SBC AWS Landing Zone Project

CIDR and Subnet Provisioning in AWS Control Tower using Service Catalog

Version 1.0 Date: 13-Jul-2022

Table of Contents

1 Overview

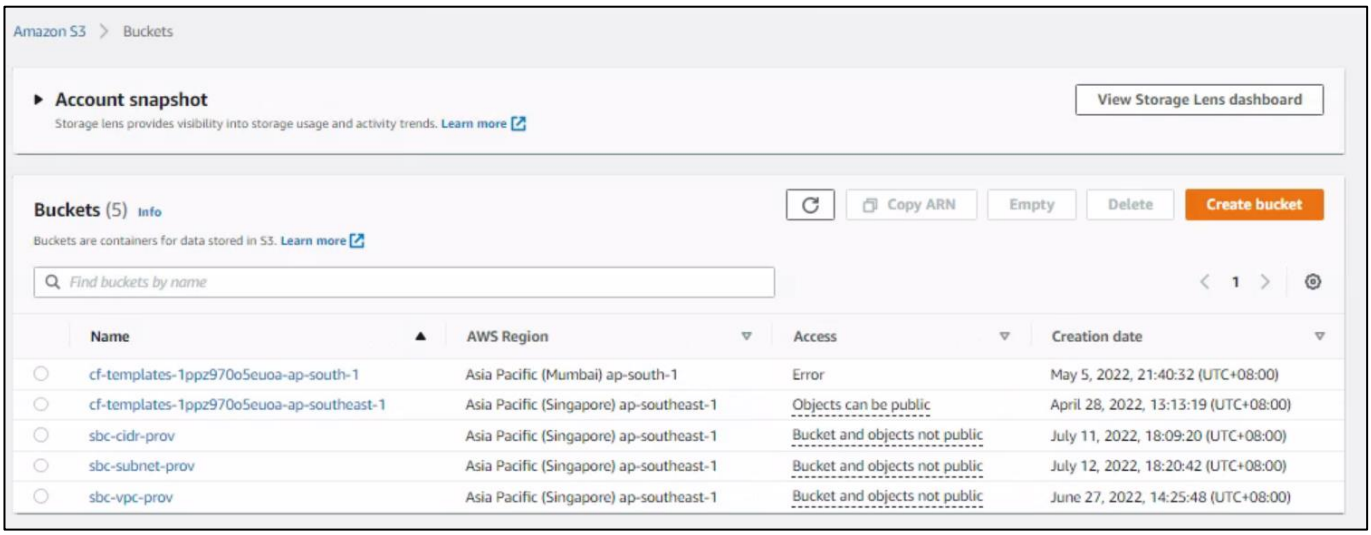
This document describes CIDR and Subnet Provisioning in AWS Control Tower using Service Catalog.

1.1 Assuming VPC Provisioning is done for 1AZ 1Subnet

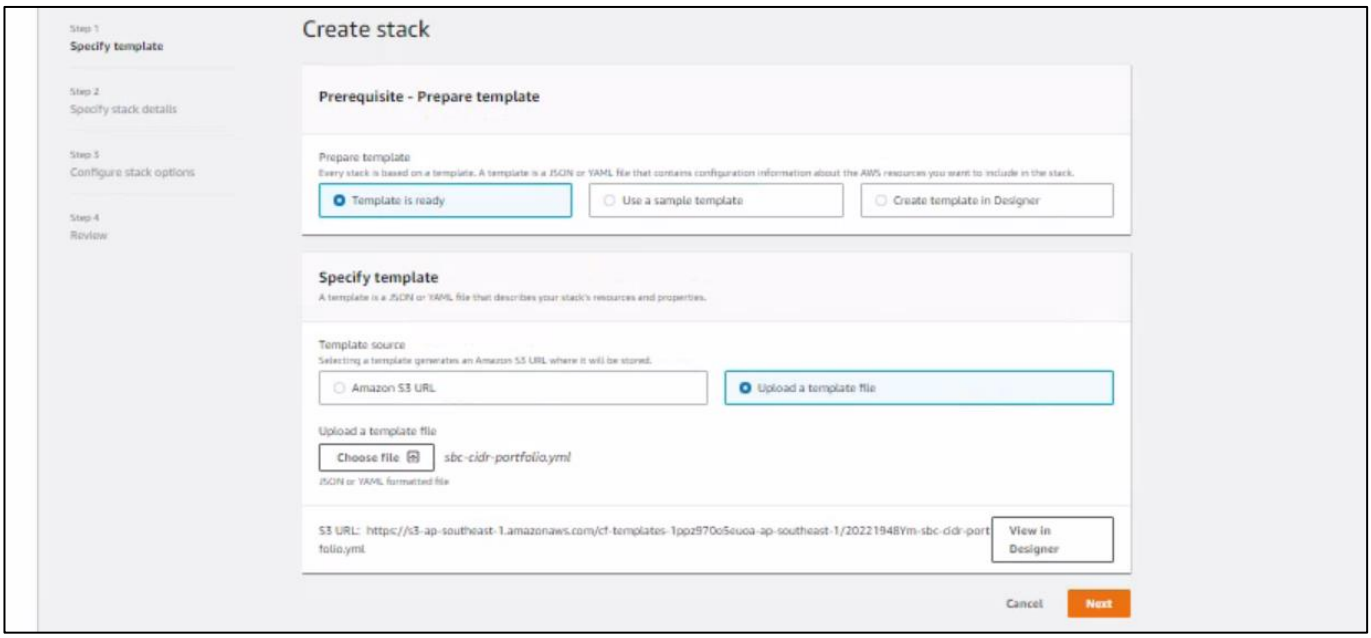
1.2 For adding additional CIDR and subnet in the existing VPC, please follow the below procedure

2 Deploy the portfolio in the AWS Service Catalog delegated administrator account

2.1 Create S3 bucket in AWS Service Catalog delegated administrator account (Refer in Appendix1.1)



2.2 Navigate to Cloud Formation template and create a CIDR Network-Portfolio Stack and upload the file sbc-add-cidr-to-vpc.yml



2.3 On the Specify stack details page, enter a stack name (for example, custom-network-portfolio).

2.4 On the Specify stack details page, enter the following parameters:

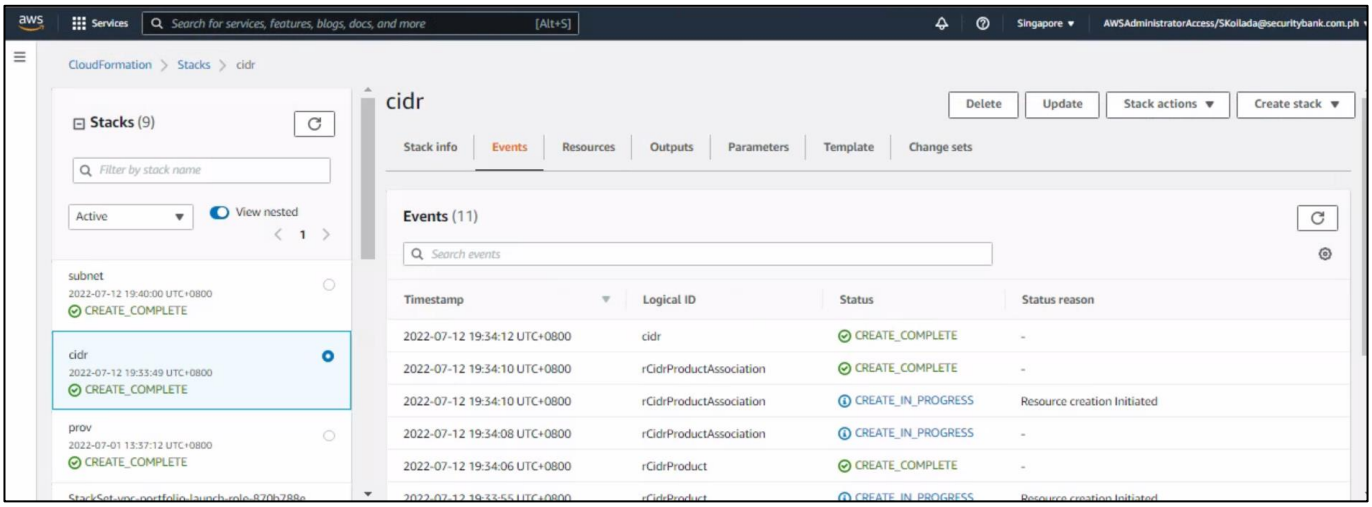
2.5 pPortfolioName: Enter a name for the portfolio (for example, Self-Service Network Portfolio).

2.6 pCidrProductKey: Accept the default Amazon S3 location for the CIDR product template.

