Instance 23
5.1 AccessView Application installation 23
5.2 AccessView configuration from pGUI 28
5.3 Verifying the AccessView functionality 29
6 Application Overview 30
6.1 Application 30
6.2 Application Redundancy 30
6.3 Data Backup and Recovery 30
7 Troubleshooting 31
8 Update Procedure 32
9 Customer Support 33
10 Best Practices 34
10.1 Configuring AWS CloudTrail 34
10.2 Key Rotation 34
10.3 IAM Best Practices 34

1 About Access View

NewNet's AccessView Cloud Edition (AV CE) captures accounting and usage statistics from NewNet's STC payment transaction routing and transport application for report generation, billing, and search analytics. AV CE offers transaction reporting and provides aggregated data for billing, statistics and analytics while providing users, service providers and operators with insight into customer usage patterns and executive dashboards on the overall payment traffic and volume. Per transaction detail delivers granularity to track performance statistics and support offline analysis for applications such as fraud detection.

AccessView always works in conjunction with NewNet's STC gateway.

2 Document Structure

The Launch Guide document is structured in the following manner.

1. The Prerequisite section states the procedures required for successful access of the AV CE instances. This section contains a Pre-Launch which is a requirement to launch the instances and Post-Launch which is required after launching the instances for accessing and configuration of the instances.
2. The Access View Cloud Edition Stack Creation section states the creation of the AV CE Instance.
3. Launching AVCE Instance section briefs about how to launch the Instances.
4. Installation Section briefs the AV application installation in AWS Instances.
5. Configuration Section briefs the configurations required for the AWS Instances.
6. Software Update section mentions if there are newer versions of the software if available.

The document contains screen shots from AWS Management Console (AWSMC) at various stages of launch. Due to size constraints the images details may not be clear. The reader is requested to expand the images to get better impression on the image contents.

3 Prerequisites

3.1 Skills Required

The user should possess a prior basic knowledge of AWS, Windows, Oracle DB basics to proceed.

3.2 Accessing STC

Refer to the STC Launch guide for details.

https://newnet.com/business-units/secure-transactions/launch-guide-standard-hourly

3.3 Accessing AV Instance

Refer the links below for accessing the AV Instances and usage/conversion of the keys required for using RDS.

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/connecting_to_windows_instance.html

3.4 *Other requirements*

The AWS Default service limits is good for STC-AV deployment.
The cloud formation template during the AWS stack creation takes care of all the required elements for deployment. For instance, the instance size, the instance type, the s3 bucket, the RDS database.

3.5 Pre-Launch

User should have an AWS account prior to continuing with the deployment. AV provides Administrator as user which will be used for the required operations.

3.5.1 Admin user key-pair generation

AV instance is preconfigured with **Administrator** user. AWS does not allow password authentication, so we use RSA public/RSA private key pair instead of password. Key pair for Administrator must be generated.

- Sign in to the EC2 Management Console, via https://aws.amazon.com/console/ using your credentials.
- After logging into the AWS account, in the left navigation pane, Under Network and Security, choose Key Pair.

  Click Services➔EC2➔Key Pairs (Under Network & Security)

1. Click “Create Key Pair”. In the Create Key Pair dialog box, provide a key pair name and Click “create”.

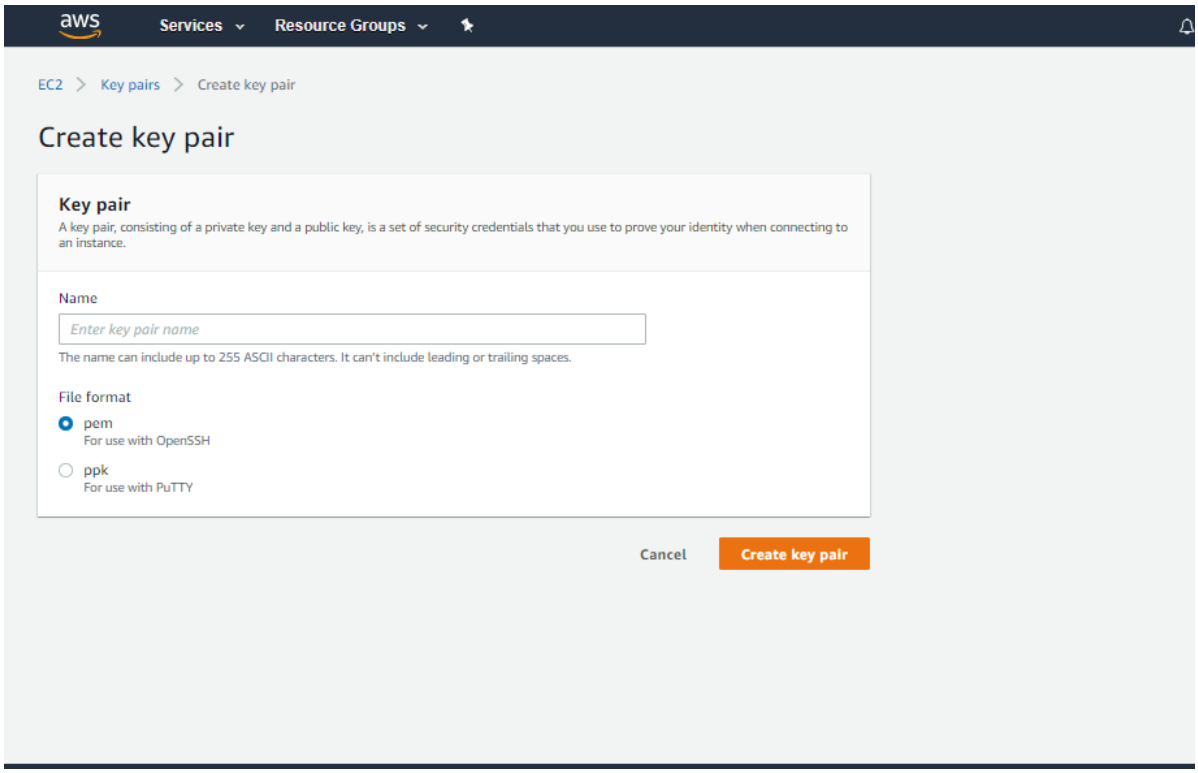


Figure 1 : Key Pair Creation

2. The key pair file, for example “keypair1.pem”, is auto downloaded by the browser to local machine.

3.5.2 Creation of VPC and Subnets

User can use the VPC and the subnet that was used for STC launches or create a new VPC and subnet as well. VPC Peering is required if new VPC are created.

Ensure to create only one Subnet per Availability Zone.

On AWS Management Console (AWSMC), choose the VPC from the available services

3.5.2.1 Creating VPC and Primary Subnet

Click “Launch VPC Wizard”. The section as in Fig.2 will be seen.

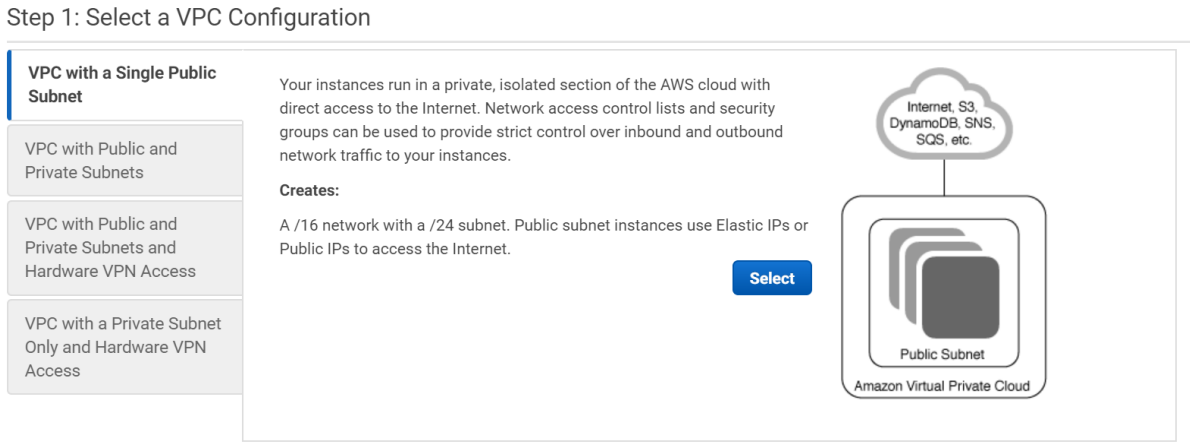


Figure 2: VPC Service Page

Choose VPC with a Single Public Subnet option.

The data to input is shown below for reference. CIDR block for the VPC and Subnet needs to be input. Choose the availability zone.

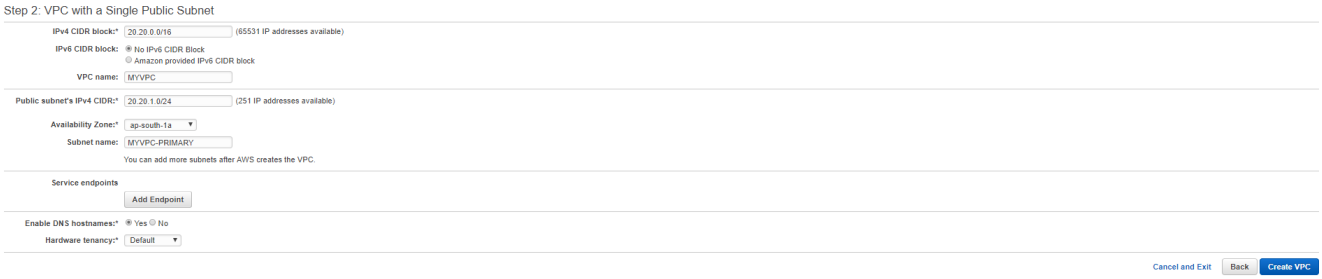


Figure 3 : VPC Creation

Once the VPC is created along with the Subnet, click on Subnet.

Click on the Route Table and note the IGW associated with the subnet. This is required if more subnets are created.

3.5.2.2 Other Subnet Creation

Create a new subnet for RDS.

Choose “Subnet” option from the VPC menu. Then click “Create subnet” option. The following screen will be seen. Choose the VPC that was created earlier. **The Availability Zone should be a different one from the one that was used in creating subnet with VPC Wizard**.

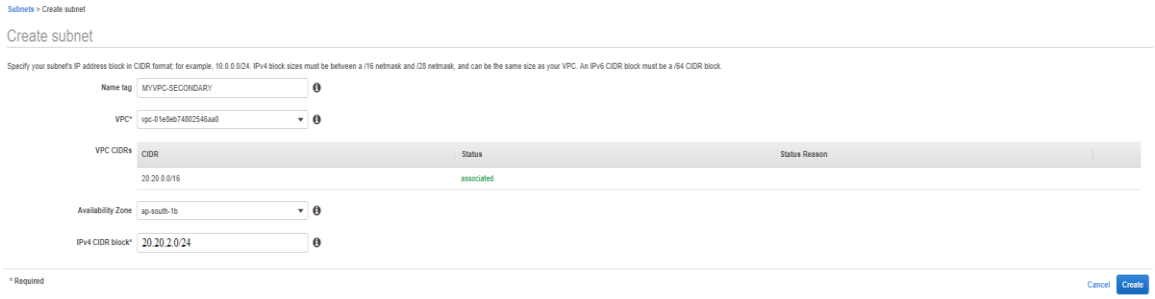


Figure 4 : Subnet Creation in a VPC

The VPC ID and Subnet IDs created should be noted. These shall be input later while launching the AV instances.

The created secondary subnet will be private and not associated with an Internet Gateway. Following is the procedure to associate the IGW.

Once the secondary Subnet/s are created, click on the created subnet, it lists the associated subnet properties.

