Building VPC, S3, EC2, and RDS Products with AWS Service Catalog

In this Lab I will be creating an AWS Service Catalog (SC) Portfolio, which contain four products:
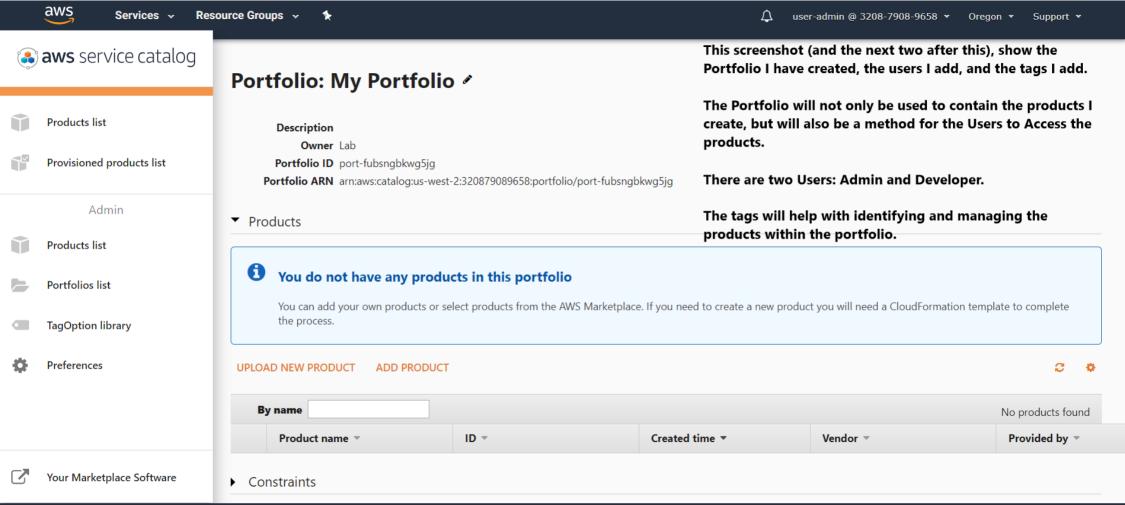
- A Virtual Private Cloud (VPC) Environment for End User development
- An Elastic Compute Cloud (EC2) Linux Instance
- A Relational Database Service (RDS) MySQL Database deployment