2.7 Choose Next.

2.8 On the Configure Stack Options page, enter any tags you want to assign to the stack, and then choose Next.

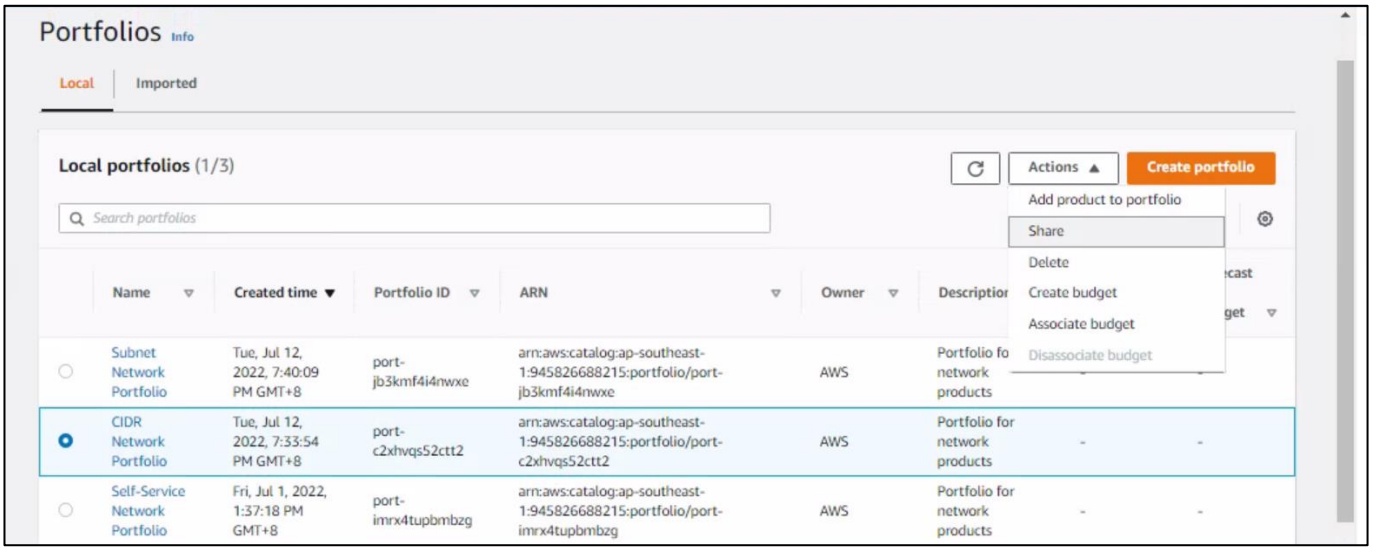
2.9 Verify that the stack has been created successfully before you move to the next step



3 Share the newly created CIDR portfolio with your organization from Delegated Administrator account

3.1 Open the AWS Service Catalog console, and from the left navigation pane, choose Portfolios.

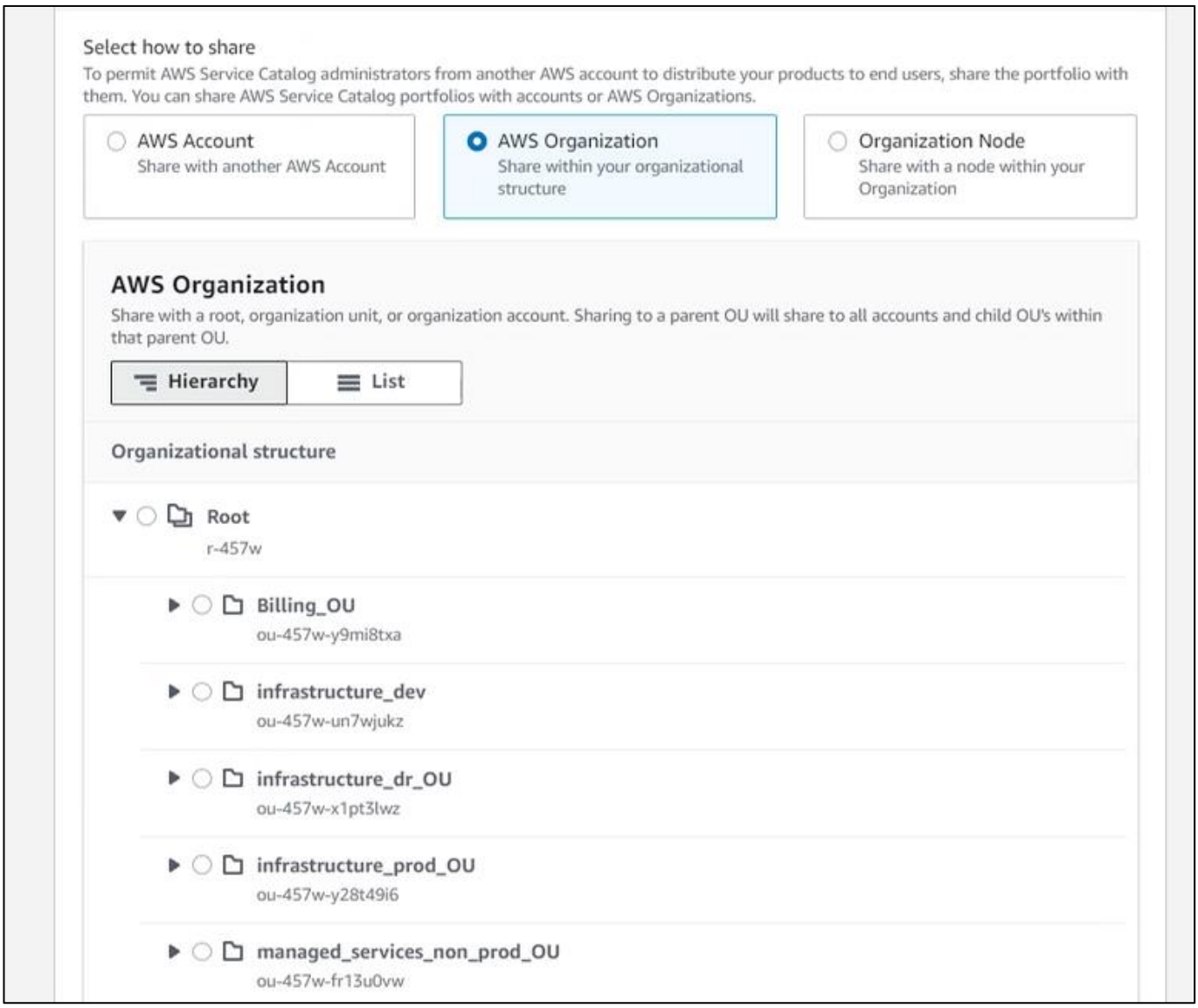
3.2 Choose the radio button next to CIDR Network Portfolio, and from Actions, choose Share.

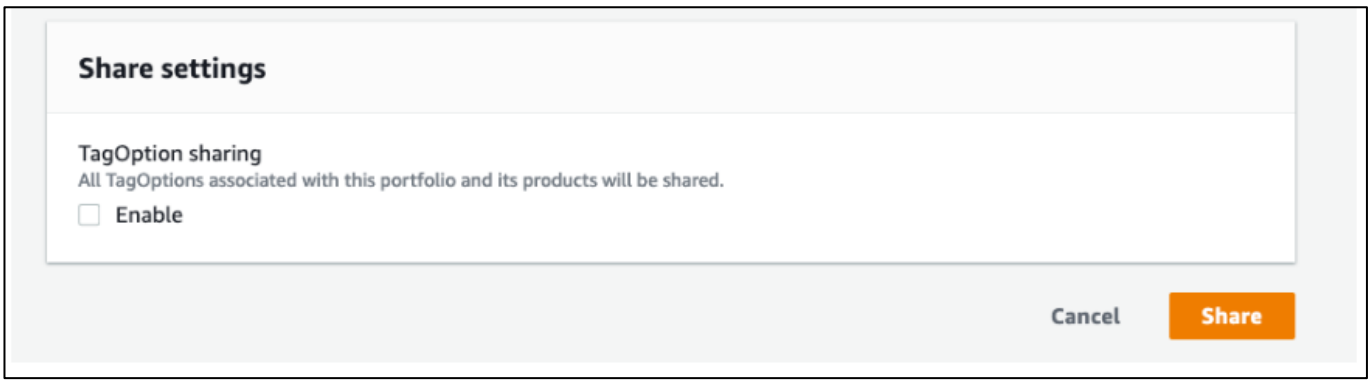


3.3 On Create share: CIDR Network Portfolio, under Select how to share, choose Organization

3.4 Under Select an organizational entity to share with, choose Organization.

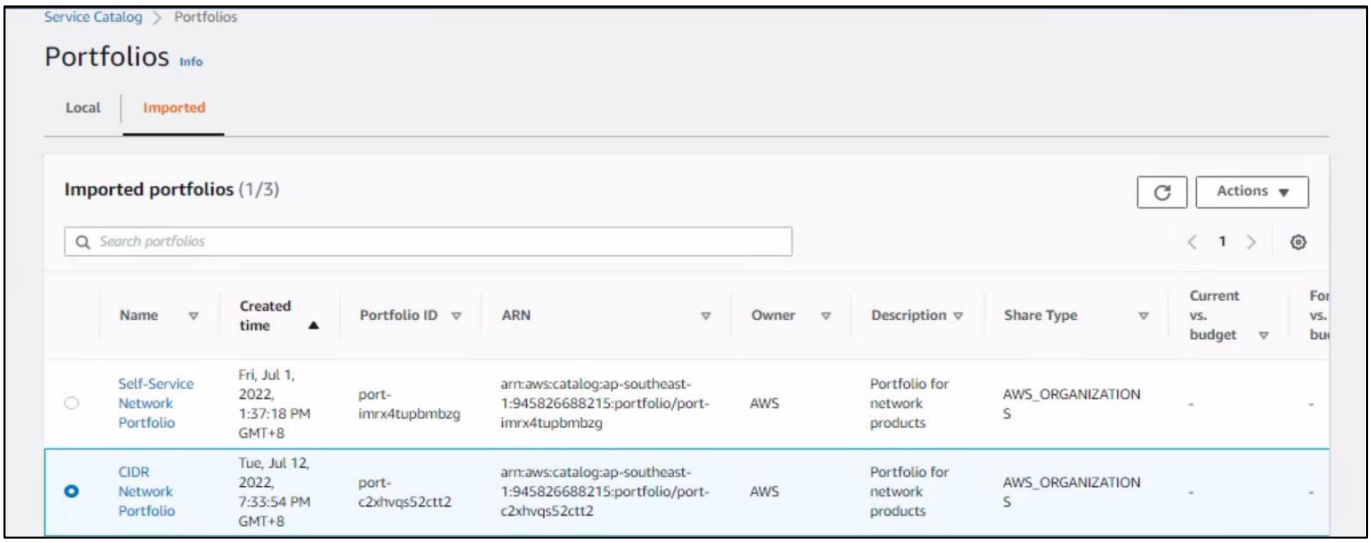
3.5 Under Organization, enter your organization ID, and then choose Share