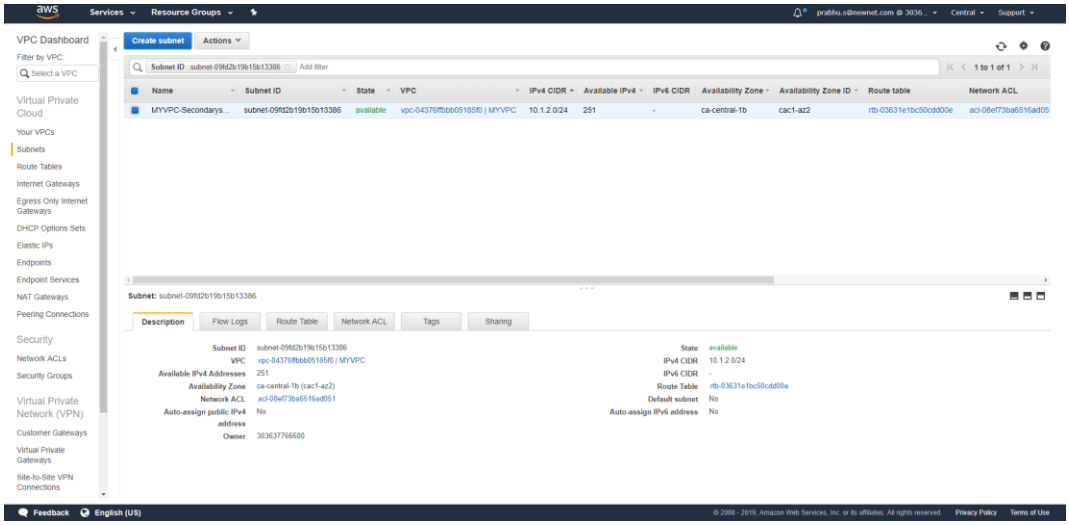


Figure 5 : Secondary Subnet

Click on “Route Table” tab. It navigates to the page below.

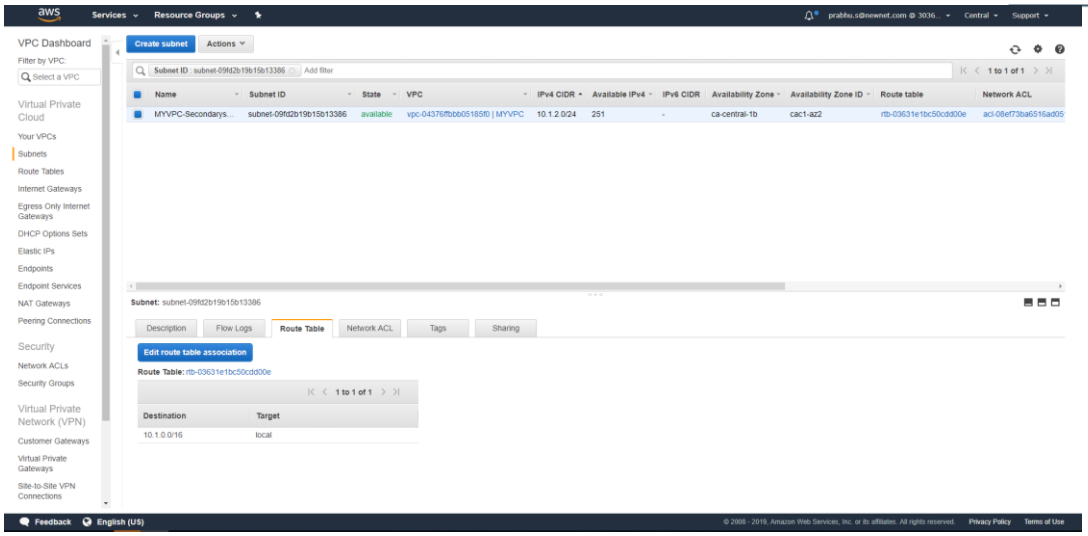


Figure 6 : Secondary Subnet's Route Table

The Route table displays the associated route table and the route entries. Click on the entry next to Route table which usually is prefixed "rtb-" . This navigates to the Route table.

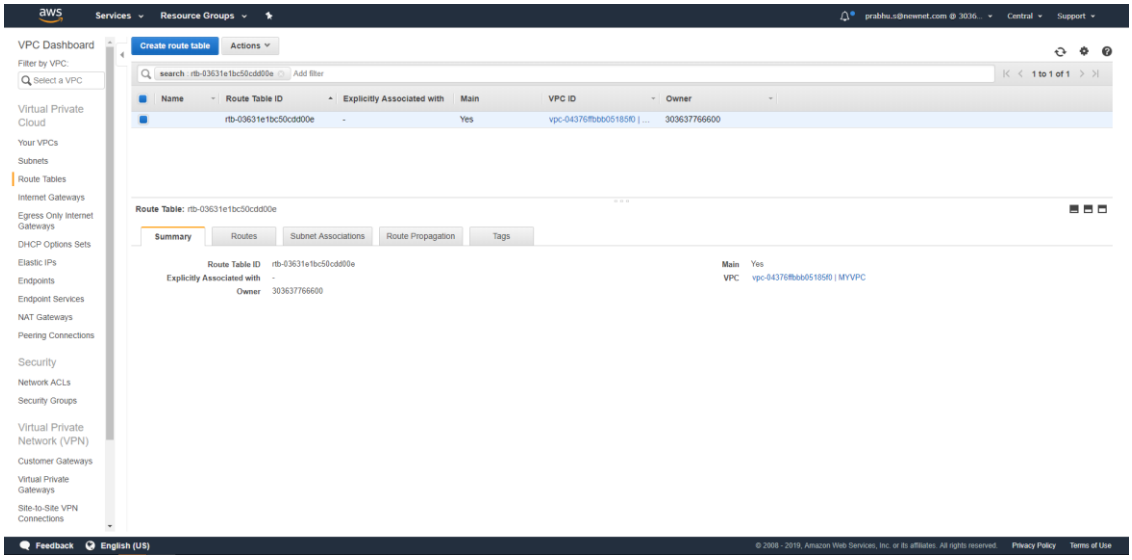


Figure 7: Associated Route Table

This page highlights the Routes. Click on the tab "Routes" and "Edit Routes"

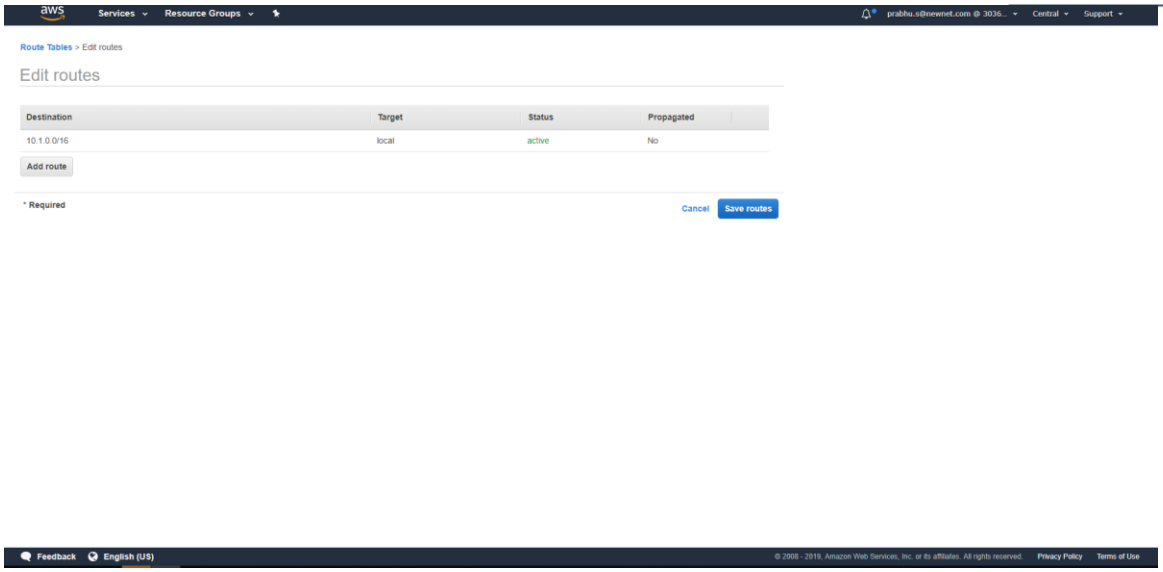


Figure 8 : Edit Routes

Now, click on the “Add Route” radio button

Add an entry with the inputs, 0.0.0.0/0 as Destination and <choose Internet Gateway from drop down menu>(This IGW is the one which gets associated to the VPC as noted in Step 3.3.3.1) as Target.
Click “save routes”.

This saves the route updates and all the subnets are associated with IGW.

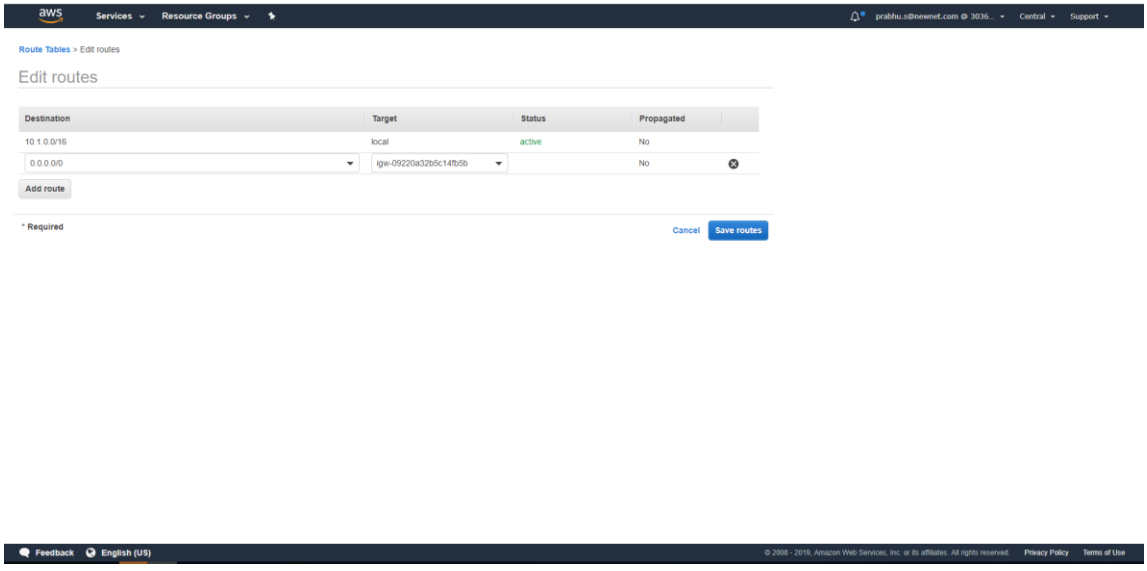


Figure 9 : Add Route

3.6 *Post-Launch*

This section of the document is required post the launch of the AV Instance. On successful completion of the AV Stack Creation,

3.6.1 Assigning IAM Role to DB

The Database must be associated with specific IAM role for transferring files between RDS and S3 bucket. Hence an S3_INTEGRATION IAM Policy is created. The IAM role assigned will only allow the transferring of files, Read and write to the files created in the S3 bucket which is created during the launch.