- Amazon Simple Storage Service (S3) – Restricted by IAM user and IP address range of VPC
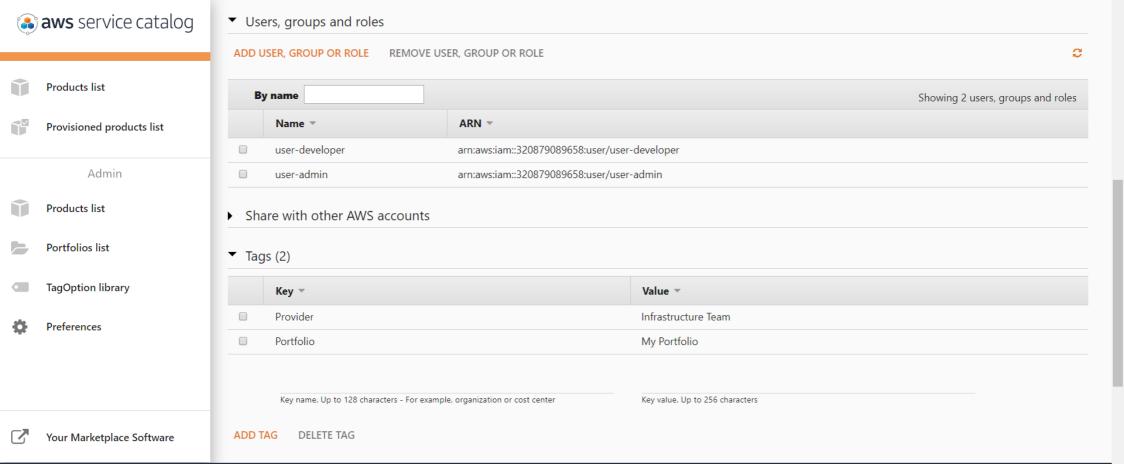
I will also be creating Template and Launch constraints for the products above, assign tags for the products and portfolios and assign AWS IAM users to use the portfolio.
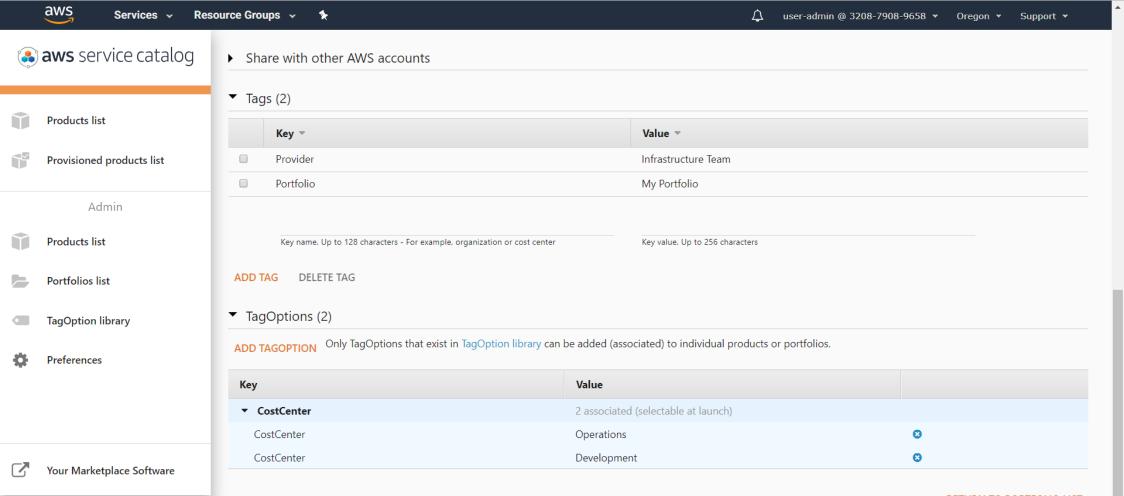
There are two IAM Users:
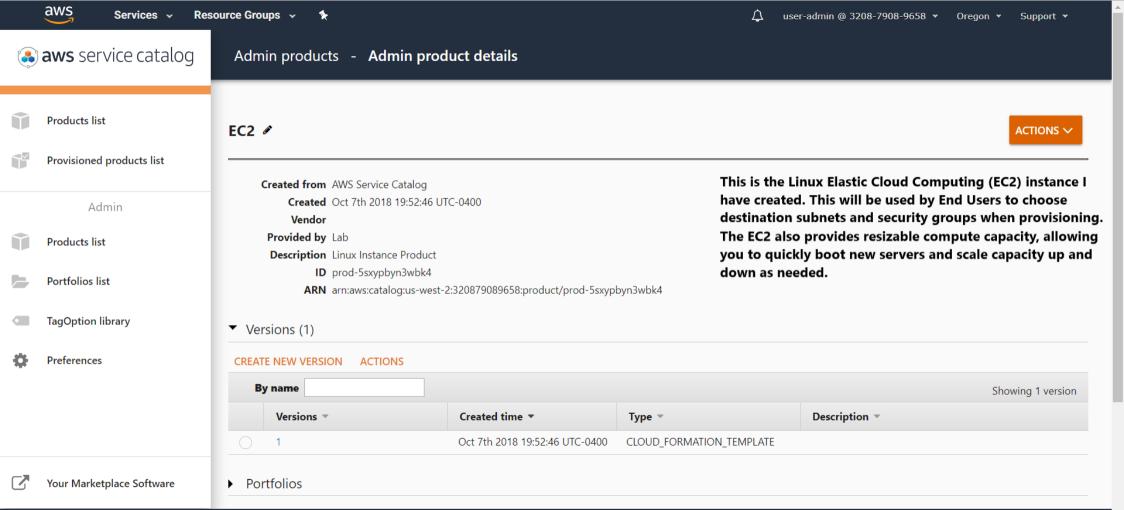