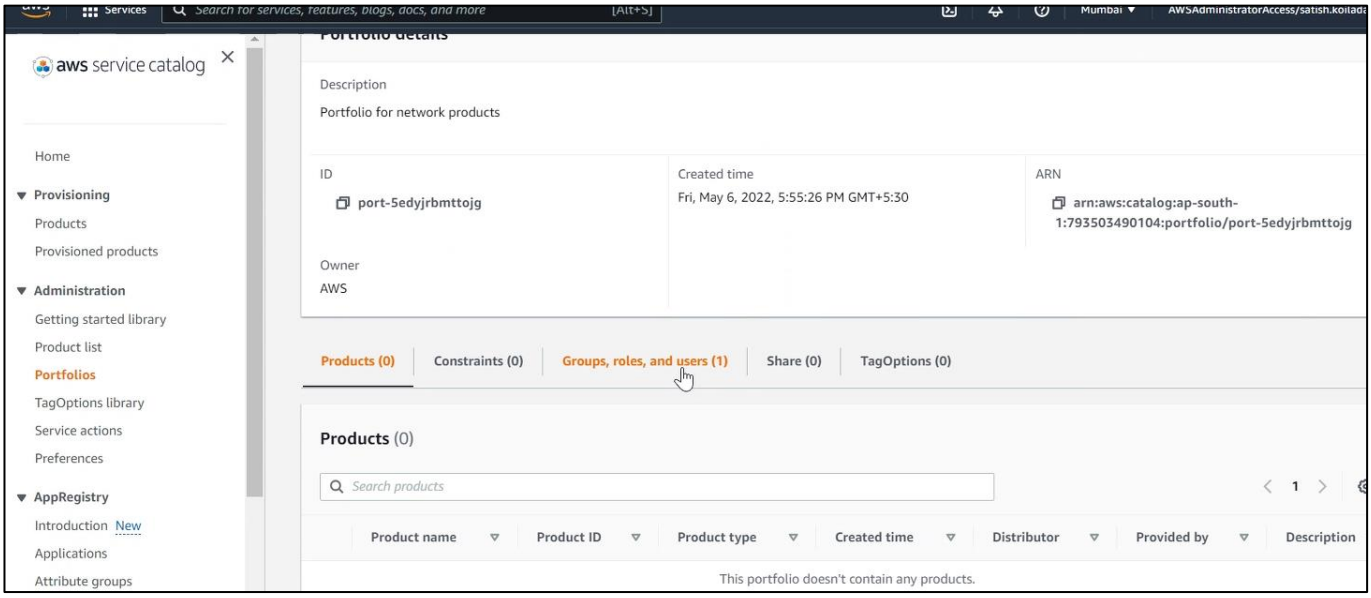

Select how to share
To permit AWS Service Catalog administrators from another AWS account to distribute your products to end users, share the portfolio with them. You can share AWS Service Catalog portfolios with accounts or AWS Organizations.
AWS Account
Share with another AWS Account
AWS Organization
Share within your organizational structure
Organization Node
Share with a node within your Organization
AWS Organization
Share with a root, organization unit, or organization account. Sharing to a parent OU will share to all accounts and child OU's within that parent OU.
Hierarchy
List
Organizational structure
Root
r-457w
Billing_OU
ou-457w-y9mi8txa
infrastructure_dev
ou-457w-un7wjukz
infrastructure_dr_OU
ou-457w-x1pt3lwz
infrastructure_prod_OU
ou-457w-y28t49i6
managed_services_non_prod_OU
ou-457w-fr13u0vw

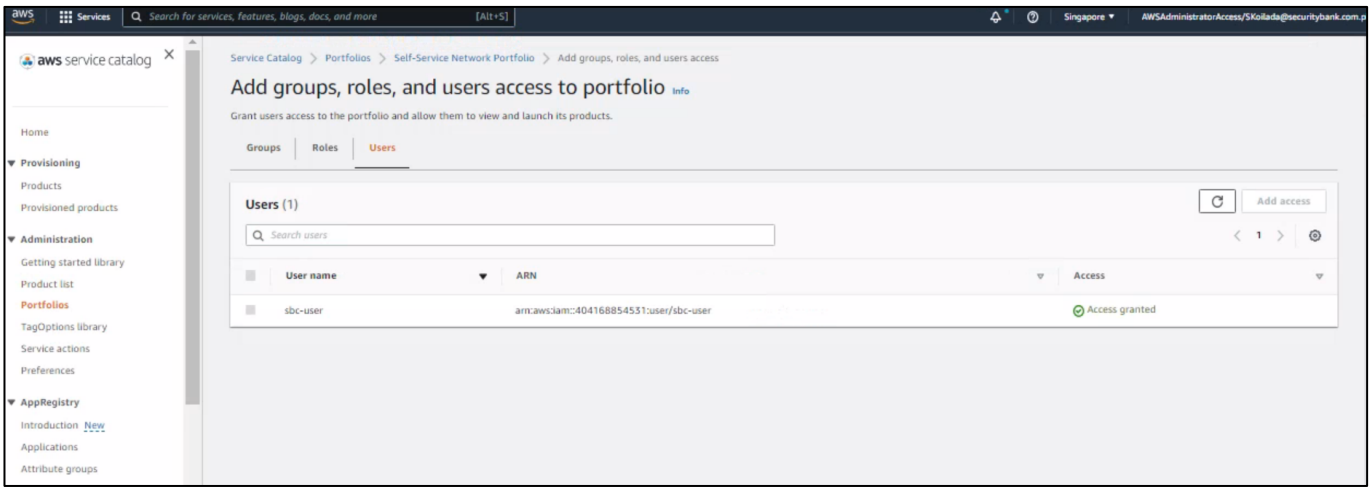

Share settings
TagOption sharing
All TagOptions associated with this portfolio and its products will be shared.
Enable
Cancel
Share

