



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

Table of Contents.....	1
1 Overview.....	2
2 Deploy the portfolio in the AWS Service Catalog delegated administrator account	2
3 Share the newly created CIDR portfolio with your organization from Delegated Administrator account	4
4 Setup user access and provision a custom CIDR using AWS Service Catalog.....	6
5 Deploy the Subnet portfolio in the AWS Service Catalog delegated administrator account.....	10
6 Share the newly created Subnet portfolio with your organization from Delegated Administrator account	12
7 Setup user access and provision a custom Subnet using AWS Service Catalog	13
8 Appendix A.....	16
9 Document Control - Version History.....	17

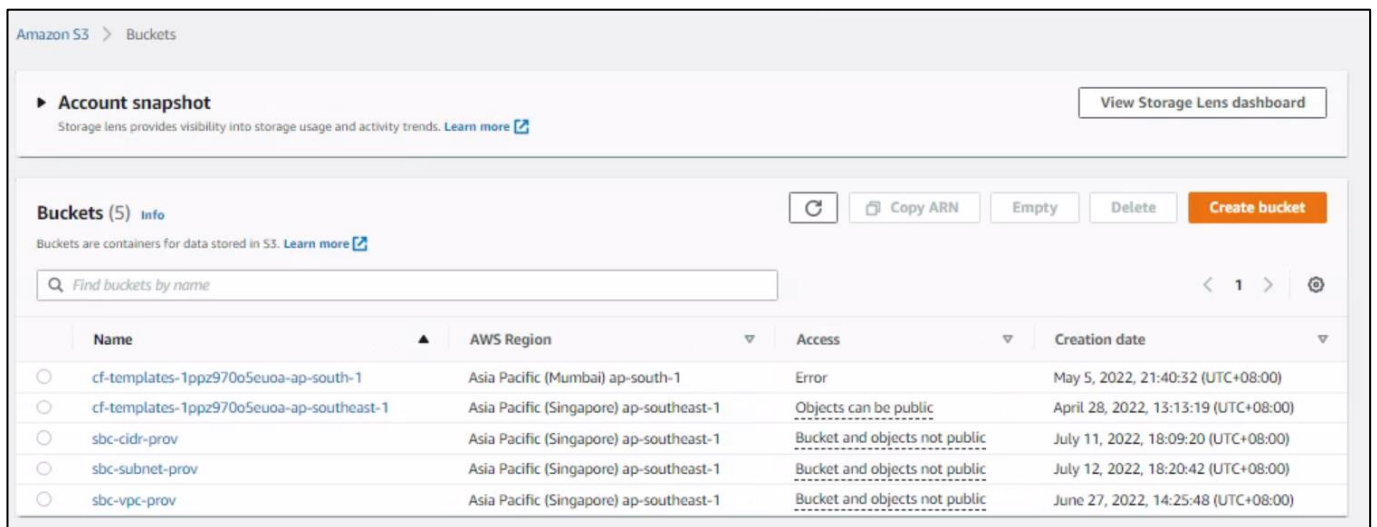
1 Overview

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)



The screenshot shows the Amazon S3 Buckets console. At the top, there's a header 'Amazon S3 > Buckets'. Below it, an 'Account snapshot' section mentions 'Storage lens provides visibility into storage usage and activity trends.' To the right is a 'View Storage Lens dashboard' button. The main section is titled 'Buckets (5) Info' and includes buttons for 'Refresh', 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. A search bar says 'Find buckets by name'. Below is a table with 5 buckets:

Name	AWS Region	Access	Creation date
cf-templates-1ppz970o5euoa-ap-south-1	Asia Pacific (Mumbai) ap-south-1	Error	May 5, 2022, 21:40:32 (UTC+08:00)
cf-templates-1ppz970o5euoa-ap-southeast-1	Asia Pacific (Singapore) ap-southeast-1	Objects can be public	April 28, 2022, 13:13:19 (UTC+08:00)
sbc-cidr-prov	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	July 11, 2022, 18:09:20 (UTC+08:00)
sbc-subnet-prov	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	July 12, 2022, 18:20:42 (UTC+08:00)
sbc-vpc-prov	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	June 27, 2022, 14:25:48 (UTC+08:00)

- 2.2 Navigate to Cloud Formation template and create a CIDR Network-Portfolio Stack and upload



the file sbc-add-cidr-to-vpc.yml

Create stack

Step 1: Specify template

Step 2: Specify stack details

Step 3: Configure stack options

Step 4: Review

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template ☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL ☒ Upload a template file

Upload a template file

Choose file

JSON or YAML formatted file

S3 URL: <https://s3-ap-southeast-1.amazonaws.com/cf-templates-1p0z970o5euoa-ap-southeast-1/20221948Ym-sbc-cidr-portfolio.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

CloudFormation > Stacks > cidr

Stacks (9)

Filter by stack name

Active View nested

subnet 2022-07-12 19:40:00 UTC+0800 CREATE_COMPLETE

cidr 2022-07-12 19:33:49 UTC+0800 CREATE_COMPLETE

prov 2022-07-01 13:37:12 UTC+0800 CREATE_COMPLETE

StackSet: usc-portfolio-launch-role-870b788e

cidr Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

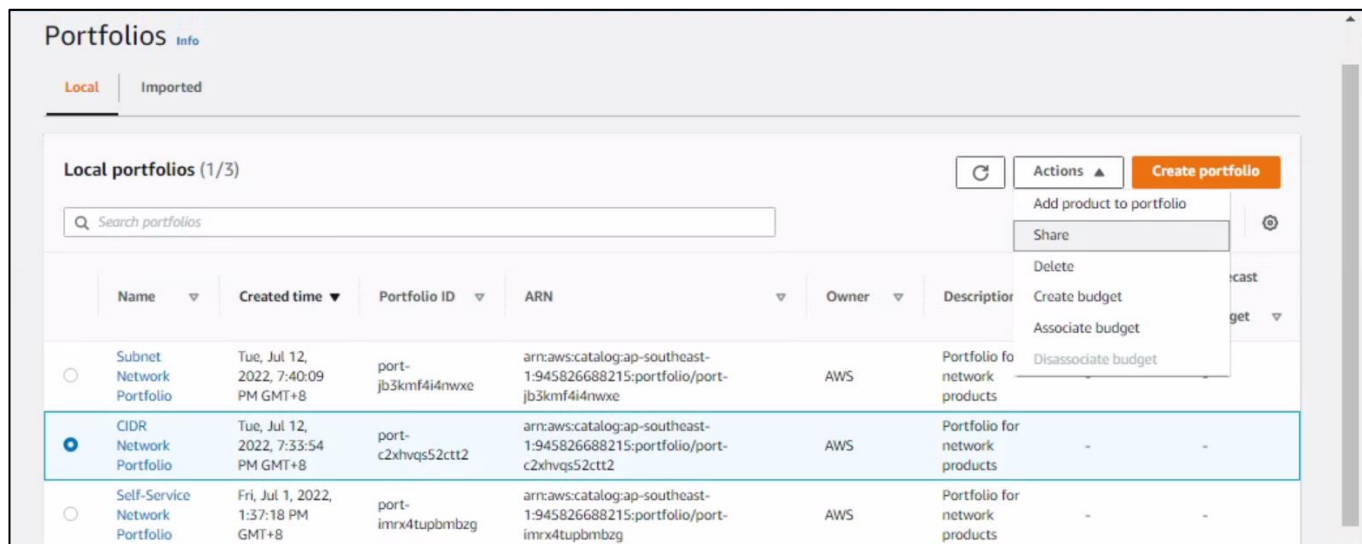
Events (11)