Assign iam-role created by AV launch template to database. Navigate to the RDS Console. (Services→RDS)

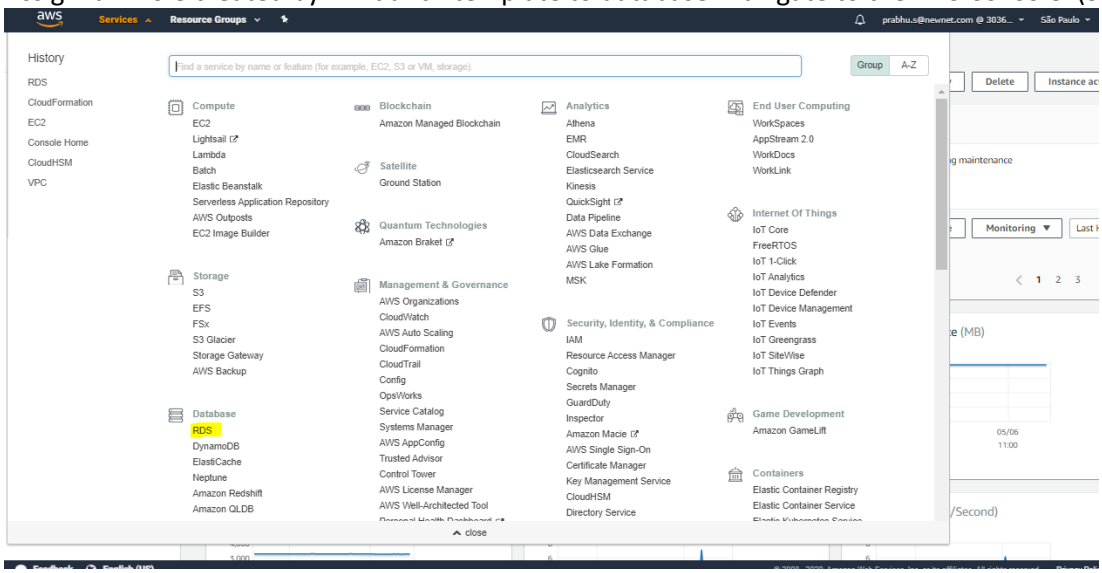


Figure 10 : RDS

Click on RDS. This navigates to the RDS dashboard where all the details are present. Click on DB Instances(highlighted)

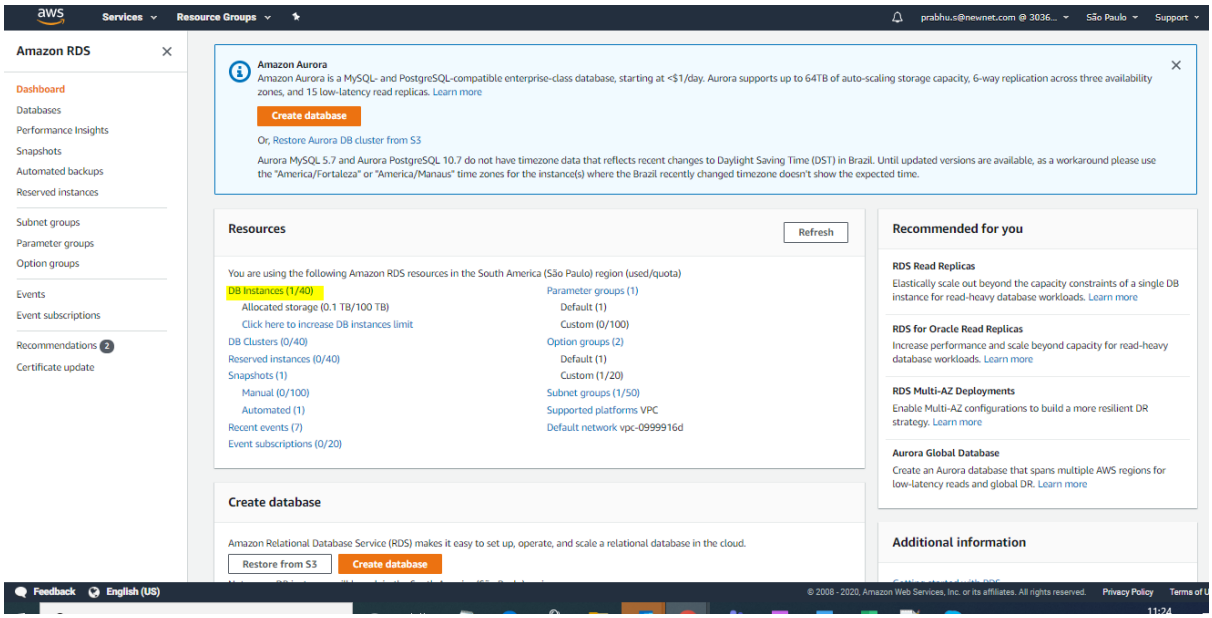
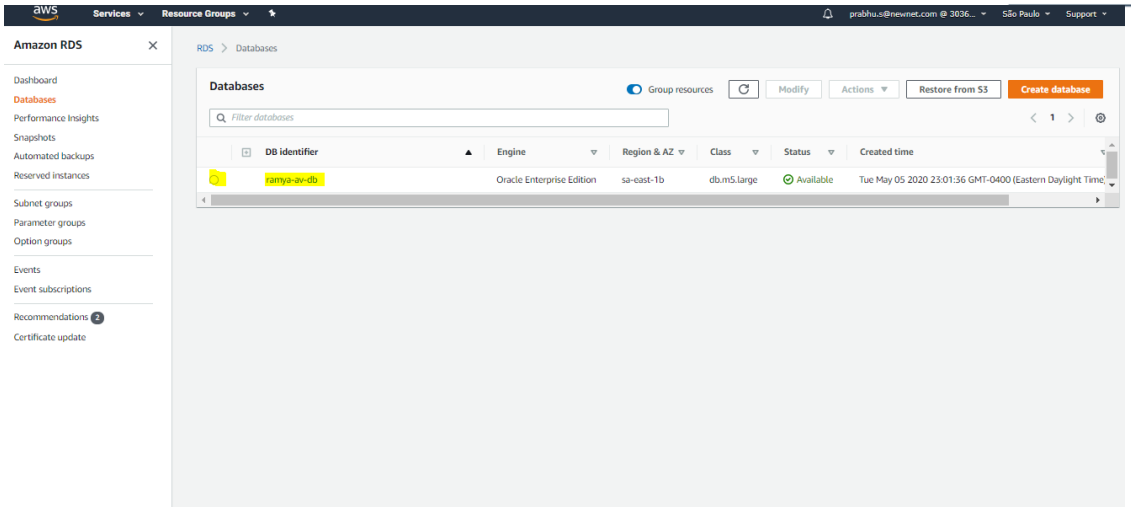


Figure 11: Database

This navigates to the created database page. Now click on the created database(highlighted)



This leads to the database created with all the relevant database properties. Scroll down in the sheet to the "Manage IAM roles".

Click on the dropdown in the "Add IAM role to this instance". Select role created by launch. (which is the one with stack-name prefix) and for the feature: Select S3_INTEGRATION.

Click on "Add rule". This takes about a minute or 2 to change itself to Active.

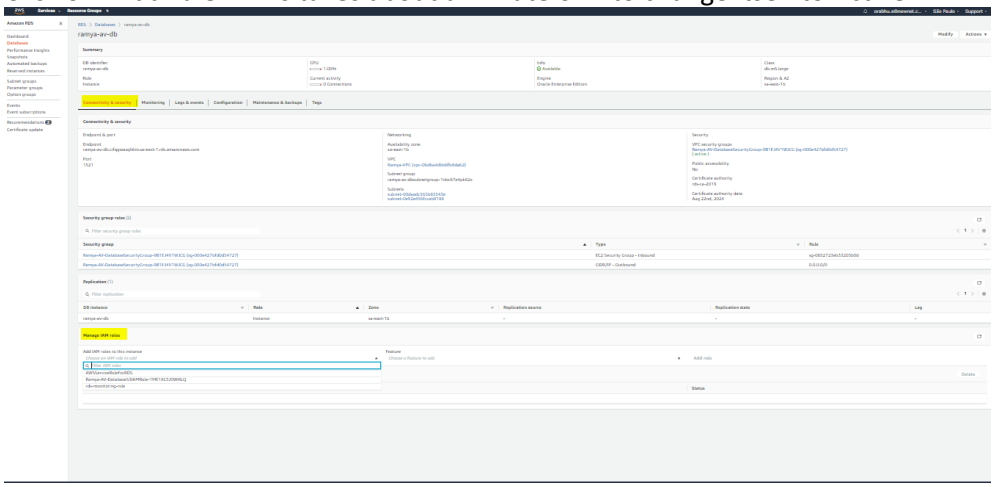
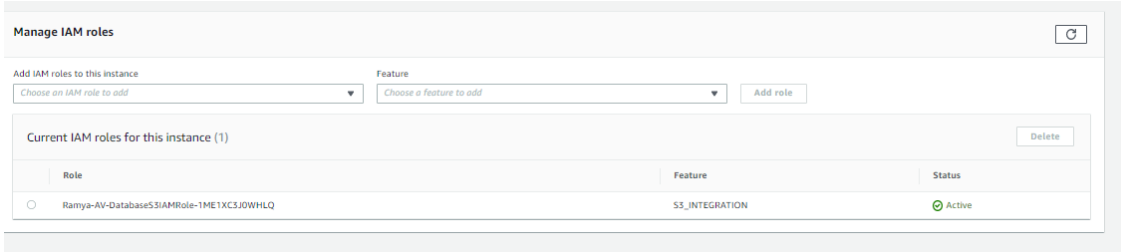


Figure 12: Add IAM Role

IAM role once it changes to active.



4 Access View Cloud Edition Stack Creation

AV CE is deployed with AWS RDS. The resources created post the launch is Windows instance on which the Access View software is deployed, Oracle RDS and a S3 bucket.

User shall be required to input the VPC ID, and Subnet IDs during the stack creation. The input for database subnets requires user to input subnet ids from 2 different AZ's for database subnet id. However, by **default**, the **Multi-AZ** feature is not enabled for the **RDS** instance.

The AV CE application is used in conjunction with the STC. The AV CE receives the CDR data from the STC. The EC2 instance and the RDS database will be of type m5.large. M5 instances are the latest generation of General-Purpose Instances powered by Intel Xeon® Platinum 8175M processors. The instance type of m5.large is validated to suffice the application performance requirement for AV CE to handle the STC instance's CDR transmission rate based on the transaction concurrent session capacity. The instance storage is EBS-Only. These are preconfigured for the AV CE Stack.

The user with the AWS account shall find the AV CE (Standard) from the marketplace. The Marketplace page for the AV CE Standard is shown below.