4 Setup user access and provision a custom CIDR using AWS Service Catalog

4.1 Login into the SSO member account and Navigate to Service Catalog Service and click on Portfolio

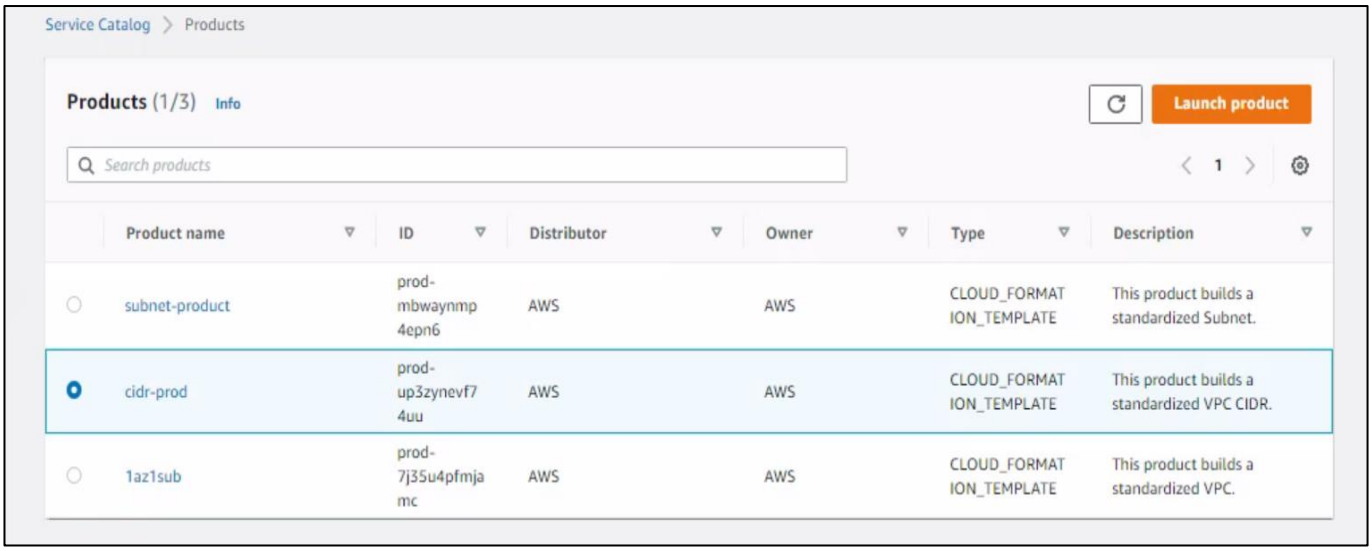




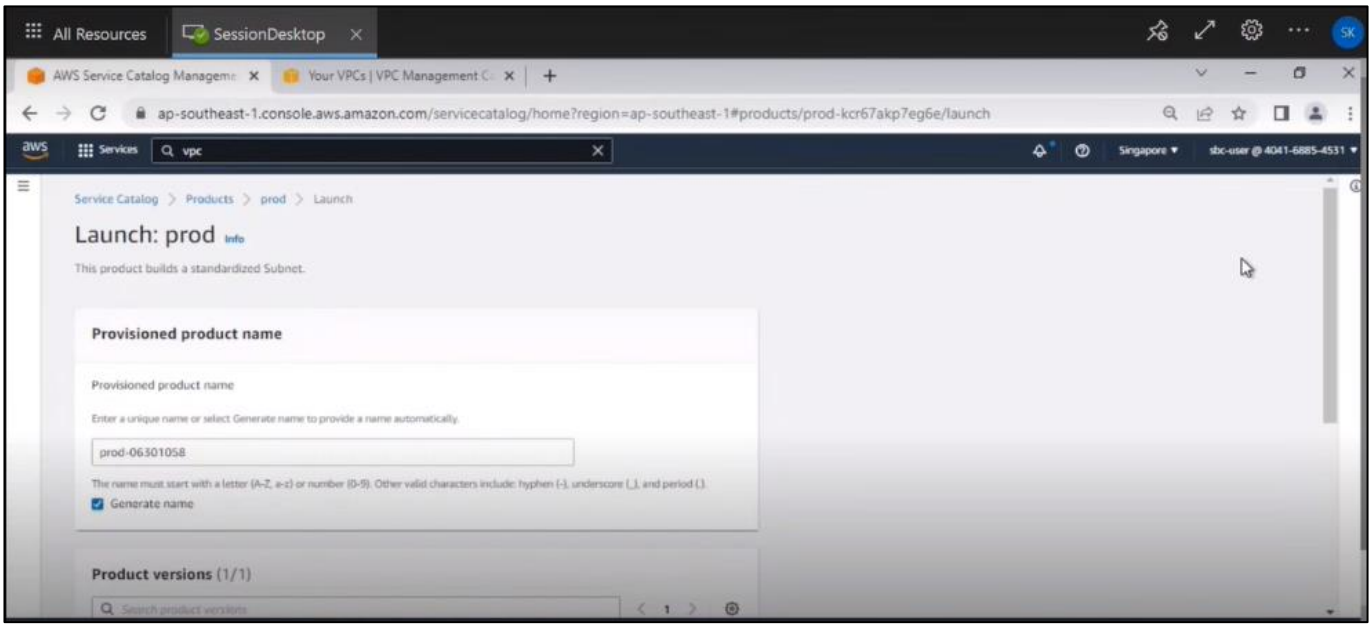


4.2 Now the access has been provided to the IAM user (IAM user which is created as Pre-requisite).

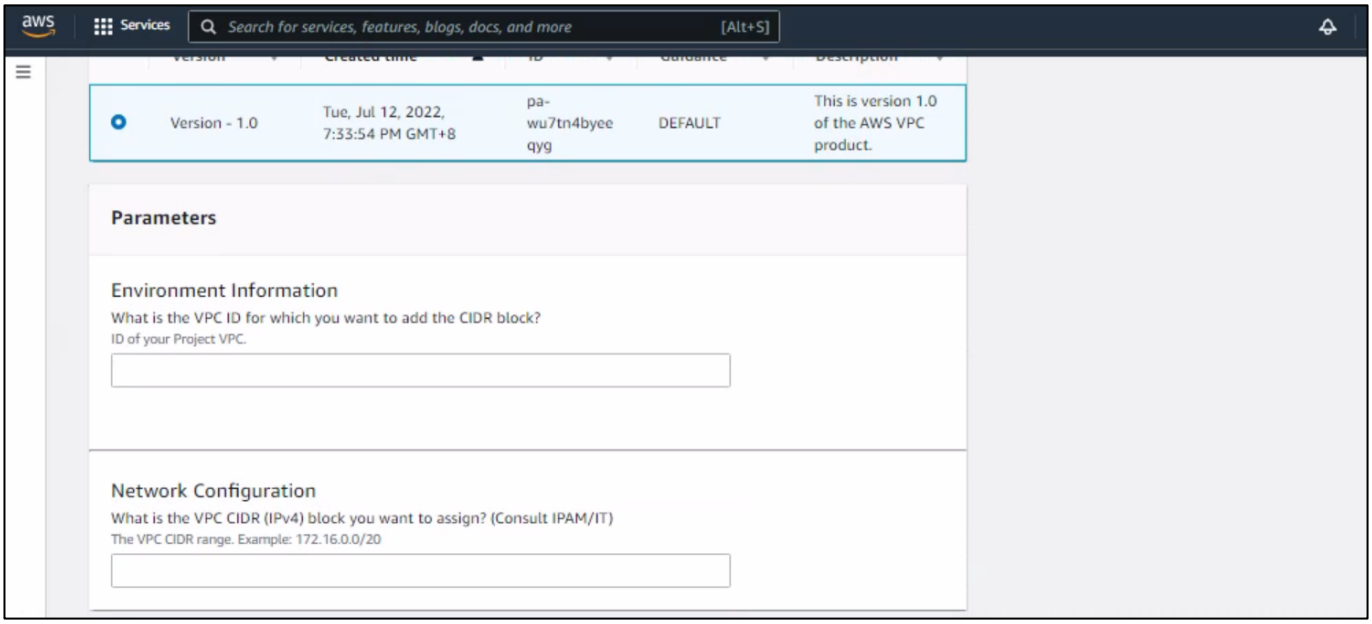
4.3 Login to the member account and Navigate to Service catalog and click on Products.



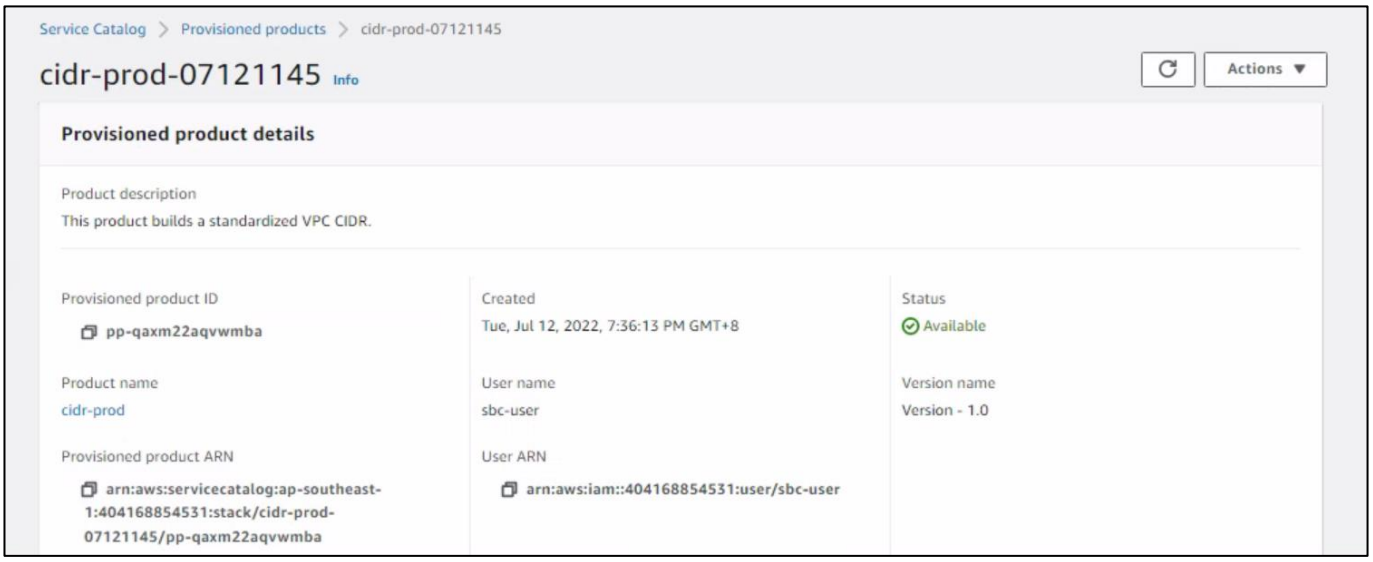
4.4 Now, Click on launch Product



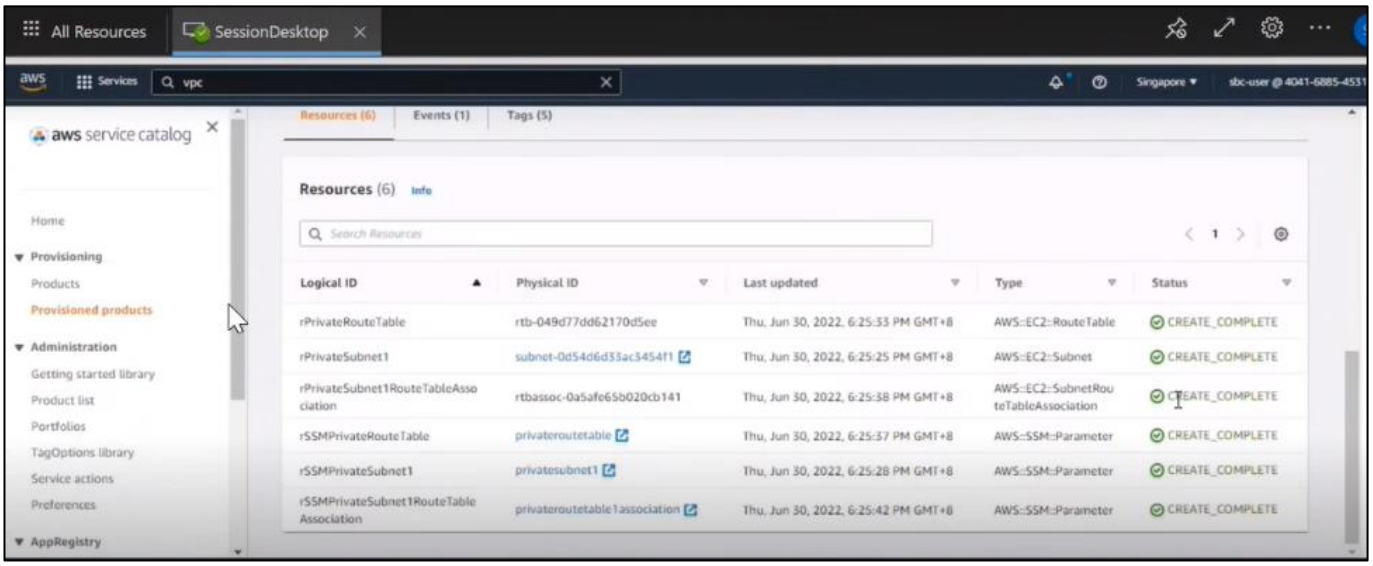
4.5 Fill the Parameter Section a shown in below screen.