- Admin User – AWS Service Catalog Admin – Ability to create portfolios and products
- Developer User – Mimic the end-user – Ability to launch AWS SC Products.
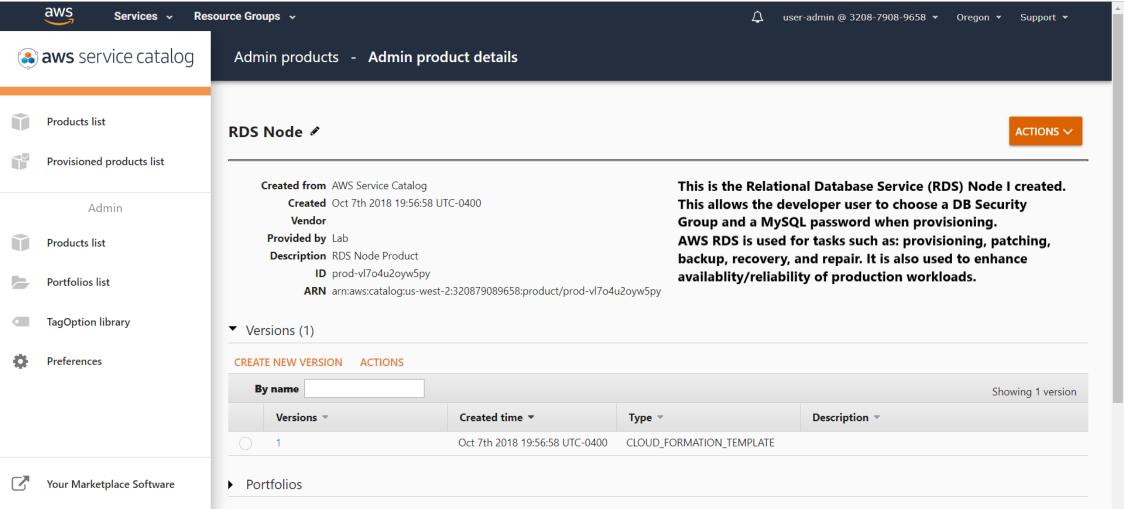
The permissions for the Users will not be given to them directly but rather they will be defined through IAM Roles. By defining Service Roles for each of the Products above, it will allow the correct users the permissions to launch those services.