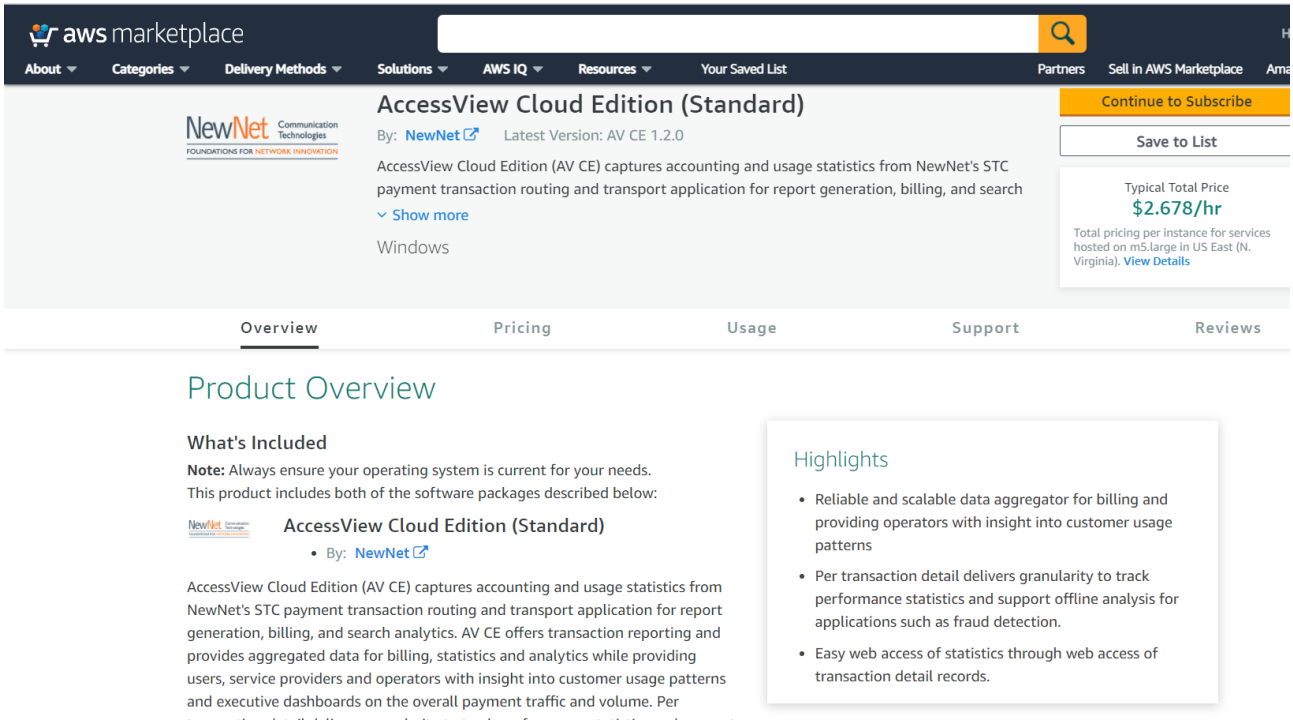


Figure 13: AV CE Market Place page

- Choose the "Continue to Subscribe" Option.
- This navigates to the "Subscribe to this software" page

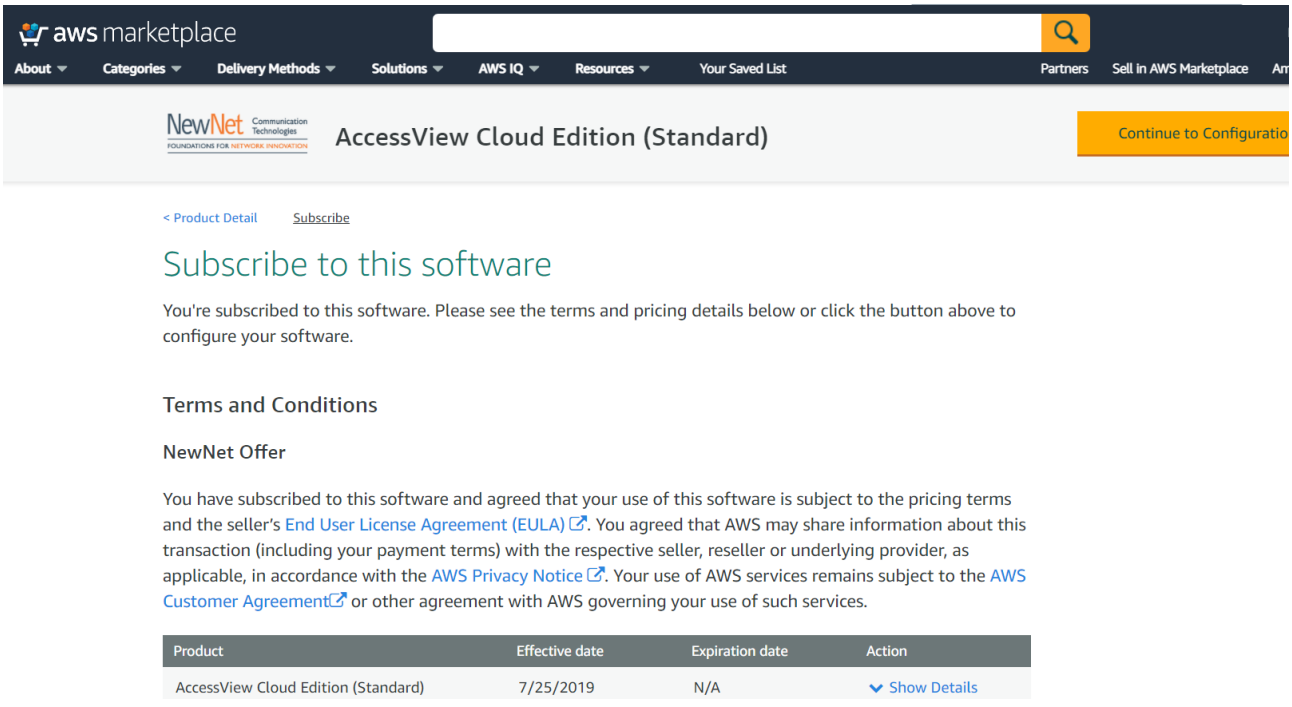


Figure 14: Subscribing to AV

- Choose on “Continue to Configuration” option. This navigates to “Configure this software” tab.
- Choose the “Region” from the dropdown menu and proceed to the launch. Click on the “Continue to Launch” button.

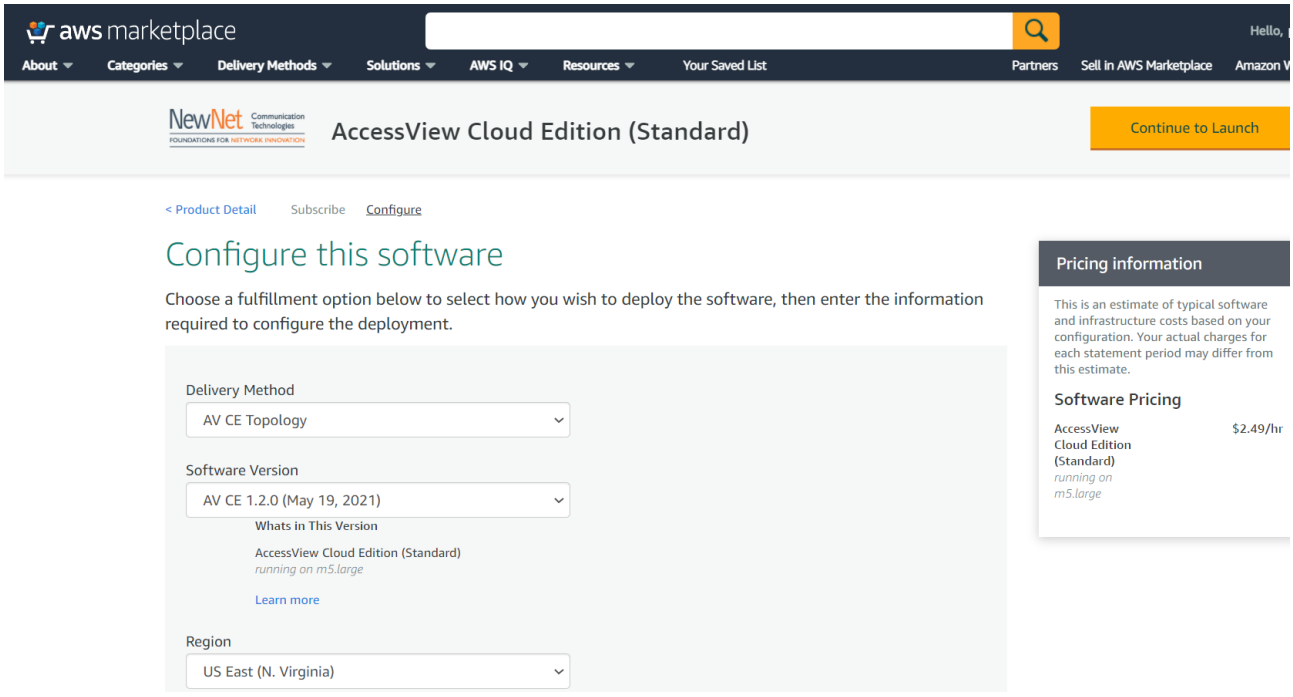


Figure 15: Configure AV

This navigates to the Launch page, choose the “Launch CloudFormation” from the drop down and click on “Launch”

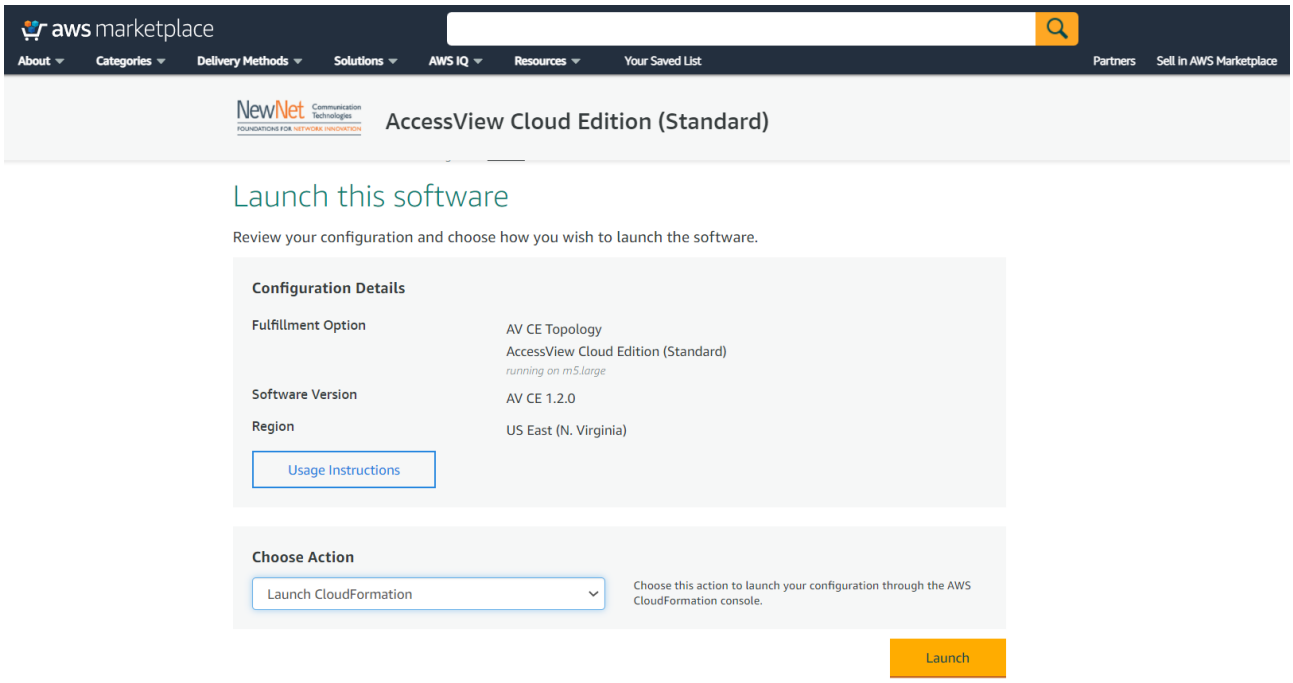


Figure 16 : Launch AV CE

This navigates to the “Create Stack” page. Click on “Next”

4.1 AV CE Cloud Launch

The cloud formation template takes care of deploying the required resources needed and these steps mentioned below guides through creation of the AV CE Stack.

- The “Create Stack” wizard guides through four step processes which are required to be completed to create the Primary Instance.
    a. Choosing Template
    b. Specify Details
    c. Options
    d. Review

Choosing Template

- On selecting the “Launch with CloudFormation Console” option it navigates to the “Choose a Template” page on the “Create Stack” section.
- Choose the “Specify an Amazon S3 template URL”. The URL comes preloaded.