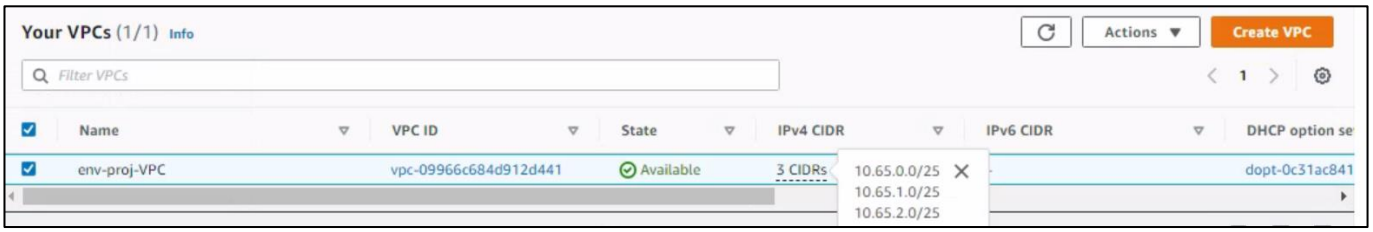
4.6 After Launching the Product, verify CIDR Provision Product.



4.7 Verify that all the resources are created.

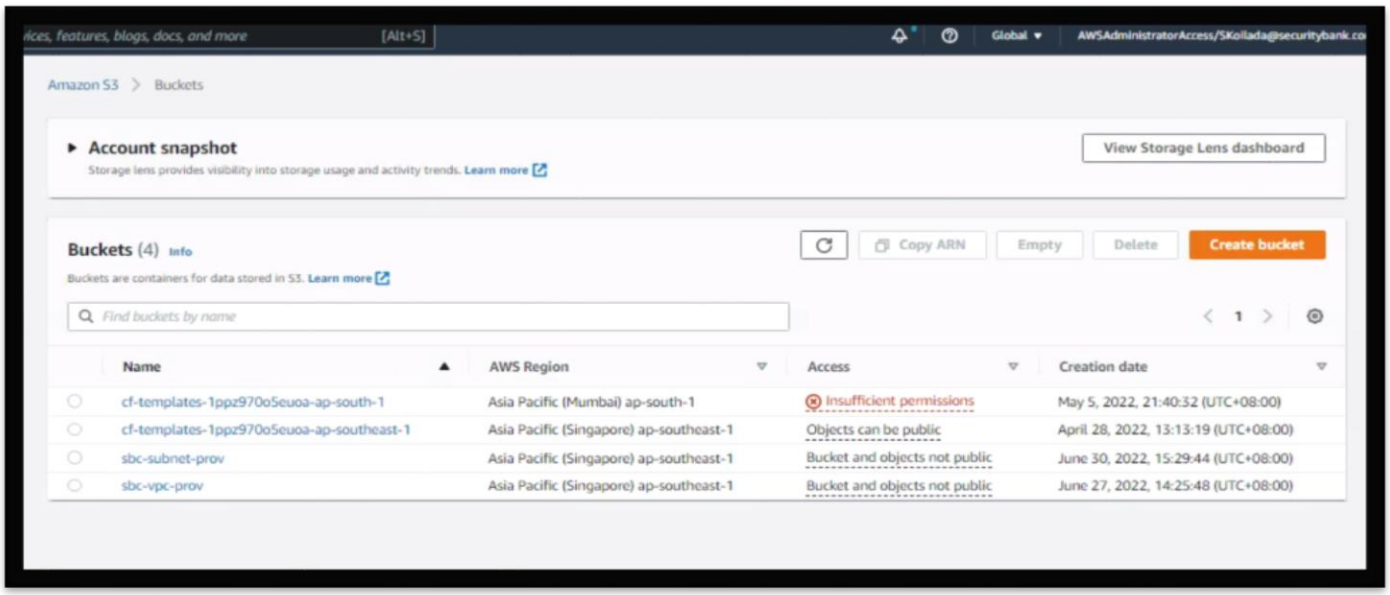


4.8 Verify the VPC and the newly created CIDR block.



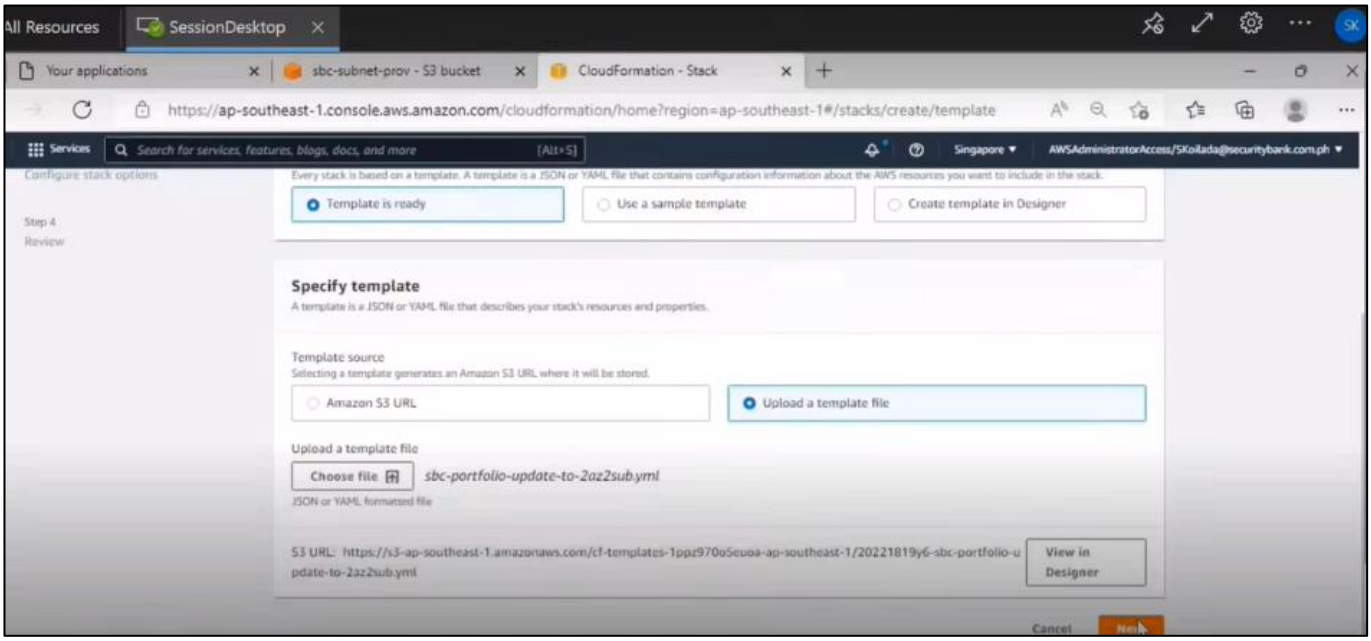
5 Deploy the Subnet portfolio in the AWS Service Catalog delegated administrator account

5.1 Create S3 bucket in AWS Service Catalog delegated administrator account (Refer in Appendix1.1)



5.2 Navigate to Cloud Formation template and create a Network-Portfolio Stack and upload the file

sbc-subnet-portfolio.yml



5.3 On the Specify stack details page, enter a stack name (for example, custom-network-portfolio).

5.4 On the Specify stack details page, enter the following parameters:

5.5 pSubnetLaunchRoleName: Enter the role name that you used earlier. AWS Service Catalog uses this role to launch the VPC product.

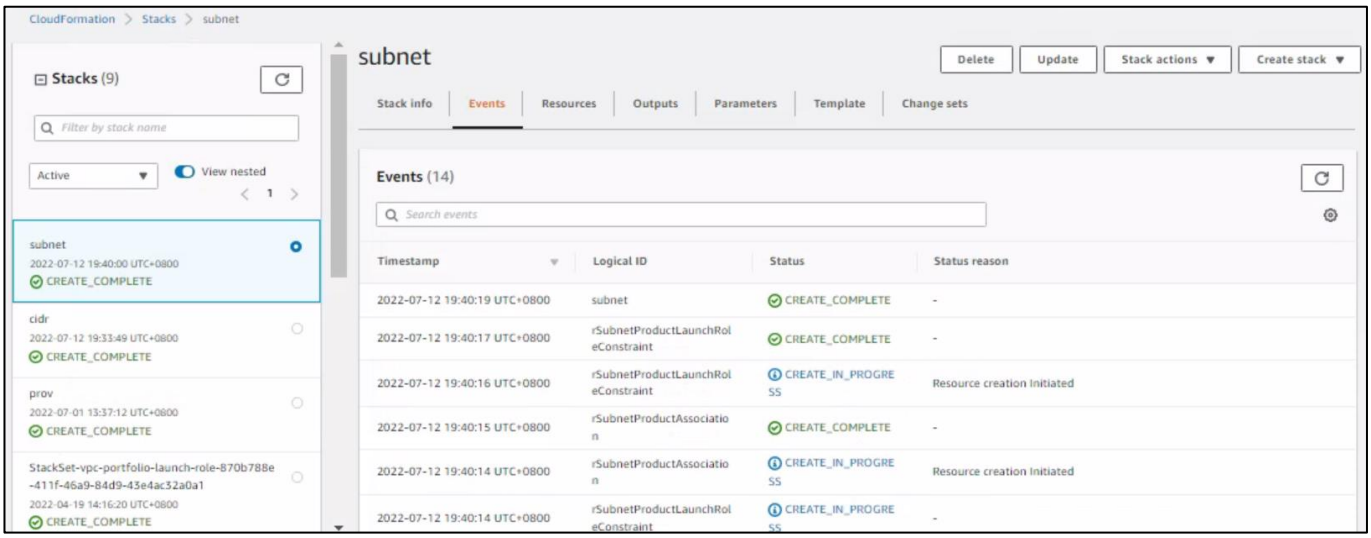
5.6 pPortfolioName: Enter a name for the portfolio (for example, Self-Service Network Portfolio).