Services ▾   **Resource Groups** ▾   📌

🔔   user-admin @ 3208-7908-9658 ▾   Oregon ▾   Support ▾

aws service catalog

Products list

Provisioned products list

Admin

Products list

Portfolios list

TagOption library

Preferences

⎋ Your Marketplace Software

Portfolio: My Portfolio ✏️

This screenshot (and the next two after this), show the Portfolio I have created, the users I add, and the tags I add.

The Portfolio will not only be used to contain the products I create, but will also be a method for the Users to Access the products.

There are two Users: Admin and Developer.

The tags will help with identifying and managing the products within the portfolio.

Description
Owner Lab
Portfolio ID port-fubsngbkwg5jg
Portfolio ARN arn:aws:catalog:us-west-2:320879089658:portfolio/port-fubsngbkwg5jg

▼ Products

ℹ️ **You do not have any products in this portfolio**

You can add your own products or select products from the AWS Marketplace. If you need to create a new product you will need a CloudFormation template to complete the process.

UPLOAD NEW PRODUCT   ADD PRODUCT   🔄 ⚙️

By name				
				No products found
Product name ▾	ID ▾	Created time ▾	Vendor ▾	Provided by ▾

▶ Constraints

aws service catalog

- Products list
- Provisioned products list

Admin

- Products list
- Portfolios list
- TagOption library
- Preferences

- Your Marketplace Software

▼ Users, groups and roles

ADD USER, GROUP OR ROLE   REMOVE USER, GROUP OR ROLE

By name		Showing 2 users, groups and roles

	Name ▾	ARN ▾
☐	user-developer	arn:aws:iam::320879089658:user/user-developer
☐	user-admin	arn:aws:iam::320879089658:user/user-admin

▸ Share with other AWS accounts

▼ Tags (2)

	Key ▾	Value ▾
☐	Provider	Infrastructure Team
☐	Portfolio	My Portfolio

Key name. Up to 128 characters - For example, organization or cost center   Key value. Up to 256 characters

ADD TAG   DELETE TAG

Products list

Provisioned products list

Admin

Products list

Portfolios list

TagOption library

Preferences

Your Marketplace Software

▸ Share with other AWS accounts

▾ Tags (2)

Key ▾	Value ▾
☐ Provider	Infrastructure Team
☐ Portfolio	My Portfolio

Key name. Up to 128 characters - For example, organization or cost center	Key value. Up to 256 characters

ADD TAG   DELETE TAG

▾ TagOptions (2)

ADD TAGOPTION   Only TagOptions that exist in TagOption library can be added (associated) to individual products or portfolios.

Key	Value	
▾ **CostCenter**	2 associated (selectable at launch)	
CostCenter	Operations	✕
CostCenter	Development	✕

aws service catalog

Products list	
Provisioned products list	

Admin

Products list

Portfolios list

TagOption library

Preferences

EC2 ✏️

ACTIONS ⌄

Created from	AWS Service Catalog
Created	Oct 7th 2018 19:52:46 UTC-0400
Vendor	
Provided by	Lab
Description	Linux Instance Product
ID	prod-5sxypbyn3wbk4
ARN	arn:aws:catalog:us-west-2:320879089658:product/prod-5sxypbyn3wbk4

This is the Linux Elastic Cloud Computing (EC2) instance I have created. This will be used by End Users to choose destination subnets and security groups when provisioning. The EC2 also provides resizable compute capacity, allowing you to quickly boot new servers and scale capacity up and down as needed.

▼ Versions (1)

CREATE NEW VERSION   ACTIONS

By name	[ ]			Showing 1 version

	Versions ⌄	Created time ⌄	Type ⌄	Description ⌄
○	1	Oct 7th 2018 19:52:46 UTC-0400	CLOUD_FORMATION_TEMPLATE	

▶ Portfolios

Your Marketplace Software

aws service catalog

Admin products - **Admin product details**

📦 Products list

✅ Provisioned products list

Admin

📦 Products list

📁 Portfolios list

🏷 TagOption library

⚙ Preferences

↗ Your Marketplace Software

RDS Node ✏

ACTIONS ⌄

Created from	AWS Service Catalog
Created	Oct 7th 2018 19:56:58 UTC-0400
Vendor	
Provided by	Lab
Description	RDS Node Product
ID	prod-vl7o4u2oyw5py
ARN	arn:aws:catalog:us-west-2:320879089658:product/prod-vl7o4u2oyw5py

This is the Relational Database Service (RDS) Node I created. This allows the developer user to choose a DB Security Group and a MySQL password when provisioning. AWS RDS is used for tasks such as: provisioning, patching, backup, recovery, and repair. It is also used to enhance availablity/reliability of production workloads.

▼ **Versions (1)**

CREATE NEW VERSION   ACTIONS

By name [   ]

Showing 1 version

	Versions ⌄	Created time ⌄	Type ⌄	Description ⌄
◯	1	Oct 7th 2018 19:56:58 UTC-0400	CLOUD_FORMATION_TEMPLATE	

▶ **Portfolios**

aws service catalog

- Products list
- Provisioned products list

Admin

- Products list
- Portfolios list
- TagOption library
- Preferences
- Your Marketplace Software

S3 ✎

ACTIONS ▾

Created from	AWS Service Catalog
Created	Oct 7th 2018 20:17:51 UTC-0400
Vendor	
Provided by	Lab
Description	Product that creates a S3 Bucket
ID	prod-z3vyvyqxkygom
ARN	arn:aws:catalog:us-west-2:320879089658:product/prod-z3vyvyqxkygom