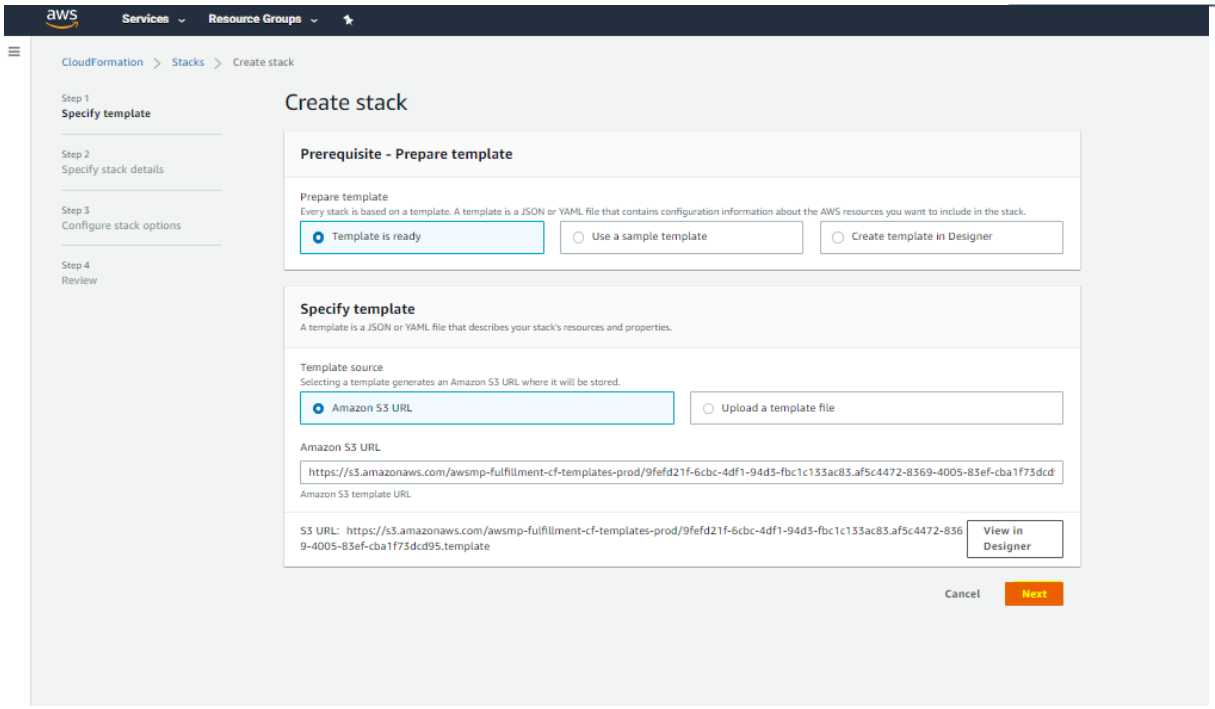


Figure 17 : Choosing Template

Choose NEXT which navigates to the “Specify Details” page.

Specify Details

1. This navigates to the “Specify stack details” page. Enter the relevant values below.

   • Stack name: Specify a Stack name which identifies your stack in AWS. The name must start with an alphabetical character and can contain alphanumeric characters and dashes. Stack name can contain a maximum of 128 characters.

   • VPC: From the drop down choose the VPC created. (Choose the VPC created for STC)

   • Database subnet-a: From the drop down choose subnet created

   • Database subnet-b: From the drop down choose secondary subnet created.

   • STCSecurityGroup: Select the security group created by STC launch or select the security group created for AV CE launch

   • Allowed Remote Access CIDR: Allowed CIDR block for external access.

   • Administrator login public key: <choose the previously created key pair>

   • Remote desktop access CIDR: Allowed CIDR block for accessing web server using RDP client.

   • WebAccessCIDR: Allowed CIDR block for web URL access

   • S3 Bucket for webserver to uploads data files from database: AV CE launch will create the S3 bucket for uploading the data files from the database for user to access. Bucket name

should not contain uppercase characters.

• DBUser : The DBA account username. This refers to the Database user's account name. **This is required during the AV Install and is case sensitive.**

• Database administrator password: The password for the DBUSer. The database administrator account password. Password must be at least 8 characters in length. Should contain at least one lowercase, at least one upper case, at least one numeric and do not contain special characters. **This is required during the AV Install and is case sensitive.**

• ConfirmDBPassword: Re-confirm the password.

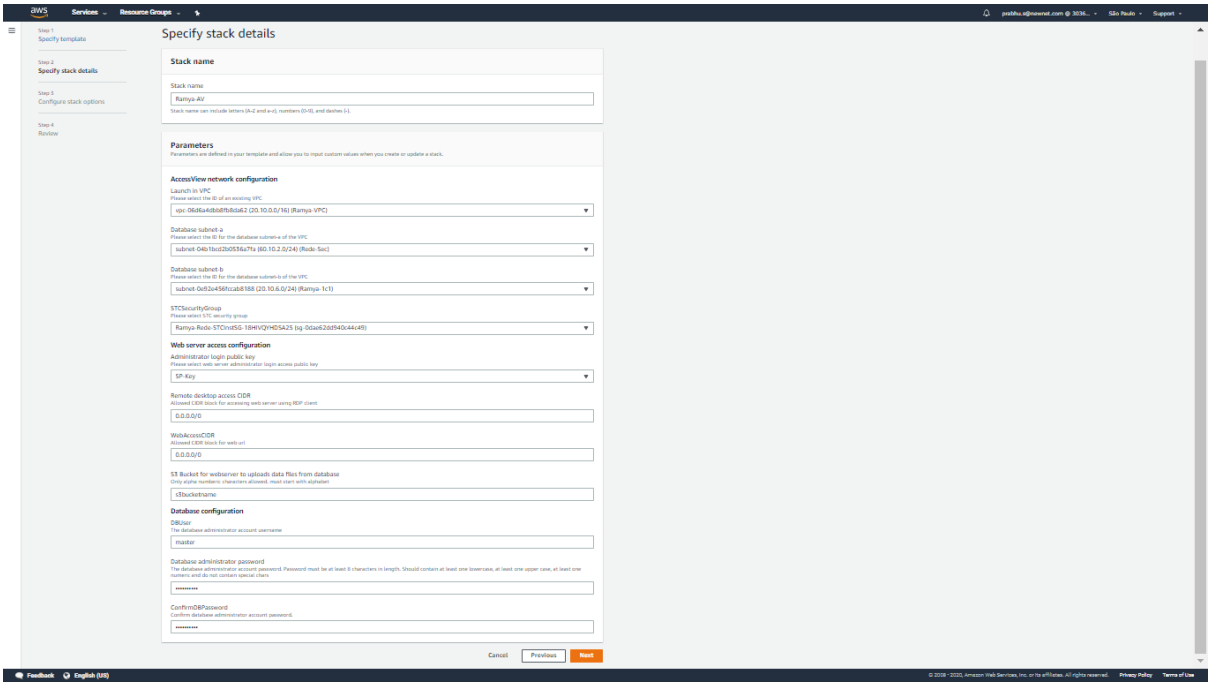


Figure 18: Specify Details Page in Stack Creation

2. Once the entries are filled, click on Next.

Options

The settings in this page are optional.

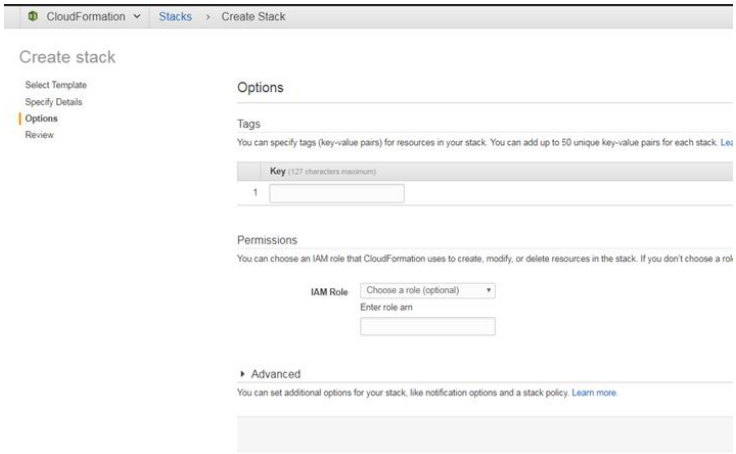


Figure 19: Options Page in Stack Creation

Click NEXT, which navigates to the REVIEW page.

Review

This navigates to the “Review” page. Please review the entries and click on the checkbox at the end of the sheet(highlighted) and click on “Create Stack”(highlighted).

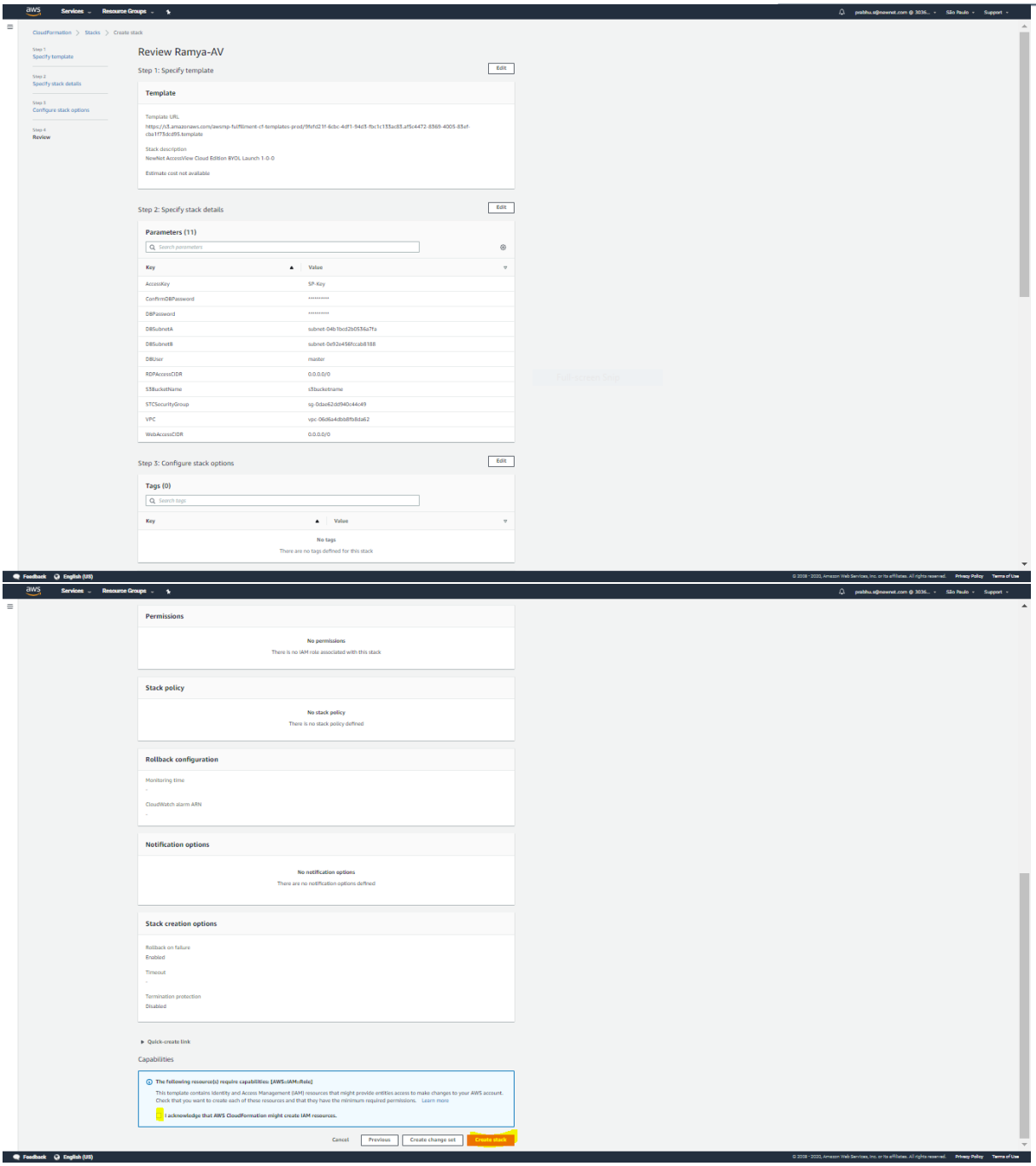


Figure 20: Review Page in Stack Creation

- On clicking on the CREATE tab, the CloudFormation Management Console screen appears.
- Click refresh button on top right corner to view the stack.
- The stack status will be “CREATE IN_PROGRESS”. This process of the stack creation takes several minutes (estimated time 20 mins). On a successful create; the stack status will change to “CREATE_COMPLETE” and this entry will be visible in the first row.