Search events

Timestamp	Logical ID	Status	Status reason
2022-07-12 19:34:12 UTC+0800	cidr	CREATE_COMPLETE	-
2022-07-12 19:34:10 UTC+0800	rCidrProductAssociation	CREATE_COMPLETE	-
2022-07-12 19:34:10 UTC+0800	rCidrProductAssociation	CREATE_IN_PROGRESS	Resource creation Initiated
2022-07-12 19:34:08 UTC+0800	rCidrProductAssociation	CREATE_IN_PROGRESS	-
2022-07-12 19:34:06 UTC+0800	rCidrProduct	CREATE_COMPLETE	-
2022-07-12 19:33:55 UTC+0800	rCidrProduct	CREATE_IN_PROGRESS	Resource creation Initiated

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

Service Catalog > Portfolios

Portfolios Info

Local Imported

Imported portfolios (1/3)

Search portfolios

	Name	Created time	Portfolio ID	ARN	Owner	Description	Share Type	Current vs. budget	For vs. bu
<input type="radio"/>	Self-Service Network Portfolio	Fri, Jul 1, 2022, 1:37:18 PM GMT+8	port-imrx4tupbmbzg	arn:aws:catalog:ap-southeast-1:945826688215:portfolio/port-imrx4tupbmbzg	AWS	Portfolio for network products	AWS_ORGANIZATION S	-	-
<input checked="" type="radio"/>	CIDR Network Portfolio	Tue, Jul 12, 2022, 7:33:54 PM GMT+8	port-c2xhvqs52ctt2	arn:aws:catalog:ap-southeast-1:945826688215:portfolio/port-c2xhvqs52ctt2	AWS	Portfolio for network products	AWS_ORGANIZATION S	-	-

aws service catalog

Home

- Provisioning
 - Products
 - Provisioned products
- Administration
 - Getting started library
 - Product list
 - Portfolios**
 - TagOptions library
 - Service actions
 - Preferences
- AppRegistry
 - Introduction New
 - Applications
 - Attribute groups

Portfolio details

Description
Portfolio for network products

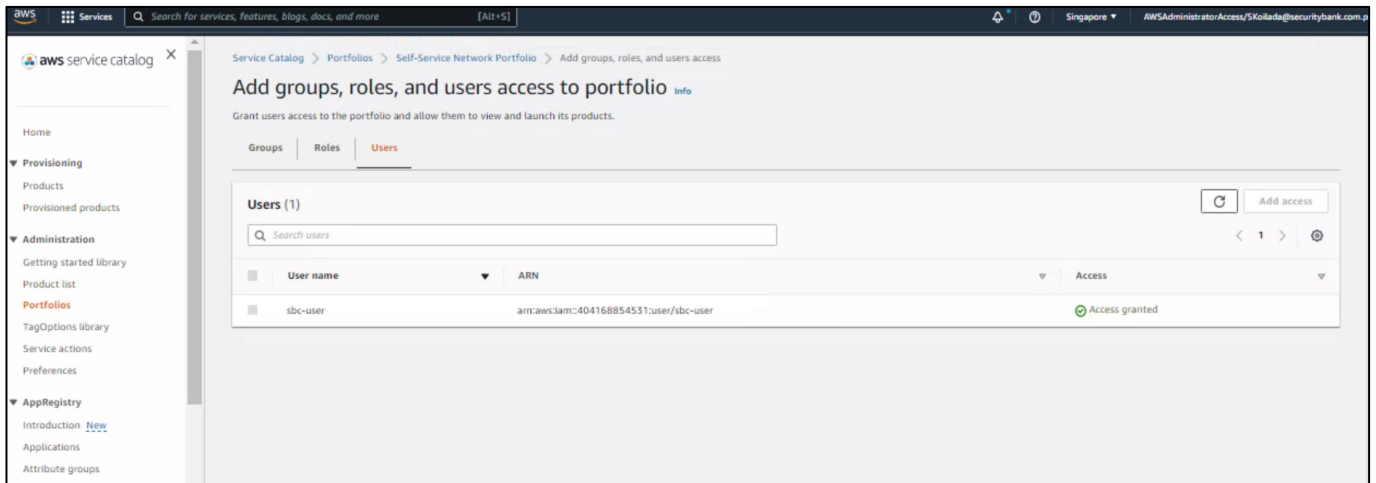
ID port-Sedyjrbmttoig	Created time Fri, May 6, 2022, 5:55:26 PM GMT+5:30	ARN arn:aws:catalog:ap-south-1:793503490104:portfolio/port-Sedyjrbmttoig
Owner AWS		

Products (0) Constraints (0) **Groups, roles, and users (1)** Share (0) TagOptions (0)

Products (0)