5.7 pSubnetProductKey: Accept the default Amazon S3 location for the Subnet product template.

5.8 Choose Next.

5.9 On the Configure Stack Options page, enter any tags you want to assign to the stack, and then choose Next.

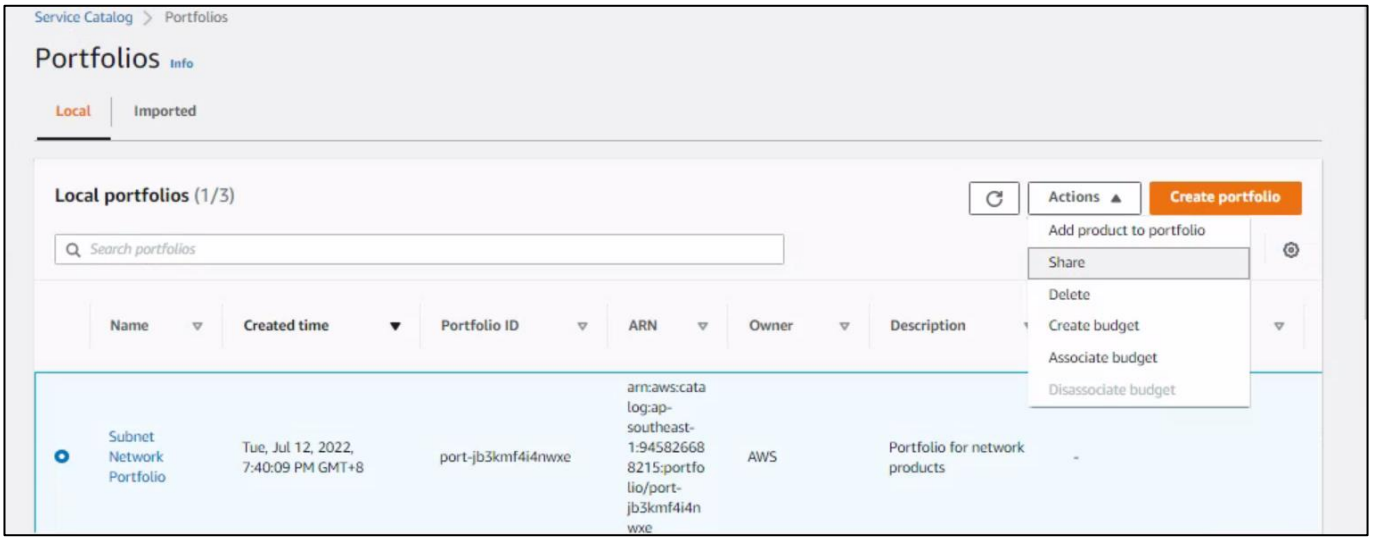
5.10 Verify that the stack has been created successfully before you move to the next step



6 Share the newly created Subnet portfolio with your organization from Delegated Administrator account

6.1 Open the AWS Service Catalog console, and from the left navigation pane, choose Portfolios.

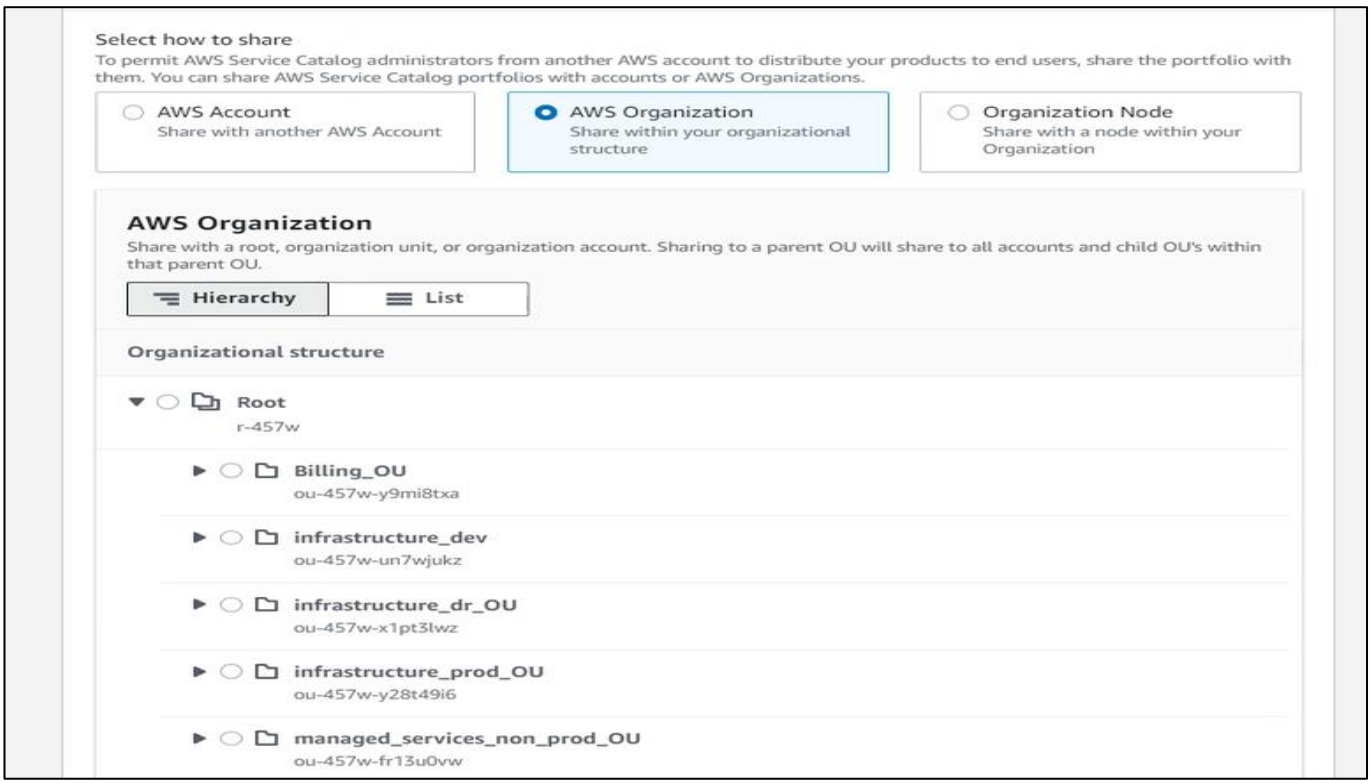
6.2 Choose the radio button next to Subnet Network Portfolio, and from Actions, choose Share.

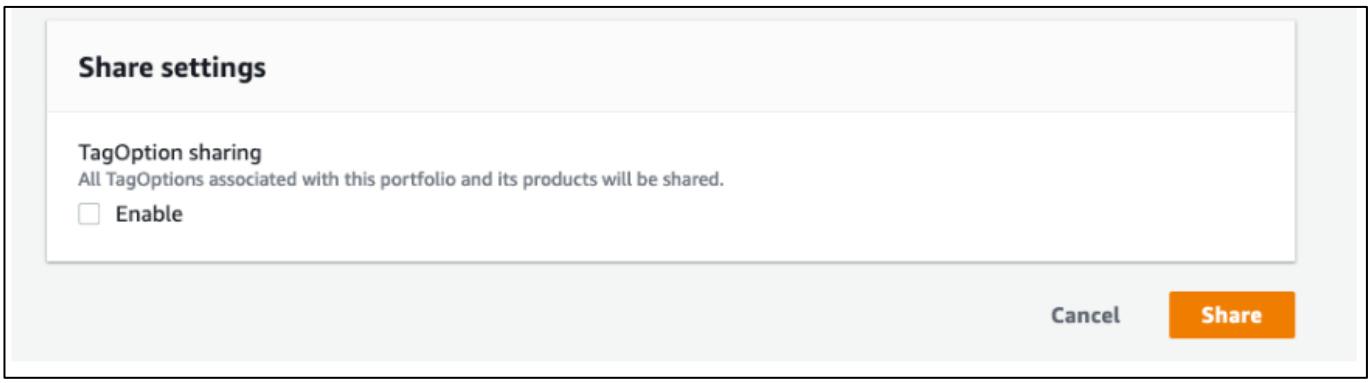


6.3 On Create share: Subnet Network Portfolio, under Select how to share, choose Organization.

6.4 Under Select an organizational entity to share with, choose Organization.

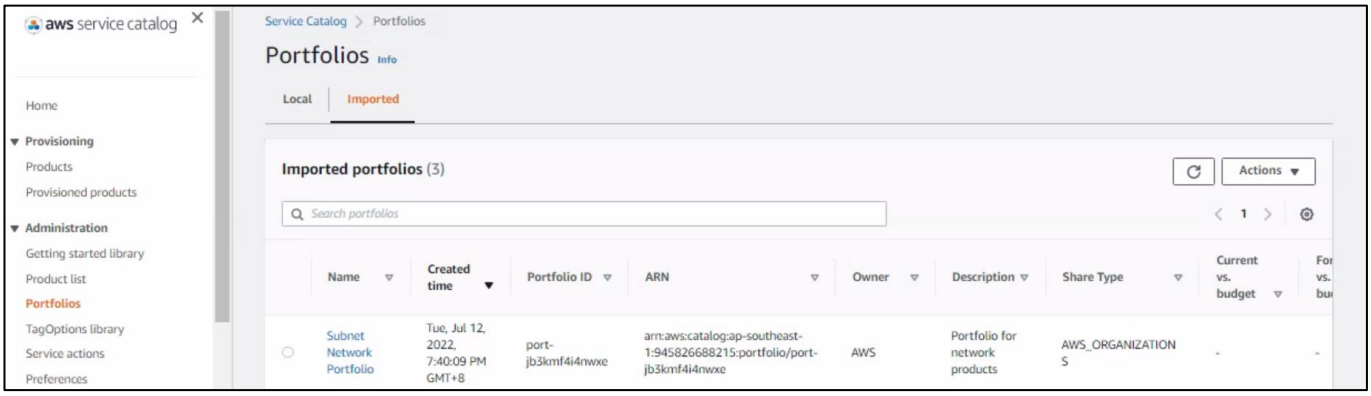
6.5 Under Organization, enter your organization ID, and then choose Share