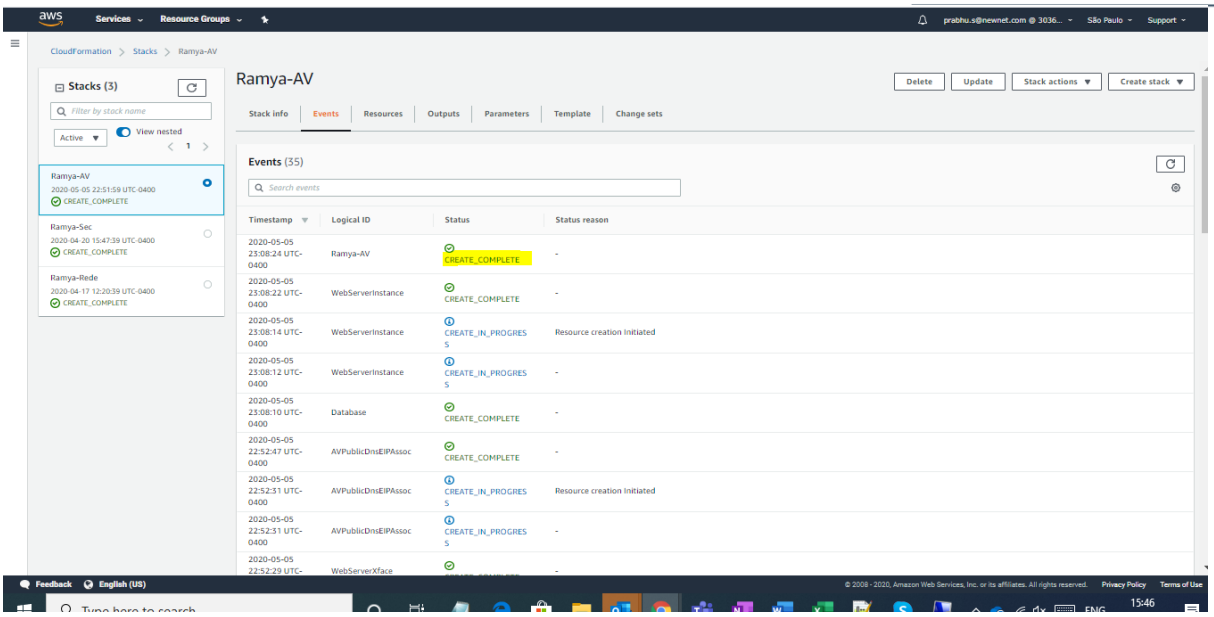


Figure 21 : Stack Creation

Note:

- If the stack detects an internal failure during creation, the cloud formation template terminates the stack.
- If the stack creation is successful, the console displays a success message.
- If stack fails to create in 30 mins, it will be rolled back.

The Output tab displays the information of AV Stack that was launched with Cloud Formation

4.2 AV CE Stack Properties

- Once the stack is created (" CREATE-COMPLETE" is observed), Please select the "Outputs" tab(highlighted) and the **Database URL value is required during AV Installation.**

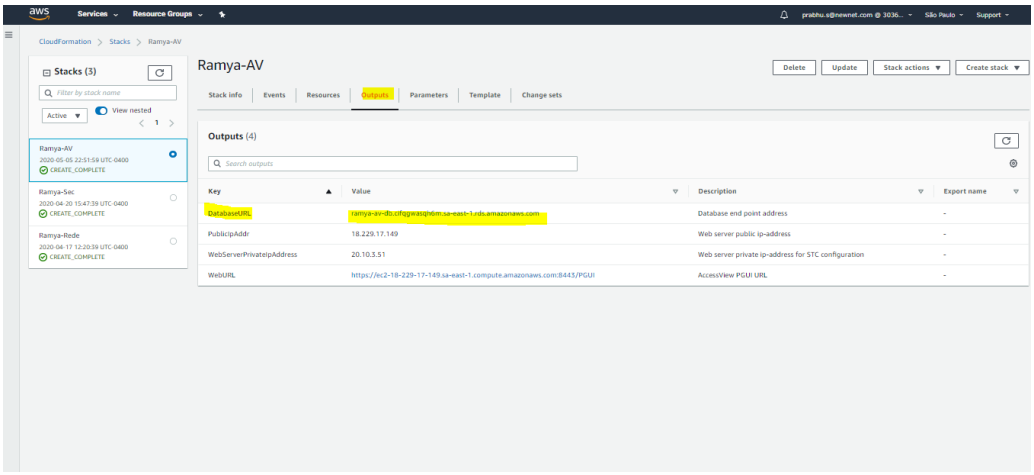


Figure 22 : Outputs tab for the Stack Created

- This completes the AccessView cloud formation and database creation.
- The details of the database created can be fetched by navigating as below(highlighted)

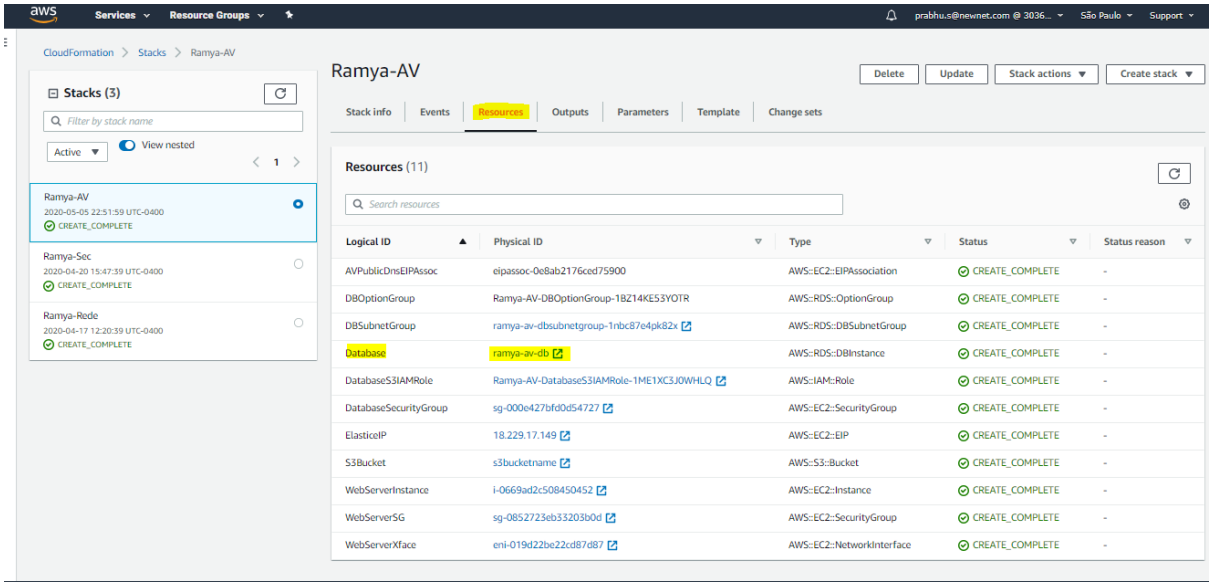


Figure 23: Resources Details for the stack created

- Click on the Resources tab in the cloudFormation sheet. Now click on the PhysicalID (highlighted, in the screenshot above) against the entry Database(highlighted).
- This navigates to the RDS database page where the created database can be found.

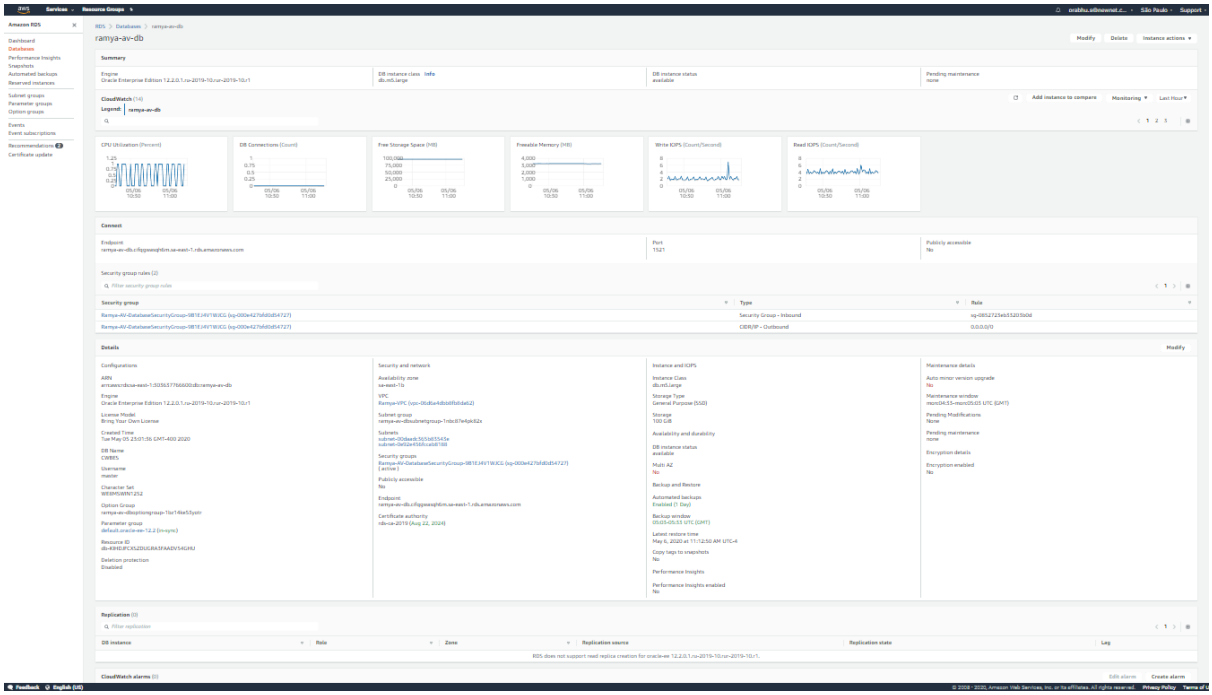


Figure 24 : Database Details

Follow the post install procedure as mentioned in Section 3.6.1. and assign the IAM Role.

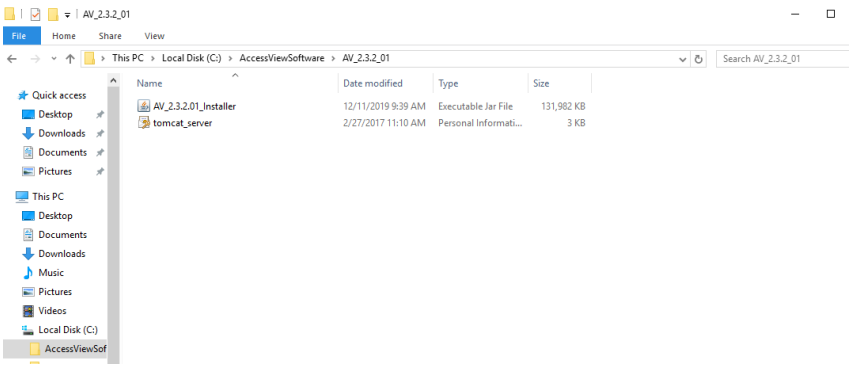
5 Launching the AV CE Instance

Follow the procedure as mentioned in Section 3.3 for logging into the instance as Administrator user.
Ensure to have the details before proceeding.