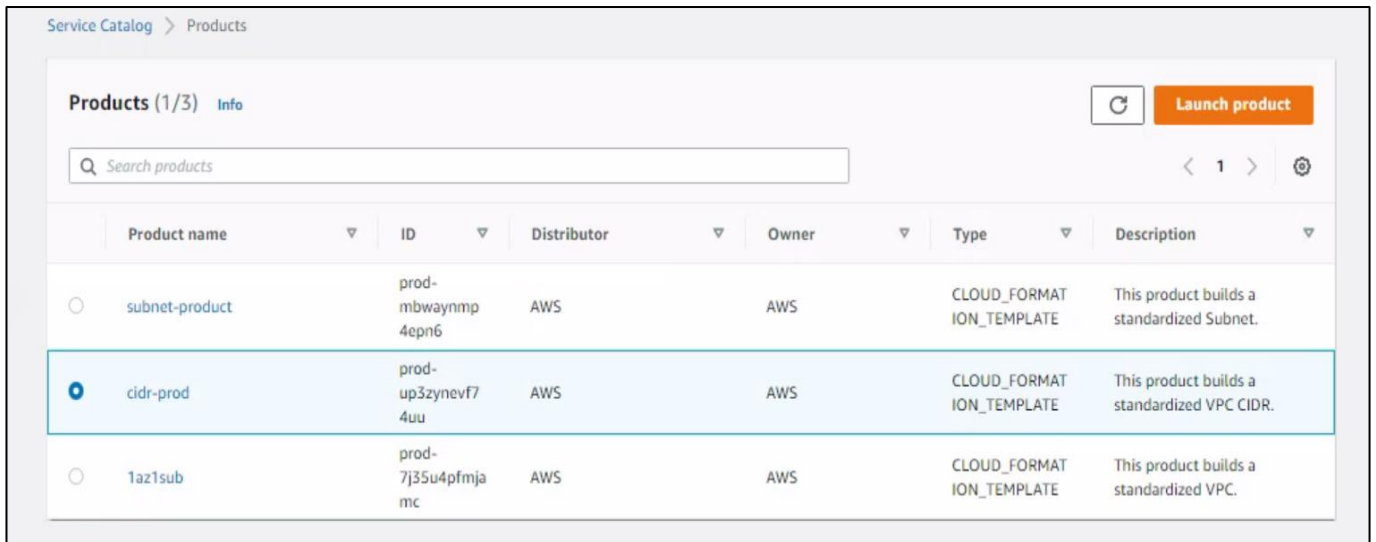
Search products

Product name	Product ID	Product type	Created time	Distributor	Provided by	Description
This portfolio doesn't contain any products.						

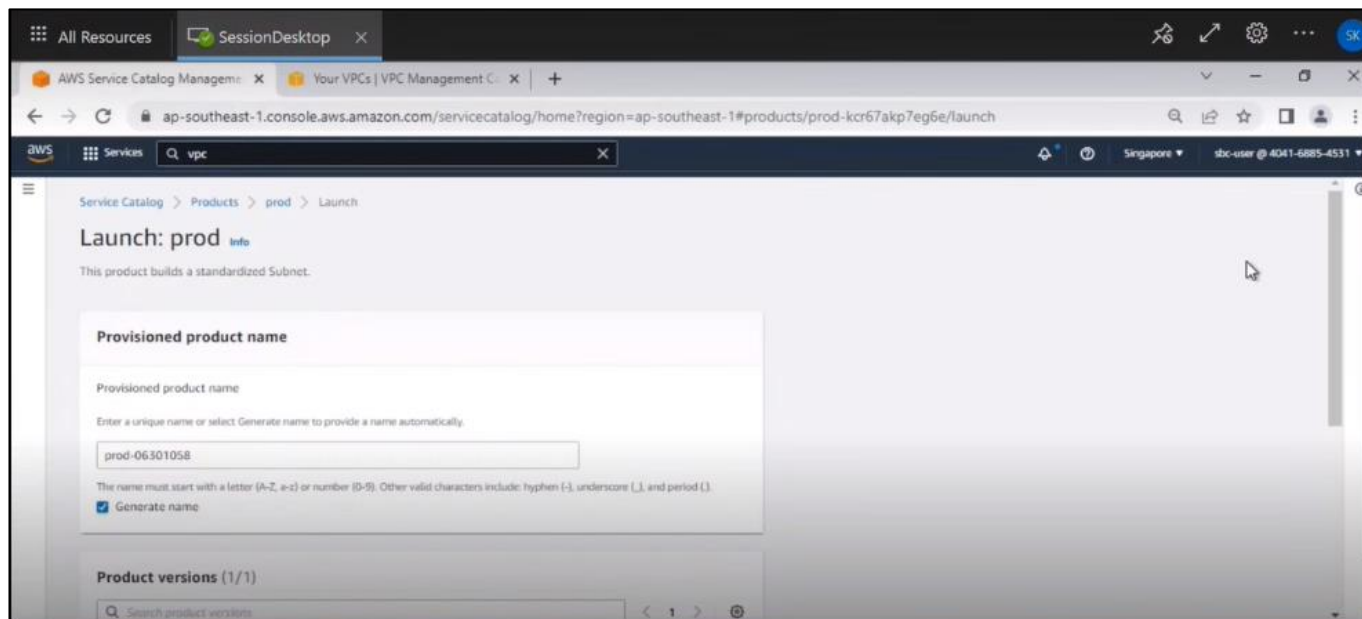


4.2 Now the access has been provided to the IAM user (IAM user which is created as Pre-requisite).

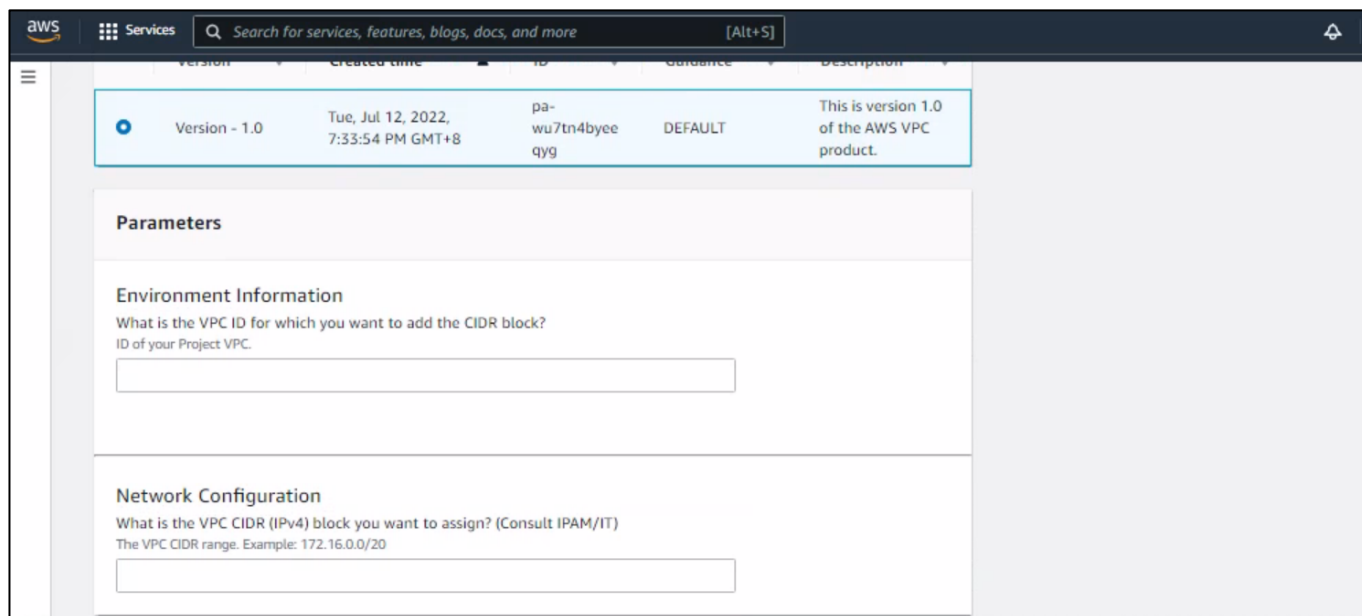
4.3 Login to the member account and Navigate to Service catalog and click on Products.