**This is the S3 bucket I have created. This will be used to access specific users and IP Ranges.
AWS S3 is used to store and analyze data on wide scale. S3 provides security and compliance capabilities to store data.**

▼ Versions (1)

CREATE NEW VERSION   ACTIONS

By name			Showing 1 version

	Versions ▾	Created time ▾	Type ▾	Description ▾
○	1	Oct 7th 2018 20:17:51 UTC-0400	CLOUD_FORMATION_TEMPLATE	

▶ Portfolios

Services ▼   Resource Groups ▼   ⚑

🔔   user-admin @ 3208-7908-9658 ▼   Oregon ▼   Support ▼

aws service catalog

Products list

Provisioned products list

Admin

Products list

Portfolios list

TagOption library

Preferences

Your Marketplace Software

VPC ✏

ACTIONS ▼

Created from   AWS Service Catalog
Created   Oct 7th 2018 19:23:42 UTC-0400
Vendor
Provided by   Lab
Description   Development VPC Product
ID   prod-gk2yijcbaeqeo
ARN   arn:aws:catalog:us-west-2:320879089658:product/prod-gk2yijcbaeqeo

This is the Virtual Private Cloud (VPC) I have created. This will be the foundation for all the other products I create. The VPC allows me to launch AWS resources in my own virtual network. A VPC allows me to control IP Address Range, creating subnets, and configuring routing tables and network gateways.

▼ Versions (1)

CREATE NEW VERSION   ACTIONS

By name [   ]

Showing 1 version

	Versions ▾	Created time ▾	Type ▾	Description ▾
○	1	Oct 7th 2018 19:23:42 UTC-0400	CLOUD_FORMATION_TEMPLATE	

▶ Portfolios

▶ Tags (0)

aws service catalog

Showing 4 products

	Product name ▾	ID ▾	Created time ▾	Vendor ▾	Provided by ▾
○	S3	prod-z3vyvyqxkygom	Oct 7th 2018 20:17:51 UTC-04...		Lab
○	RDS Node	prod-vl7o4u2oyw5py	Oct 7th 2018 19:56:58 UTC-04...		Lab
○	EC2	prod-5sxypbyn3wbk4	Oct 7th 2018 19:52:46 UTC-04...		Lab
○	VPC	prod-gk2yijcbaeqeo	Oct 7th 2018 19:23:42 UTC-04...		Lab

Products list

Provisioned products list

Admin

Products list

▾ Constraints

✔ **Success**

New constraint created.

These are the Launch Constraints I have created for each of the products. The Launch Constraints are acting as a proxy for the end users, allowing them to access resources without giving special permissions to a specific user.
In this scenario, the admin only has access to create portfolios and products and read-only access but is not allowed to launch any products.

Portfolios list

TagOption library

Preferences

ADD CONSTRAINTS   EDIT CONSTRAINTS   REMOVE CONSTRAINTS

	Description ▾	Type ▾	Product ▾	Origin ▾	ID ▾
○	Launch as arn:aws:iam::32087908...	LAUNCH	VPC	320879089658	
○	Launch as arn:aws:iam::32087908...	LAUNCH	RDS Node	320879089658	
○	Launch as arn:aws:iam::32087908...	LAUNCH	EC2	320879089658	
○	Launch as arn:aws:iam::32087908...	LAUNCH	S3	320879089658	

Your Marketplace Software

aws service catalog

Provisioned products list - **Provisioned product details**

Products list

Provisioned products list

Development-VPC-10080155

ACTIONS ▾

Status Available

Product VPC

Version 1

Provided by Lab

Notice I am in a Developer Role when launching

This is showing the VPC being launched from the end user. This VPC has a Public and Private subnet with an internet gateway.

This also shows the IAM Role defined for whatever end user which allows them to dynamically create a VPC in the portfolio but not allowing them to make changes to the products within the portfolio.