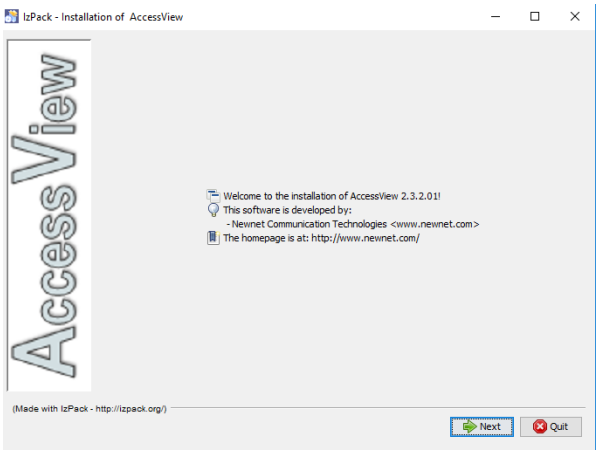
- RemoteDesktop Details; the RDP client, the username and decrypted password
- Database URL
- Database admin username
- Database password.
- Obtain the AV License key from Newnet Services team.

5.1 *AccessView Application installation*

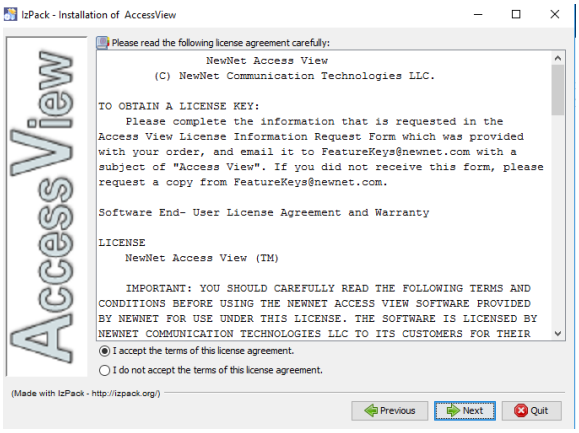
1. AV installer is available at C:\AccessViewSoftware\AV_2.3.2\AV_2.3.2.01_Installer.jar Double click on the installer or alternatively user can run from command prompt. java -jar AV_2.3.2.01_Installer.jar



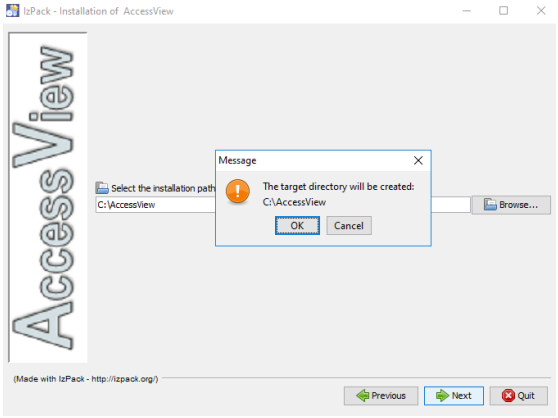
2. Click on “Next”



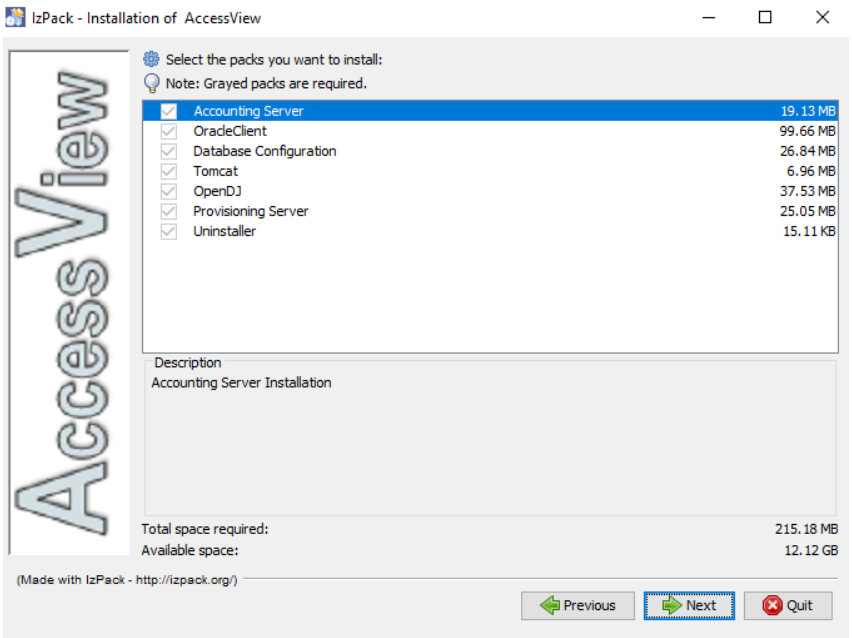
3. After reading the license choose the “I accept the terms of this license” and click on “Next”



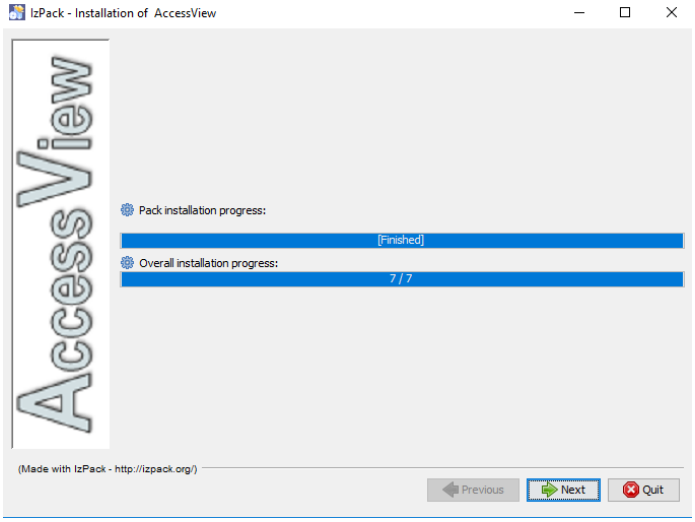
4. Select the Installation path or retain the prompted path and click on “Next”. This prompts for the directory to be created for AV install if not present. Click on “OK”



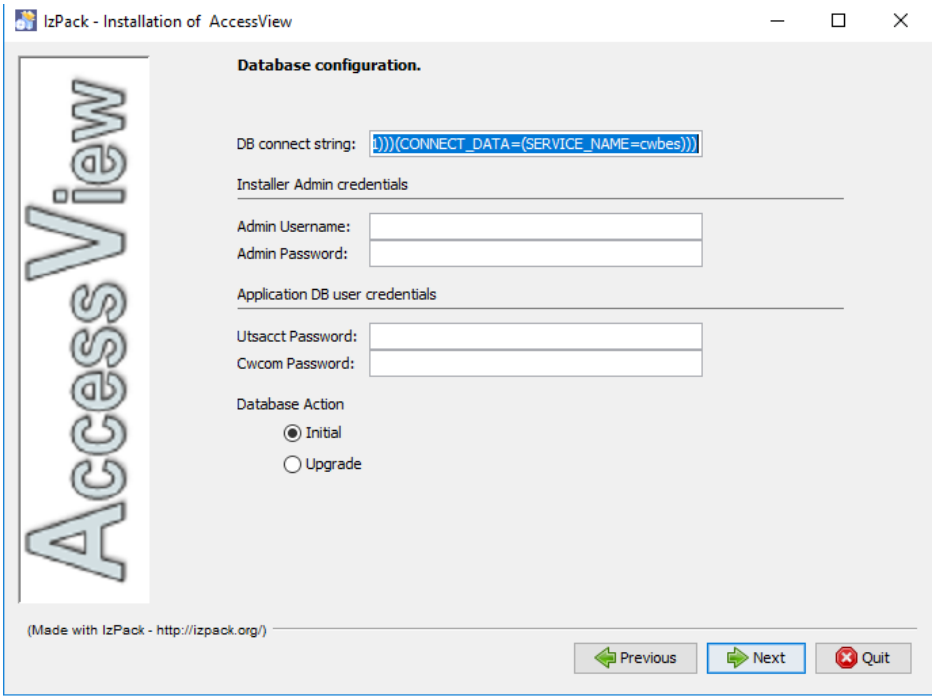
5. Click on “Next”. Wait for a few minutes for all the modules to be installed.



Once this is complete, u see the below screen, click on “Next”



6. Enter the below values and click on “Next”



DB Connect String: Edit the connect string replacing the Host value with “DatabaseURL”. (Provided from CloudFormation).

(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=**”Database URL”**)(PORT=1521))
)(CONNECT_DATA=(SERVICE_NAME=cwbes)))

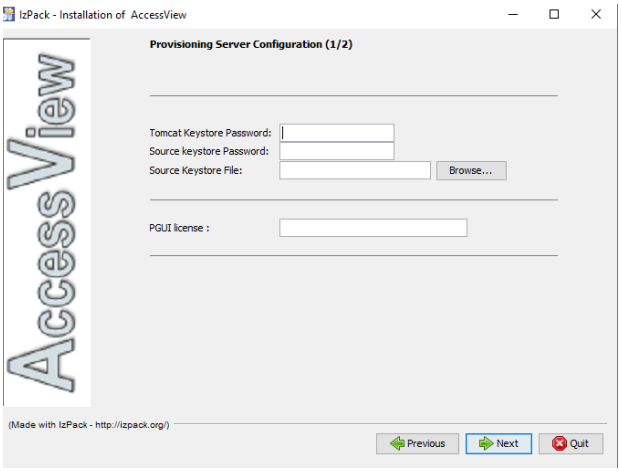
Admin Username: The Database user that was created while launching the AV CE Instance launch (Provided from CloudFormation)
Admin Password: The Database password that is given during the AV CE Instance launch (Provided from CloudFormation)

Utsacct password: Key in the desired password for DB user “utsacct” that will created for AccessView application.
Cmcom password: Key in the desired password for DB user “cwcom” that will created for AccessView application.

Database Action: Select “Initial” as this is a fresh installation. Click on “Next”

The database secrets created that are required to connect to the DB are stored in File systems and is encrypted by the application.

7. Key in the values as mentioned and click on “Next”



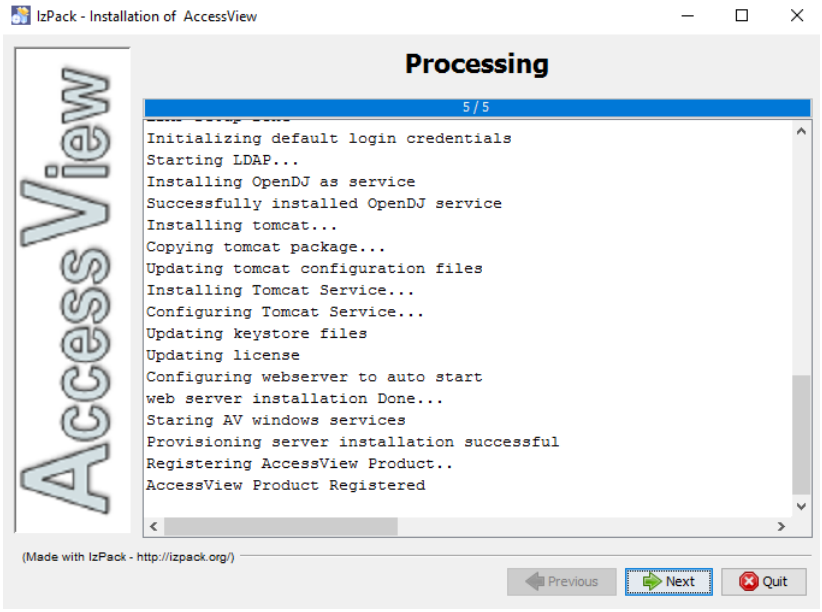
The tomcat Keystore is already generated and placed in the instance and the password for the same is newnet.