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.

Provisioned product details

Product description
This product builds a standardized VPC CIDR.

Provisioned product ID pp-qaxm22aqvwmba	Created Tue, Jul 12, 2022, 7:36:13 PM GMT+8	Status Available
Product name cidr-prod	User name sbc-user	Version name Version - 1.0
Provisioned product ARN arn:aws:servicecatalog:ap-southeast-1:404168854531:stack/cidr-prod-07121145/pp-qaxm22aqvwmba	User ARN arn:aws:iam::404168854531:user/sbc-user	

4.7 Verify that all the resources are created.

Resources (6)

Logical ID	Physical ID	Last updated	Type	Status
rPrivateRouteTable	rtb-049d77dd62170d5ee	Thu, Jun 30, 2022, 6:25:33 PM GMT+8	AWS::EC2::RouteTable	CREATE_COMPLETE
rPrivateSubnet1	subnet-0d54d6d33ac345411	Thu, Jun 30, 2022, 6:25:25 PM GMT+8	AWS::EC2::Subnet	CREATE_COMPLETE
rPrivateSubnet1RouteTableAssociation	rtbassoc-0a5afe65b020cb141	Thu, Jun 30, 2022, 6:25:38 PM GMT+8	AWS::EC2::SubnetRouteTableAssociation	CREATE_COMPLETE
rSSMPrivateRouteTable	privateroutetable	Thu, Jun 30, 2022, 6:25:37 PM GMT+8	AWS::SSM::Parameter	CREATE_COMPLETE
rSSMPrivateSubnet1	privatesubnet1	Thu, Jun 30, 2022, 6:25:28 PM GMT+8	AWS::SSM::Parameter	CREATE_COMPLETE
rSSMPrivateSubnet1RouteTableAssociation	privateroutetable1association	Thu, Jun 30, 2022, 6:25:42 PM GMT+8	AWS::SSM::Parameter	CREATE_COMPLETE

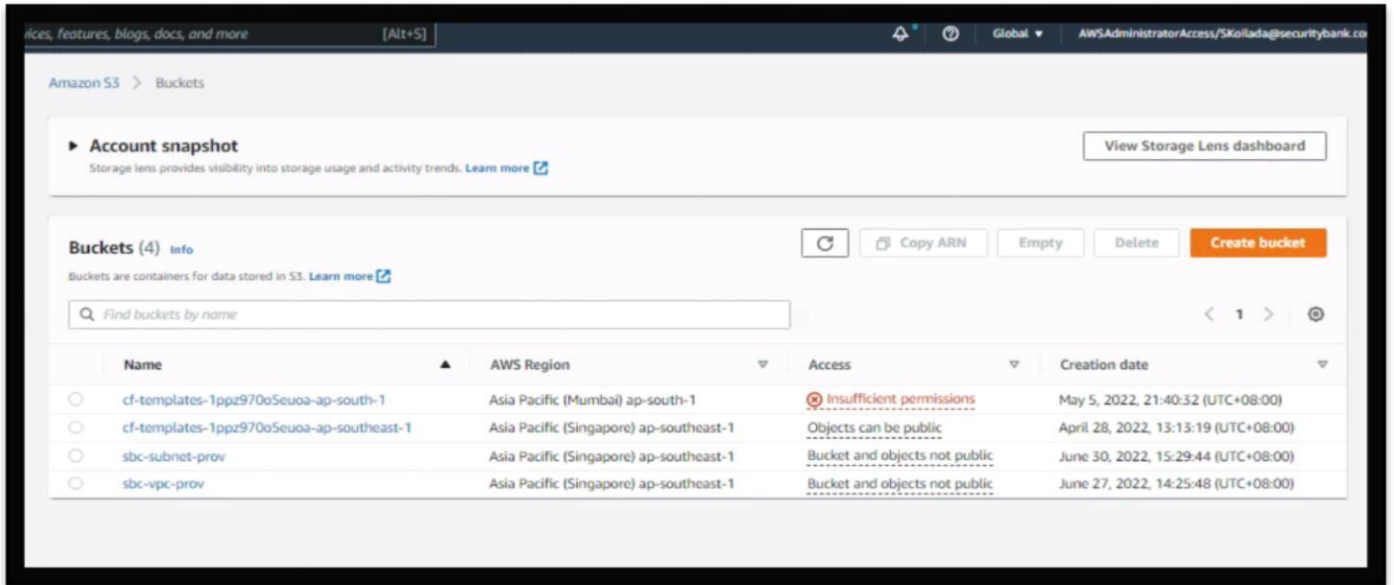
4.8 Verify the VPC and the newly created CIDR block.