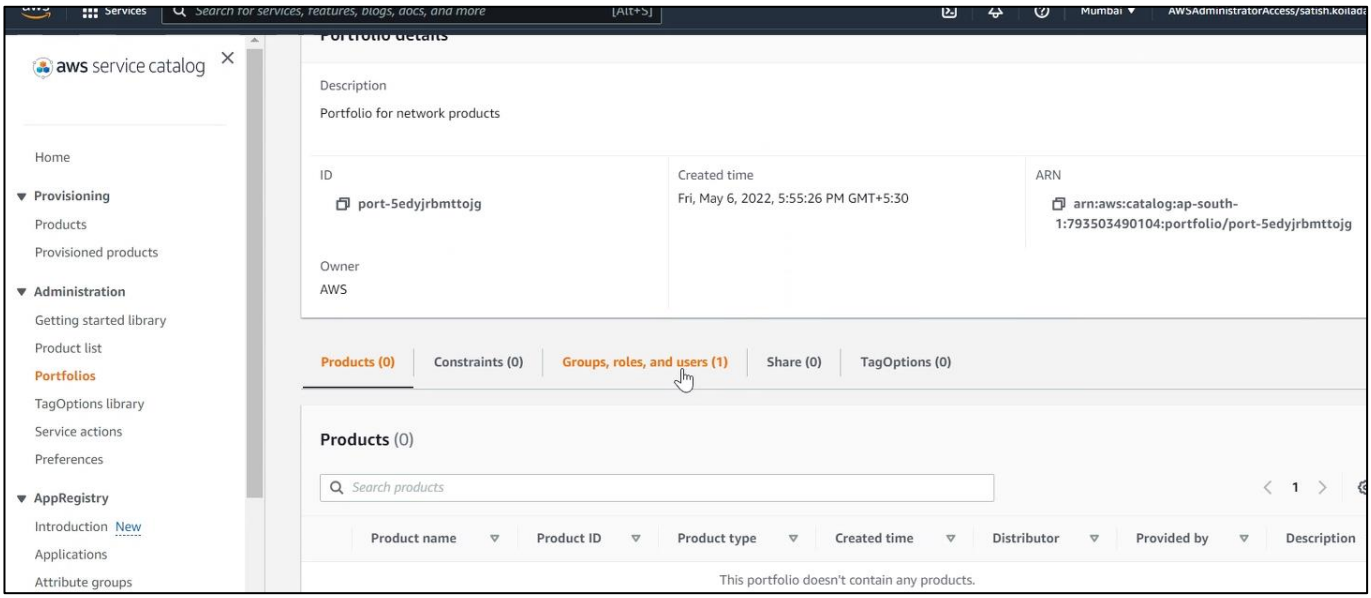


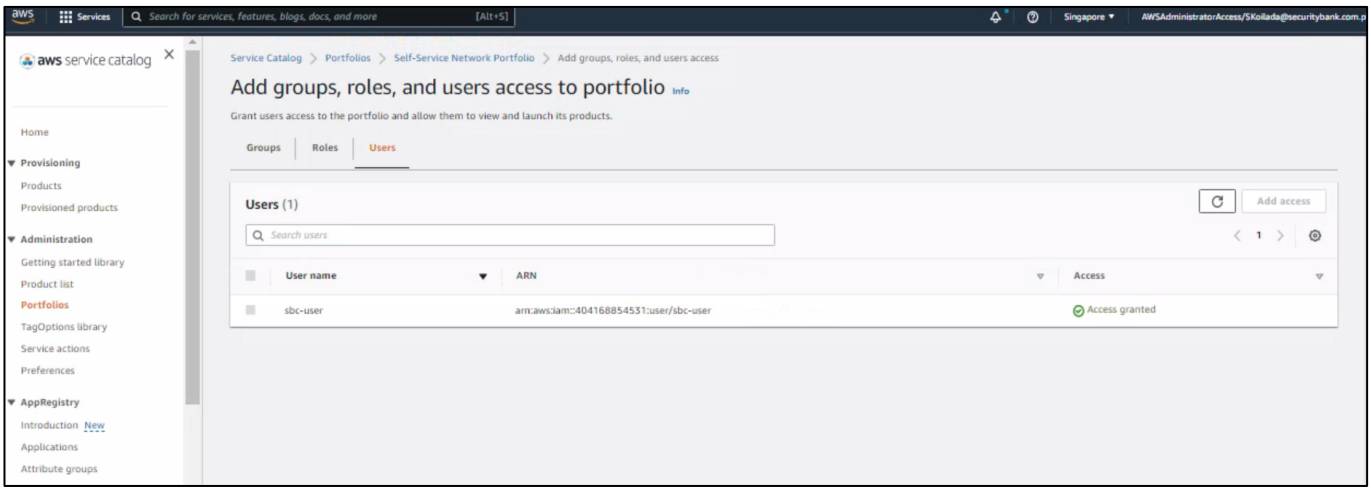


7 Setup user access and provision a custom Subnet using AWS Service Catalog

7.1 Login into the SSO member account and Navigate to Service Catalog Service and click on Portfolio

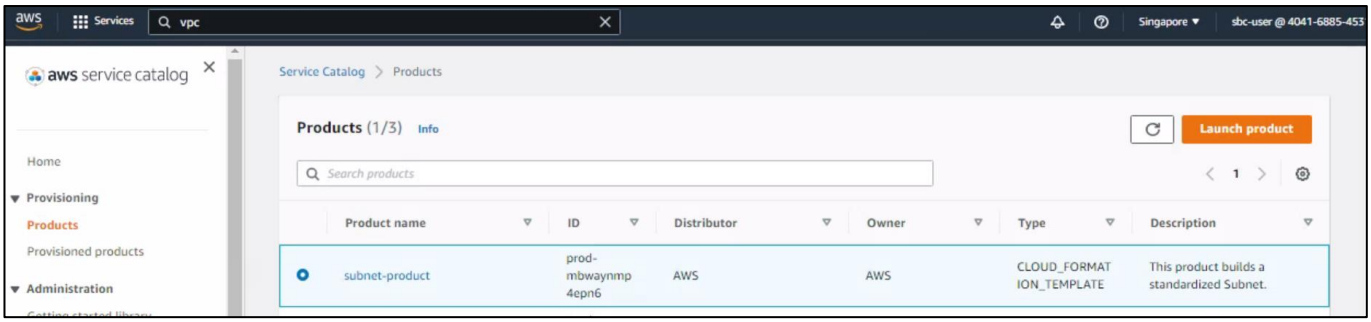




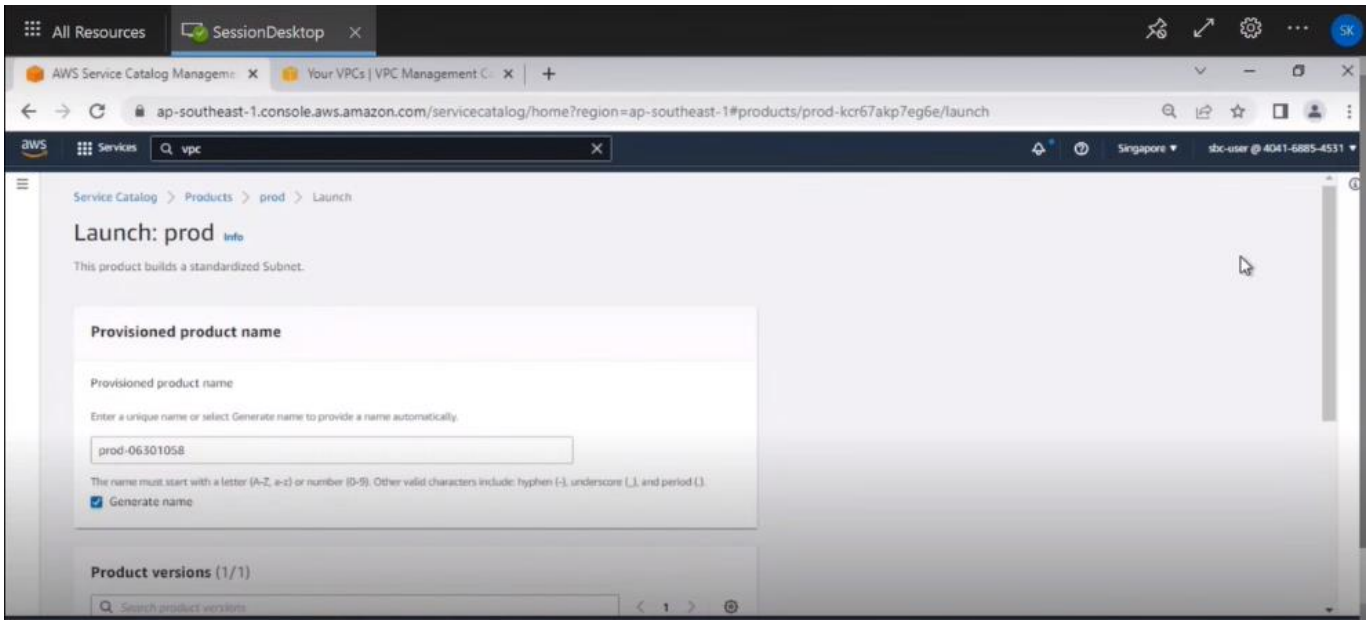


7.2 Now the access has been provided to the IAM user (IAM user which is created as Pre-requisite).

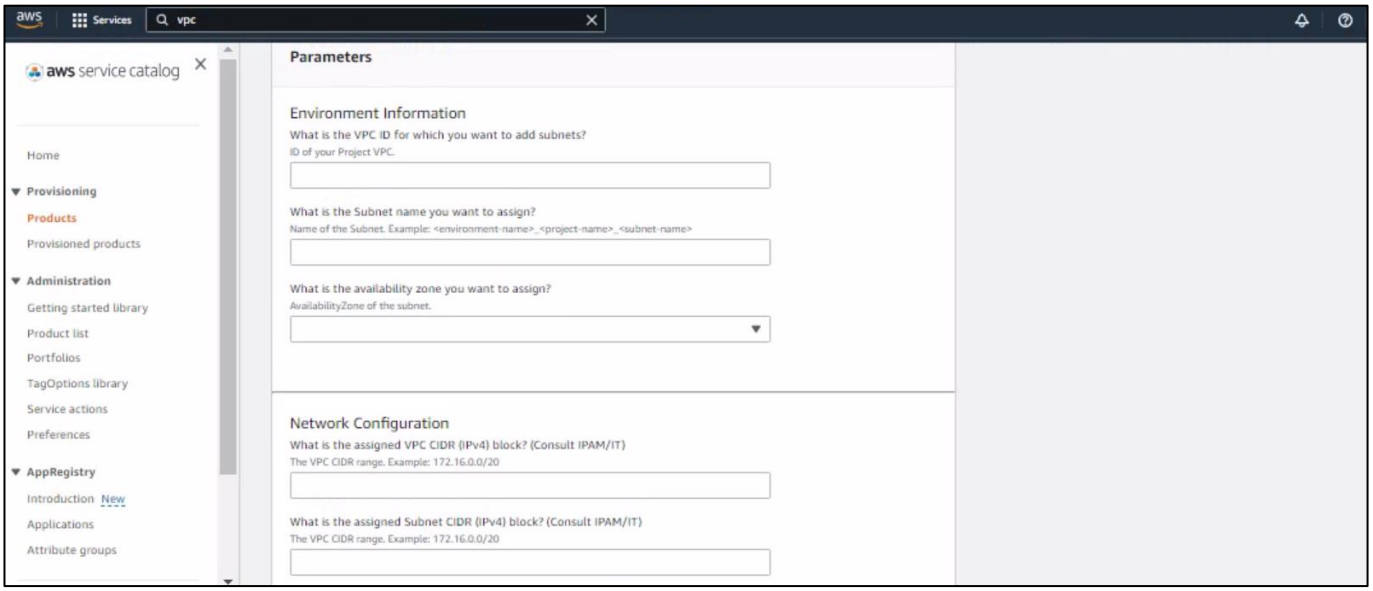
7.3 Login to the member account and Navigate to Service catalog and click on Products.



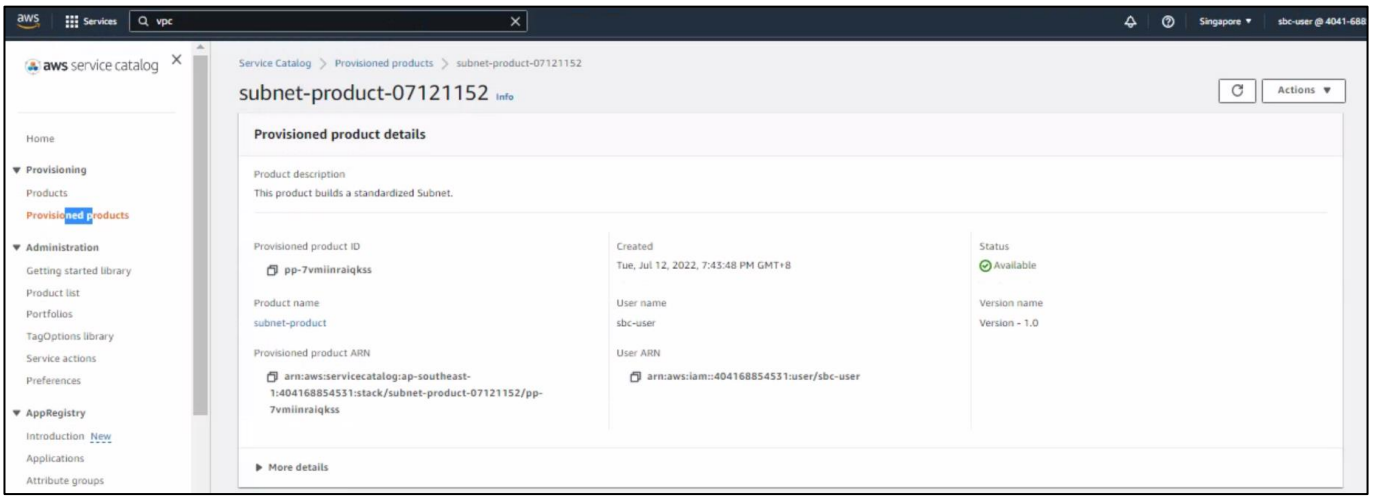
7.4 Now, Click on launch Product



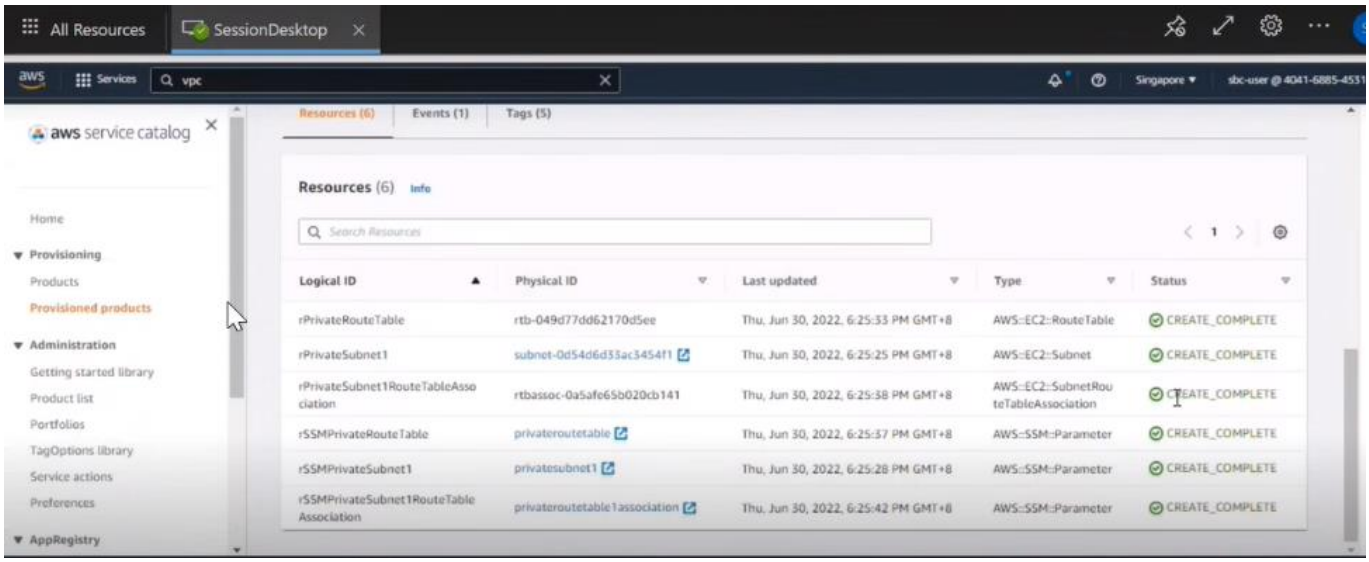
7.5 Fill the Parameter Section a shown in below screen.