- Tomcat Keystore Password: Key in “newnet”; the password for the keystore file for the tomcat web server.
- Source keystore Password: Key in “newnet”; the password for the source keystore for the Tomcat Server.
- Source Keystore File: The self-signed keystore file is present at “C:\AccessViewSoftware\AV_2.3.2.01\tomcat_server.p12”

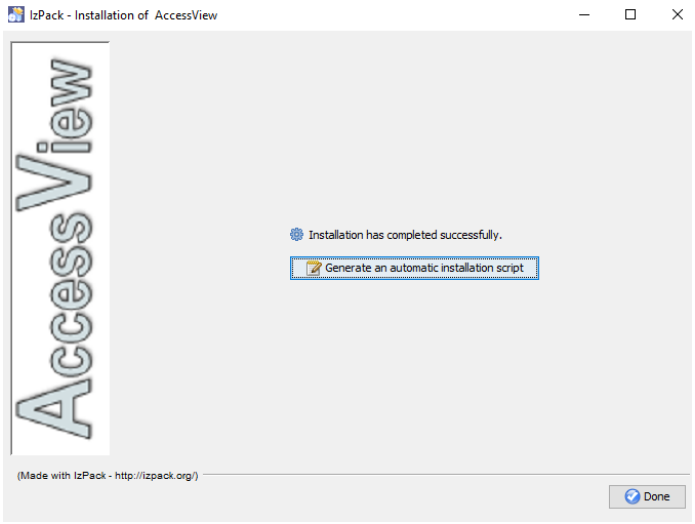
PGUI License: AVCE.

Click on “Next” This will take few minutes as it will create the DB users and the Tables spaces in DB

8. This is the AV Application Installation progress window. Once complete, You will notice “AccessView product Registered” at the end of the screen. Click Next.

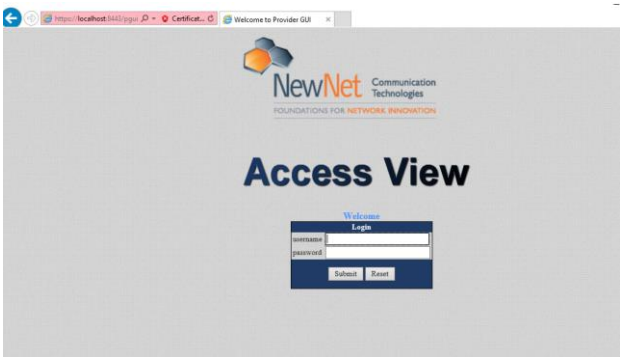


9. Click “Done”

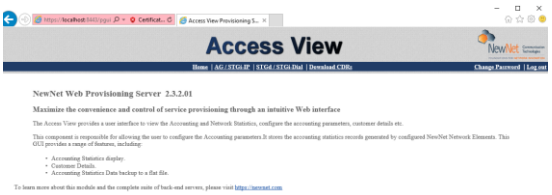


This completes the AccessView application installation.

10. Login to the pGUI of the AccessView application to configure and view the radius packets.
    URL: ***https://<IP>:8443/pgui***
    Username: admin
    Password: besgroup (user can change the password after logging in)
    Click on submit.



11. This navigates to the AccessView pGUI Home page.

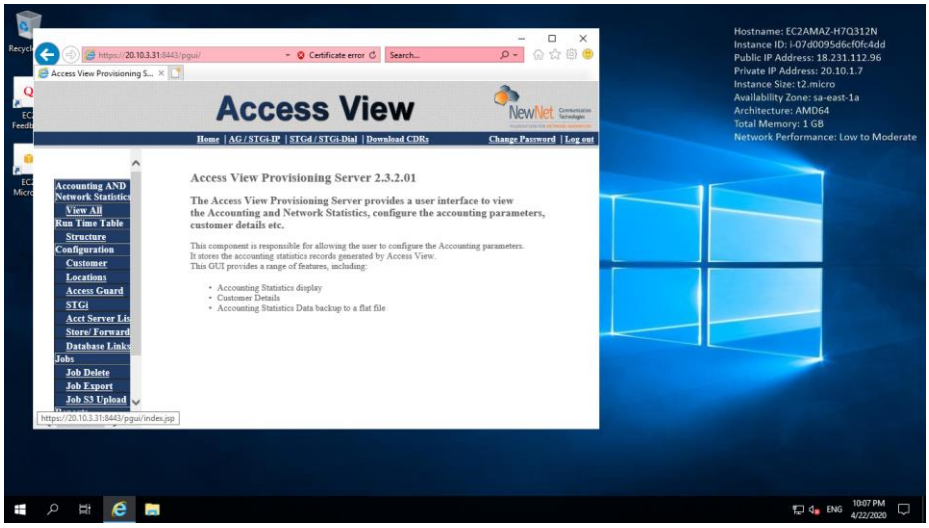


5.2 *AccessView configuration from pGUI*

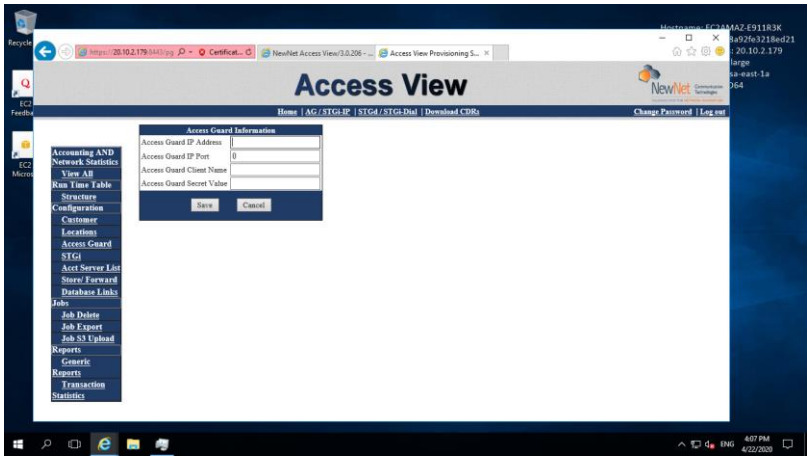
1. Login to the pGUI of the AccessView application to configure and view the radius packets.

URL: ***https://<IP>:8443/pgui***
Username: admin
Password: <password>
Click on submit.

2. Navigate to AG/STGi tab on the top of the page.



3. Click on AccessGuard in the left navigation pane. Click on “Add AccessGuard.”
Add AG (STC IP) and secret (same as configured in the STC)



4. Reboot the AV Instance.

5.3 *Verifying the AccessView functionality*

The Access View server installs the following services during installation and enables them for the functioning.

1. AcctServer
2. AVTomcat
3. OpenDJ

On ensuring the above services are in enabled state and the configurations are present as mentioned in section 5.2, the user can test by receiving a few CDRs from the STC application.
The AccessView pGUI will display these CDRs. These CDRs received from the STC application are stored in the database created.

Logs for the application are available in the following path

1. Accounting server logs are at <AccessView Install path\AS\logs>
2. Tomcat logs are available at < AccessView Install path\tomcat\logs>
3. OpenDJ logs are available at AccessView Install path\opendj\logs>

6 Application Overview

6.1 *Application*

The following resources are created as a part of Accessview Deployment.

- Windows Instance on which the AccessView software will be installed.
    - The AccessView Application installation takes about approximately 10 mins for the complete installation.
- Oracle RDS database
- S3 bucket
    - The Access View application writes the CDRs to the S3 bucket, and this can be viewed only by the account owner and is not public.
    - The S3 bucket created is with permission “Block public and cross-account access to buckets and objects through any public bucket or access point policies.”

6.2 *Application Redundancy*

AccessView application is always installed in conjunction with the Secure Transaction Cloud(STC) instance. It is recommended that AV CE be operated in redundancy mode where two instances of the Access View are launched. STC handles the CDR distribution to the 2 x AccessView instances in a manner to ensure there is suitable redundancy to avoid loss of transmitted CDR data.

Based on the configuration in STC, the CDRs can be mirrored to the second AV CE, or can be configured to accept CDRs in case the first AV CE instance fails.

In active-backup scenario where the primary AV CE goes down, STC can be configured to route the transactions to the secondary AV CE that is setup. Once the primary AV CE is up again, the instance can resume operations for normal functions, and the database will be replicated for synchronization of data.

6.3 *Data Backup and Recovery*

Data backup can be achieved via means where there are 2 instances of the AccessView operational, and they are both configured to receive the data. This ensures both the databases will have all the data received. In the case of active-backup mode, when the failed instance returns to service after downtime, database will be replicated for synchronization of data.

The database snapshot can be generated and later used to retrieve the data as per the documentation of AWS

Create Snapshot :
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_CreateSnapshot.html

Restore from Snapshot :
https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_RestoreFromSnapshot.html

7 Troubleshooting

1. During the Stack Creation process, the process can fail for certain reasons. In such conditions, the stack creation process will roll back and all resources of AWS that was created as part of the process shall be deleted. Some of the reasons for rollback can be.

   Non-Availability of EIPs to allocate in a region
   Not having satisfied the pre-requisite conditions of VPC and subnet creations

2. Incase of an application failure, once the instance is up login to the instance and verify if the AcctServer, AVTomcat, OpenDJ services are enabled. If they are not enabled, try enabling them by a rightclick on the service and setting it to “start” and check the status. If the services donot start, refer to the logs for the specific service in the installation folder.

3. If the webpage fails to login, check if the port 8443 is allowed in Security group. Also, verify if the tomcat service is enabled and has not popped out any error in the logs.

4. If pgui displays a database issue, check if the RDS is active.

5. Incases where the AcctServer service fails to start even on a manual start, look for the logs for license expiry. Contact Newnet support.

6. The recovery of the application is user driven. In case of failure of the AccessView application, the user logs into the system and troubleshoots the system. Contact Newnet support.

8 Update Procedure

1. Double click on the new version of the AV jar file provided.
2. Follow all the steps as mentioned in Section 5.1.1 except for a minor change in Step 6. Choose the option as “Upgrade”.
3. Follow the remaining steps as mentioned.

9 Customer Support

Urgent issues will be prioritized for response within 24 hours and Email queries will be answered within 2 days.

The NewNet Support team can be reached via the link below

https://newnet.com/business-units/secure-transactions/support/support-contact/

10 Best Practices

10.1 *Configuring AWS CloudTrail*

This is an optional configuration left to the discretion of the user. It's recommended to configure CloudTrail for better traceability.

This helps to enable governance, compliance, and operational and risk auditing of the AWS account.
With AWS CloudTrail user can:

- view event history of their AWS account activity, including AWS Management Console actions, AWS SDKs, CLI and other AWS services.
- identify who or what took which action, what resources, when the event occurred.

This event history will help simplify security analysis, resource change tracking, and troubleshooting.
For further information, please refer
https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-getting-started.html

To enable AWS CloudTrail on all production AWS accounts and in every region refer,
https://aws.amazon.com/about-aws/whats-new/2015/12/turn-on-cloudtrail-across-all-regions-and-support-for-multiple-trails/

10.2 *Key Rotation*

User-Keys are generated to access the systems. These keys provide access to the Access View systems. Access keys rotation on a regular schedule is a well-known security best practice because it shortens the period an access key is active and therefore reduces the business impact if they are compromised. For Access Key rotation please refer,

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html#Using_RotateAccessKey
https://aws.amazon.com/blogs/security/how-to-rotate-access-keys-for-iam-users/

10.3 *IAM Best Practices*

To help secure AWS resources, there are some recommendations from AWS for AWS Identity and Access Management (IAM) service.

Please refer the link
https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html