Your VPCs (1/1)

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
env-proj-VPC	vpc-09966c684d912d441	Available	3 CIDRs 10.65.0.0/25 10.65.1.0/25 10.65.2.0/25		dopt-0c31ac841

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

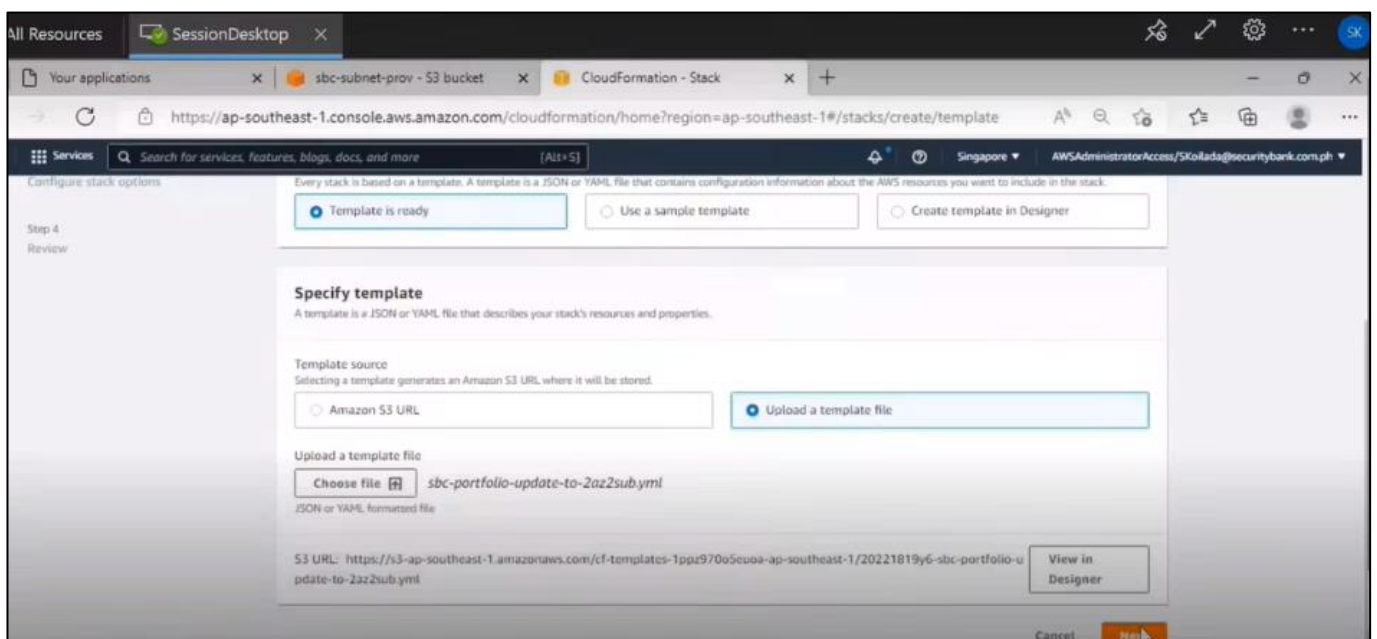
5.1 Create S3 bucket in AWS Service Catalog delegated administrator account (Refer in Appendix1.1)



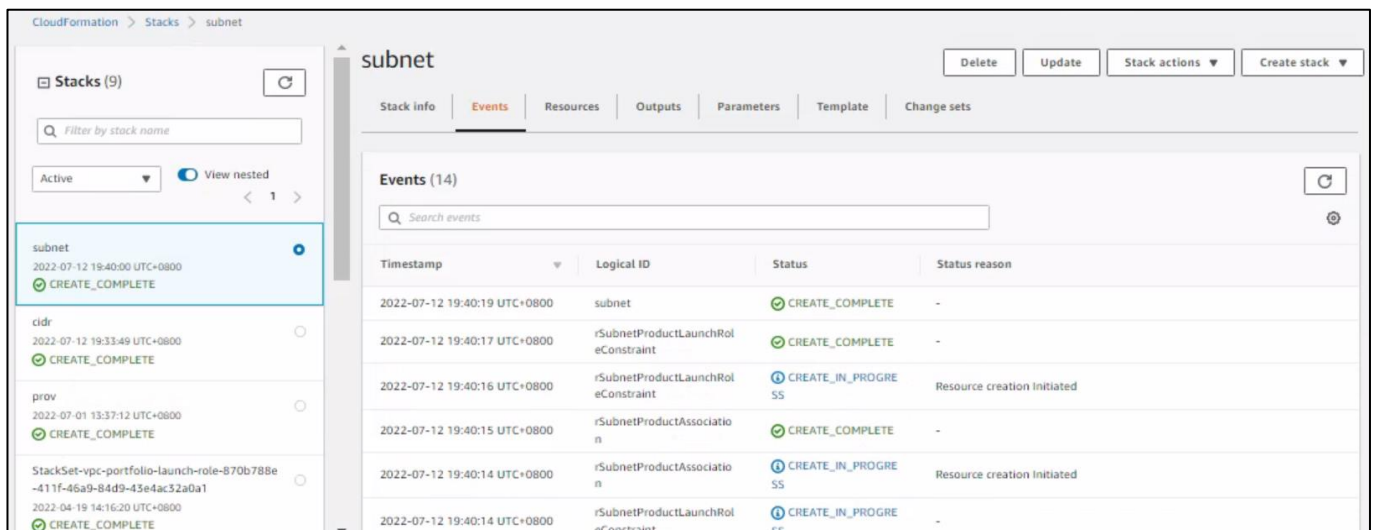
5.2 Navigate to Cloud Formation template and create a Network-Portfolio Stack and upload the file



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



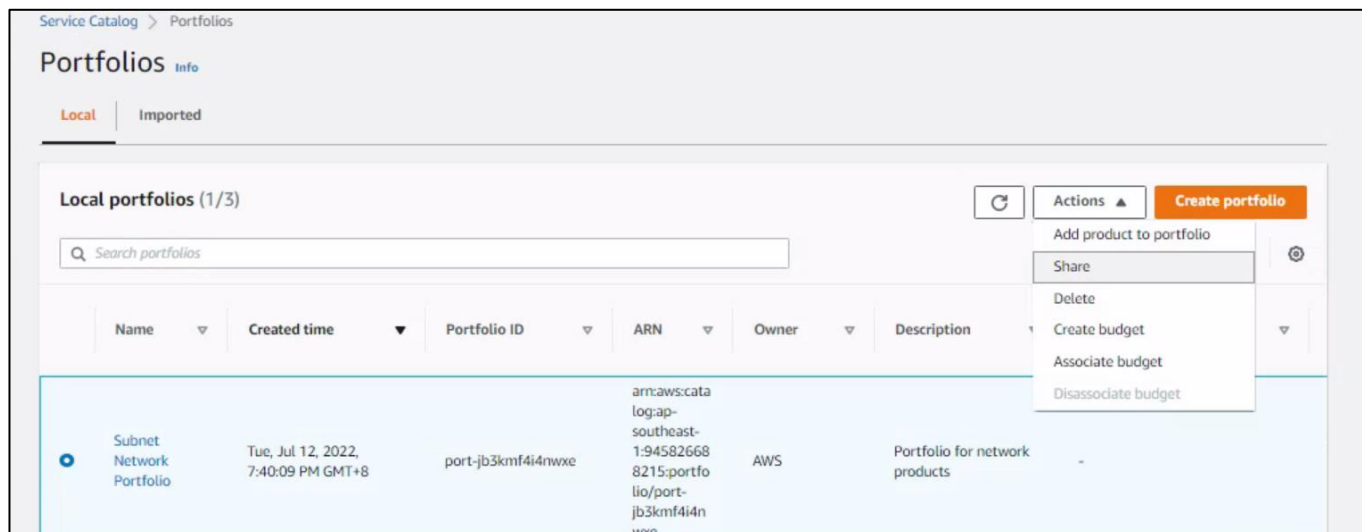
The screenshot shows the AWS CloudFormation console for a stack named 'subnet'. The 'Events' tab is selected, displaying a list of 14 events. The stack is in a 'CREATE_COMPLETE' state, as indicated by the green checkmark in the 'Status' column of the first event.