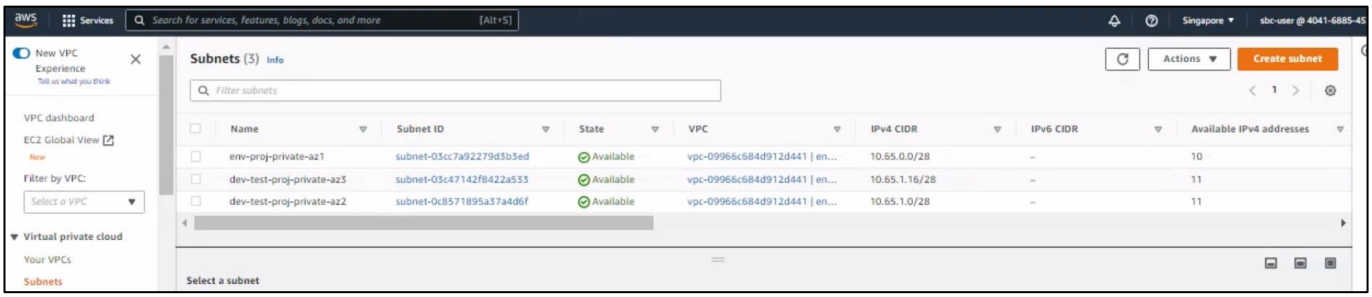
7.6 After Launching the Product, verify VPC Provision Product.



7.7 Verify that all the resources are created.



7.8 **Verify** the VPC and the newly created Subnet.



8 Appendix A

A.1 The naming convention we followed is as follows:

sbc-<product_name>-<no_of_AZ><no_of_subnet_per_AvailabilityZone>

A.2 Created new S3 bucket named "**sbc-subnet-provisioning**", keeps folders and files as follows: -

a) sbc-subnet-1az1sub

9 Document Control - Version History

AMENDMENT LOG						
Version	**Date dd-mmm-yyyy**	**Prepared By**	**Reviewed By**	**Section**	**A/M/D**	**Brief Description of change**
1.0	13-Jul-2022	Sagarika Kanikella and Satish Koilada	SBC	All	A	Initial version of adding additional CIDR and SUBNET to existing VPC