▾ Events (1)

↻

Oct 7th 2018	**Status**	**Type**	**Event message**
▾ 21:07:19 UTC-0400	Succeeded	PROVISION_PRODUCT	

Record ID:rec-kkcggoizhry6a

Provisioned product ID:pp-dg3efwqflai4i

▾ Outputs:

Key	**Value**	**Description**
CloudformationStackARN	arn:aws:cloudformation:us-west-2:328268938246:stack/SC-328268938246-pp-dg3efwqflai4i/5b36bfe0-ca9	The ARN of the launched Cloudformation Stack

🔔 user-developer @ 3282-6893-... ▾   Oregon ▾   Support ▾

aws service catalog

Provisioned products list   -   **Provisioned product details**

📦 Products list

☑ Provisioned products list

Development-S3-10080146

ACTIONS ▾

Status	Available
Product	S3
Version	1
Provided by	Lab

Internal App

Notice I am in a Developer Role when launching

This is showing the S3 Product being launch by the end user. This has created an S3 Bucket that will give specific access to the developer user's Amazon Resource Name and to a specific IP range.

▾ Events (1)

🔄

Oct 7th 2018	Status	Type	Event message
▾ 21:16:25 UTC-0400	Succeeded	PROVISION_PRODUCT	

Record ID:rec-gzi7ye4sckgjq
Provisioned product ID:pp-hnru6npqbtt5g
▾ Outputs:

Key	Value	Description
CloudformationStackARN	arn:aws:cloudformation:us-west-2:328268938246:stack/SC-328268938246-pp-hnru6npqbtt5g/b36010d0-c	The ARN of the launched Cloudformation Stack

aws

aws service catalog

Provisioned products list   -   **Provisioned product details**

Products list

Provisioned products list

Development-EC2-10080151

ACTIONS ∨

Status	Under change
Product	EC2
Version	1
Provided by	Lab

Notice I am in a Developer Role when launching

This is showing the EC2 product being launched by the end user. This has created a Linux EC2 Instance that will have a specific security group and subnet.

Security Groups act as a virtual firewall. You can add rules to each Security Group that allows traffic to or from its associated instances. These rules can be modified at anytime.

▾ Events (1)

🔄

Oct 7th 2018	Status	Type	Event message
▾ 21:22:56 UTC-0400	In progress	PROVISION_PRODUCT	

Record ID:rec-ry453ql5zklvw
Provisioned product ID:pp-chmtx2yrbx2w6

Key	Value	Description
No outputs found.		

▾ Support details

aws

aws service catalog

Provisioned products list   -   **Provisioned product details**

Products list

Provisioned products list

Development-RDS-10080113

ACTIONS ▼

Status	Under change	
Product	RDS Node	
Version	1	
Provided by	Lab	

Notice I am in a Developer Role when launching

This is showing the RDS Product being launched by the end user. This will create a RDS node with a specific security group and subnet group.

▼ Events (1)

🔄

Oct 7th 2018	Status	Type	Event message
▼ 21:25:19 UTC-0400	In progress	PROVISION_PRODUCT	

Record ID:rec-4eawblyaia2za

Provisioned product ID:pp-37vznwpwdcllu

Key	Value	Description
No outputs found.		

▼ Support details

aws service catalog

Template constraint

Products list

Provisioned products list

Admin

Products list

Portfolios list

TagOption library

Preferences

Your Marketplace Software

Template constraint builder

Allows you to limit the options that are available to end users when they launch the product by narrowing the allowable values for parameters defined in the AWS CloudFormation template.

Description*   RDS-Development-Constraints

This description should summarize the constraint being enforced.

| **Rule Builder** | **Constraint Text Editor** |

Name	Rule description	
RDS-Subnet-Group-Constraint	Restricts to Private DB Subnet Group	✖
RDS-Security-Group-Constraint	Restricts by RDS Security Group	✖

Name*

Rule description

Constraint*   Use Interactive Editor ▾