Timestamp	Logical ID	Status	Status reason
2022-07-12 19:40:19 UTC+0800	subnet	CREATE_COMPLETE	-
2022-07-12 19:40:17 UTC+0800	rSubnetProductLaunchRoleConstraint	CREATE_COMPLETE	-
2022-07-12 19:40:16 UTC+0800	rSubnetProductLaunchRoleConstraint	CREATE_IN_PROGRESS	Resource creation initiated
2022-07-12 19:40:15 UTC+0800	rSubnetProductAssociation	CREATE_COMPLETE	-
2022-07-12 19:40:14 UTC+0800	rSubnetProductAssociation	CREATE_IN_PROGRESS	Resource creation initiated
2022-07-12 19:40:14 UTC+0800	rSubnetProductLaunchRoleConstraint	CREATE_IN_PROGRESS	-

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.

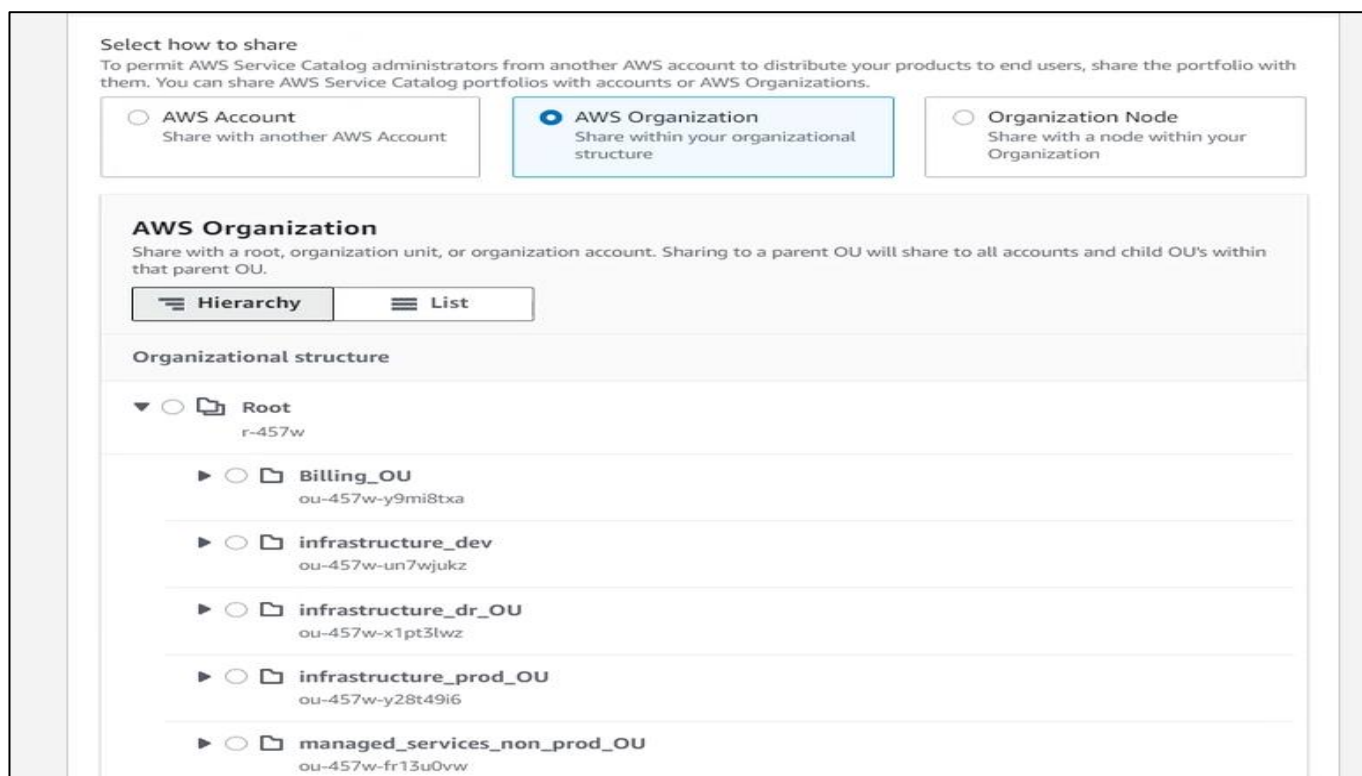
6.2 Choose the radio button next to Subnet Network Portfolio, and from Actions, choose Share.



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



Share settings

TagOption sharing

All TagOptions associated with this portfolio and its products will be shared.

☐ Enable

Cancel

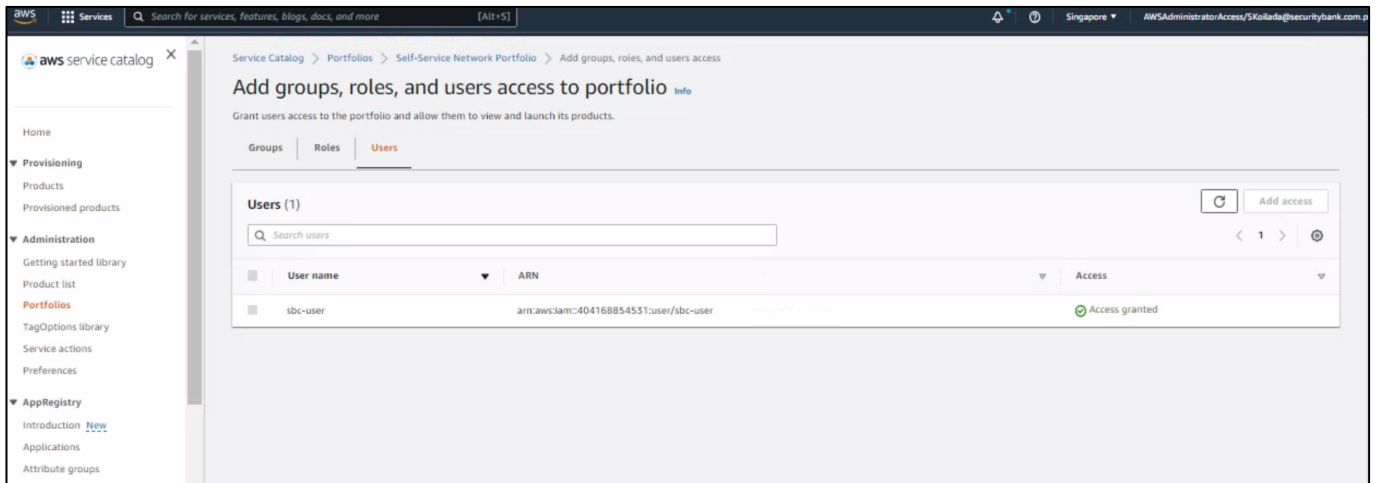
Share

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

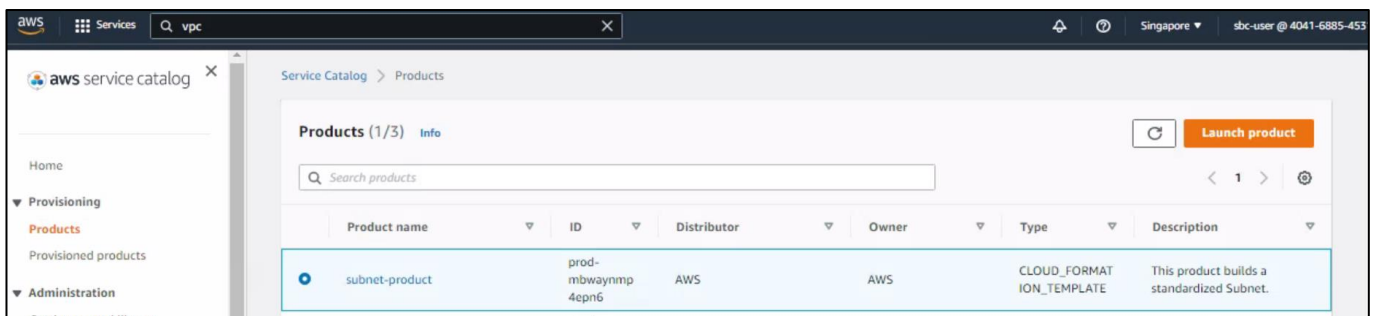
The screenshot shows the AWS Service Catalog 'Portfolios' page. The 'Imported' tab is selected, displaying a table of imported portfolios. The table has columns: Name, Created time, Portfolio ID, ARN, Owner, Description, Share Type, Current vs. budget, and For vs. budget. One portfolio is listed: 'Subnet Network Portfolio' created on Tue, Jul 12, 2022, with Portfolio ID 'port-jb3kmf4i4nwxe' and ARN 'arn:aws:catalog:ap-southeast-1:945826689215:portfolio/port-jb3kmf4i4nwxe'. The owner is 'AWS' and the share type is 'AWS_ORGANIZATION S'.

The screenshot shows the 'Portfolio details' page for the portfolio 'port-Sedyjrjrbmttojg'. The description is 'Portfolio for network products'. The ID is 'port-Sedyjrjrbmttojg', the created time is 'Fri, May 6, 2022, 5:55:26 PM GMT+5:30', and the ARN is 'arn:aws:catalog:ap-south-1:793503490104:portfolio/port-Sedyjrjrbmttojg'. The owner is 'AWS'. Below the details, there are tabs for 'Products (0)', 'Constraints (0)', 'Groups, roles, and users (1)', 'Share (0)', and 'TagOptions (0)'. The 'Groups, roles, and users (1)' tab is selected. Below the tabs, there is a section for 'Products (0)' with a search bar and a table with columns: Product name, Product ID, Product type, Created time, Distributor, Provided by, and Description. A message at the bottom states 'This portfolio doesn't contain any products.'

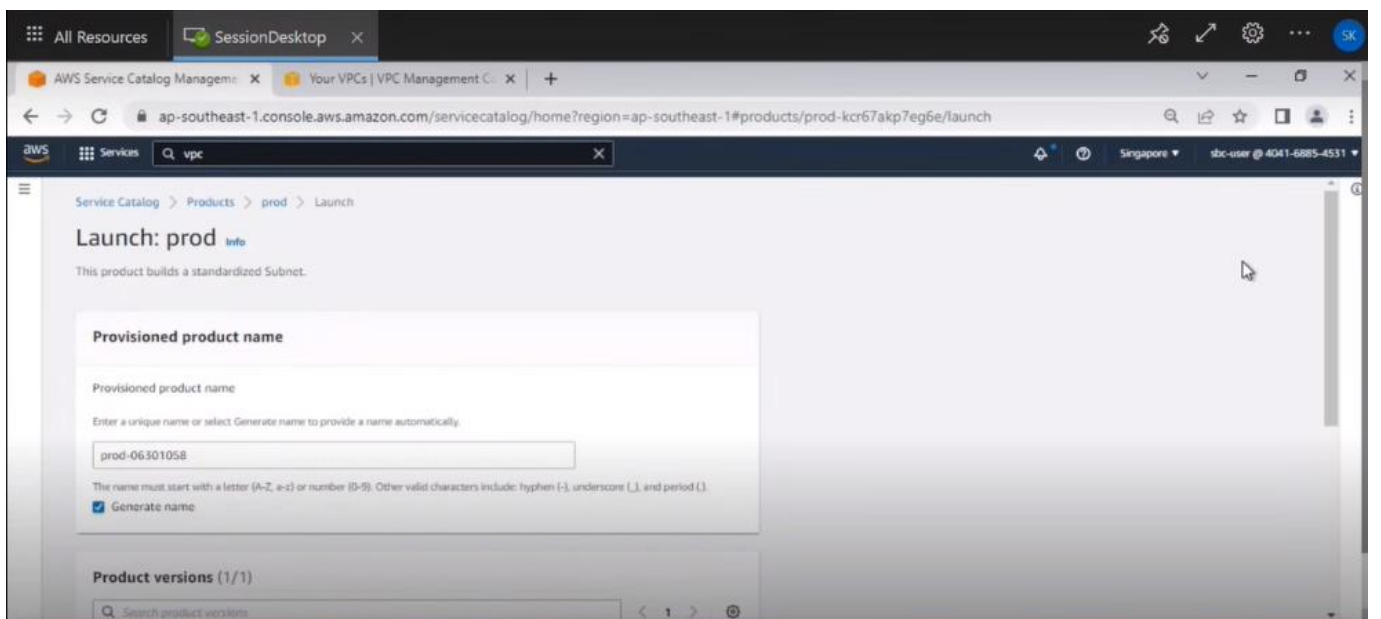


7.2 Now the access has been provided to the IAM user (IAM user which is created as Pre-requisite).

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.

The screenshot shows the AWS Service Catalog console with the 'Parameters' section for a VPC product. The left sidebar contains navigation links: Home, Provisioning, Products, Provisioned products, Administration, Getting started library, Product list, Portfolios, TagOptions library, Service actions, Preferences, AppRegistry, Introduction, Applications, and Attribute groups. The main content area is titled 'Parameters' and contains two sections:

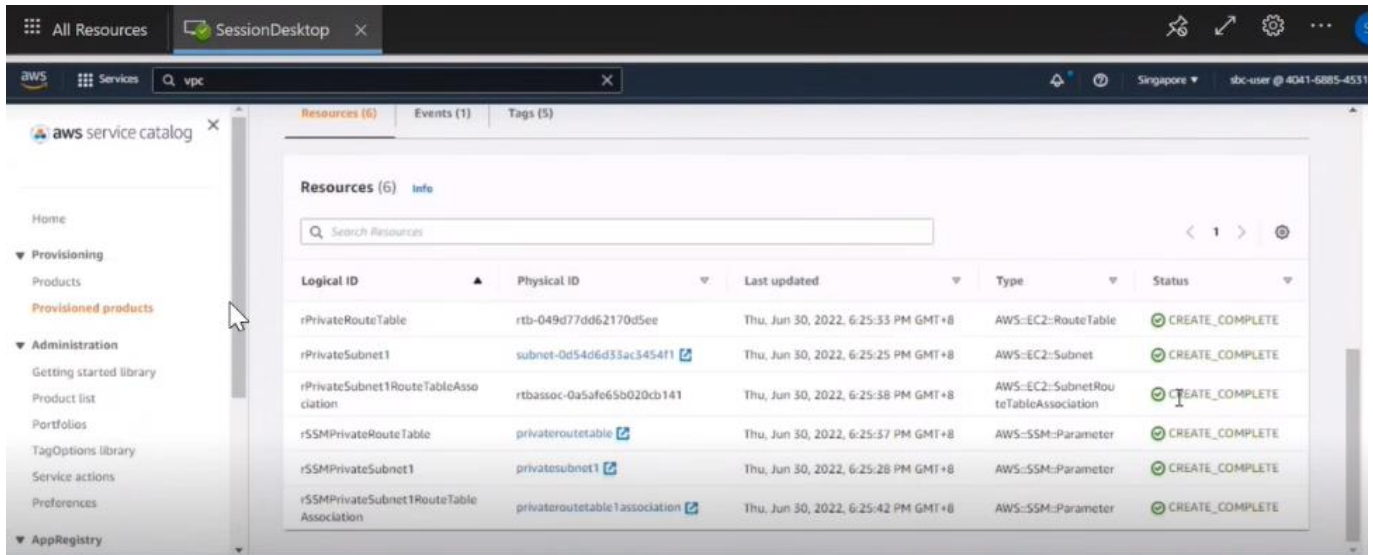
- Environment Information**
 - What is the VPC ID for which you want to add subnets?
ID of your Project VPC. (Text input field)
 - What is the Subnet name you want to assign?
Name of the Subnet. Example: <environment-name>.<project-name>.<subnet-name> (Text input field)
 - What is the availability zone you want to assign?
AvailabilityZone of the subnet. (Dropdown menu)
- Network Configuration**
 - What is the assigned VPC CIDR (IPv4) block? (Consult IPAM/IT)
The VPC CIDR range. Example: 172.16.0.0/20 (Text input field)
 - What is the assigned Subnet CIDR (IPv4) block? (Consult IPAM/IT)
The VPC CIDR range. Example: 172.16.0.0/20 (Text input field)

7.6 After Launching the Product, verify VPC Provision Product.

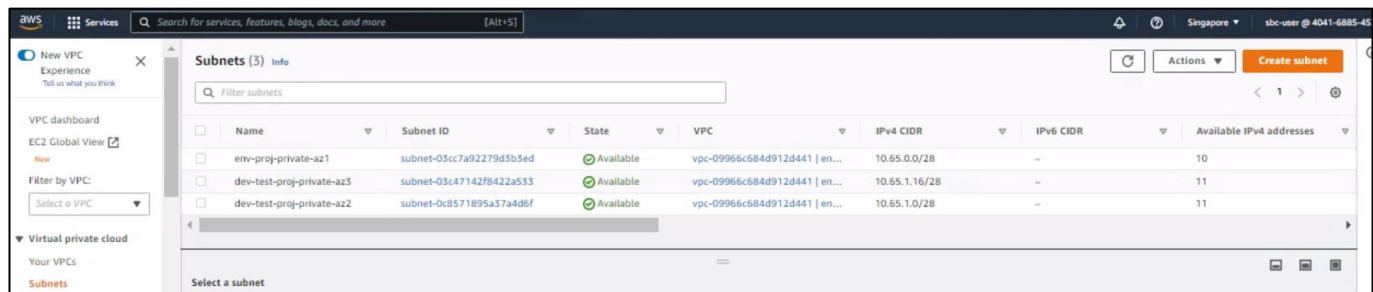
The screenshot shows the AWS Service Catalog console with the 'Provisioned product details' section for a VPC product. The left sidebar contains navigation links: Home, Provisioning, Products, Provisioned products, Administration, Getting started library, Product list, Portfolios, TagOptions library, Service actions, Preferences, AppRegistry, Introduction, Applications, and Attribute groups. The main content area is titled 'Provisioned product details' and contains the following information:

- Product description**
 - This product builds a standardized Subnet.
- Provisioned product ID**
 - pp-7vmlinraiqlkss
- Product name**
 - subnet-product
- Provisioned product ARN**
 - arn:aws:servicecatalog:ap-southeast-1:404168854531:stack/subnet-product-07121152/pp-7vmlinraiqlkss
- Created**
 - Tue, Jul 12, 2022, 7:43:48 PM GMT+8
- User name**
 - sbc-user
- User ARN**
 - arn:aws:iam::404168854531:user/sbc-user
- Status**
 - Available
- Version name**
 - Version - 1.0

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