Automating AWS Organizations Set-Up Using CloudFormation's

Many of the customers are using the AWS Landing Zone concept which consists of separate AWS accounts so that they can meet the different needs of their organization. For one of our customers, we have the below accounts setup using Landing Zone:

- **Master Account:** The Main Account where the AWS Organizations are created for the separate accounts. This is the login point for all the organizations.
- **Shared Services Account:** The common practices are enabled in this account. All the tools shared across multiple accounts reside here. For example, Common EC2 servers for DevOps practices such as Jenkins, SonarQube, Nexus, etc.
- **Logging Account:** This account is majorly used for gathering the logs across all the accounts. Security Account: This account acts as a master account for GuardDuty and all the findings across all the organizations are fetched here.
- **Dev/UAT/Prod Accounts:** These accounts are for applications.

Although multiple organizations have simplified the operational issues and provide isolation based on the functionality, it takes manual efforts to configure the baseline security practices. To save time and effort in creating the new account, we use "Account Vending Machine". The Account Vending Machine (AVM) is an AWS Landing Zone key component. The AVM is provided as an AWS Service Catalog product, which allows customers to create new AWS accounts pre-configured with an account security baseline. For an overview, the AVM uses the below AWS Services:

- AWS Service Catalog
- AWS Lambda
- AWS Organizations
- S3 Bucket

In this blog, we are discussing how we can create, update and delete (CUD) an AWS account using AVM. The new account will be created with the following Baseline services preconfigured in it.

- **AWS CloudTrail:** It can log, continuously monitor, and retain account activity related to actions across your AWS infrastructure
- **AWS Config:** Enables you to assess, audit, and evaluate the configurations of your AWS resources.
- **AWS Guardduty:** Threat detection service that continuously monitors for malicious activity and unauthorized behaviour to protect your AWS accounts and workloads.
- **AWS Config Rule:** Managed rules for the ideal configuration settings.

The CloudFormation templates and Lambda Script are uploaded to the below GitHub Repo.

https://github.com/awsautomation/account-vending-machine

Copy the CF templates in an S3 bucket and provide the S3 path while creating the CloudFormation stack.

Prerequisites

The CF templates and the python scripts are stored in a S3 bucket of the Master account. Below are the templates/scripts which are used in the AVM workflow:

- CloudFormation Templates:
  - 01AccountCreationLambdaSetup-cfn.yaml

To start off the AVM Infrastructure, CloudFormation stack to be created with this template which creates the below two resources:

- Service Catalog AVM Product
  - Lambda Function

- 02Accountbuilder.yml

Creates a custom resource that triggers the Lambda Function with the required parameters. This template is required while launching the Service Catalog AVM Product.

- 03Accountbaselinetemplate.yml

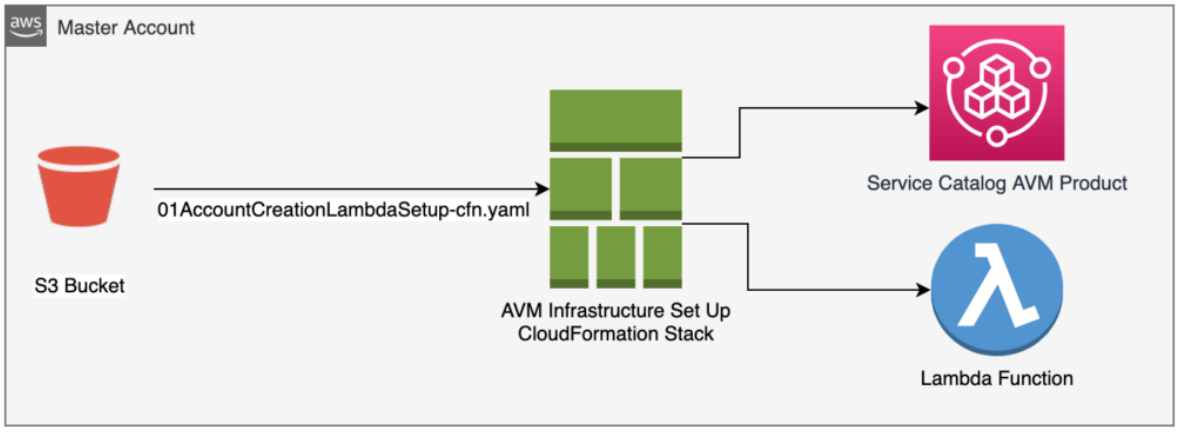
The Lambda function will create a CloudFormation stack with this baseline template in the newly created target account. It creates the predefined service catalog products such as:

- CloudTrail Service Catalog Product
  - Config Service Catalog Product
  - Guardduty Service Catalog Product

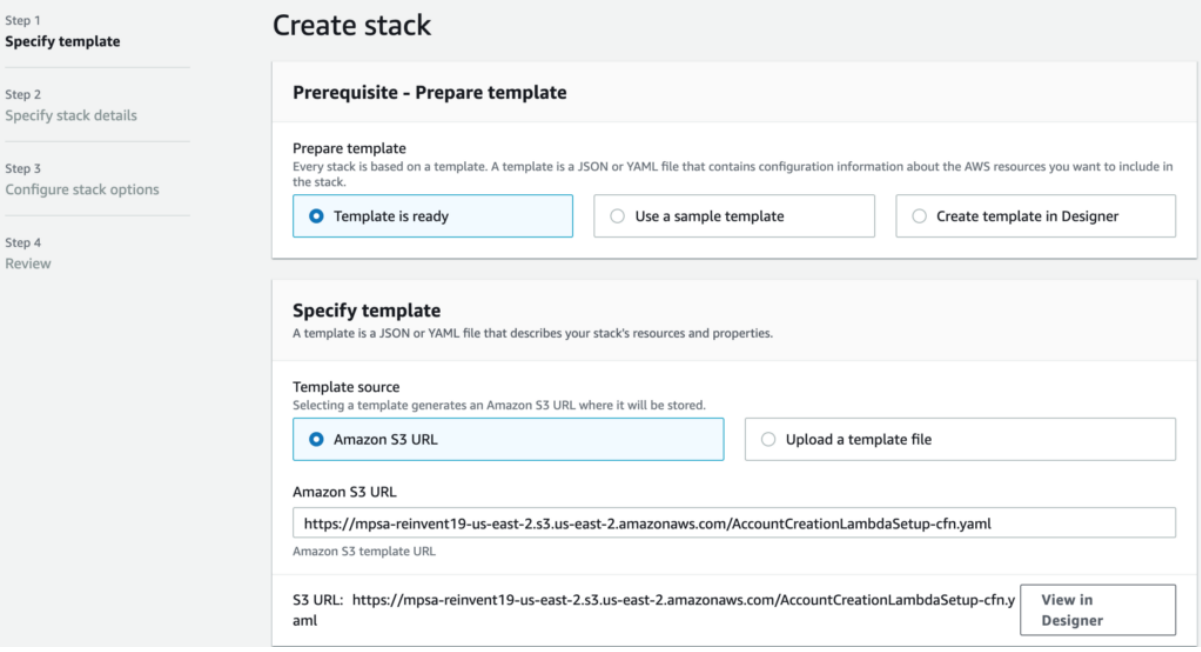
- Lambda Function

AccountCreationLambda.py: The script is required to create AWS organization in the Master account and assume the IAM Role to create Service Catalog product in the target account.

AVM Infrastructure Setup in the Master Account

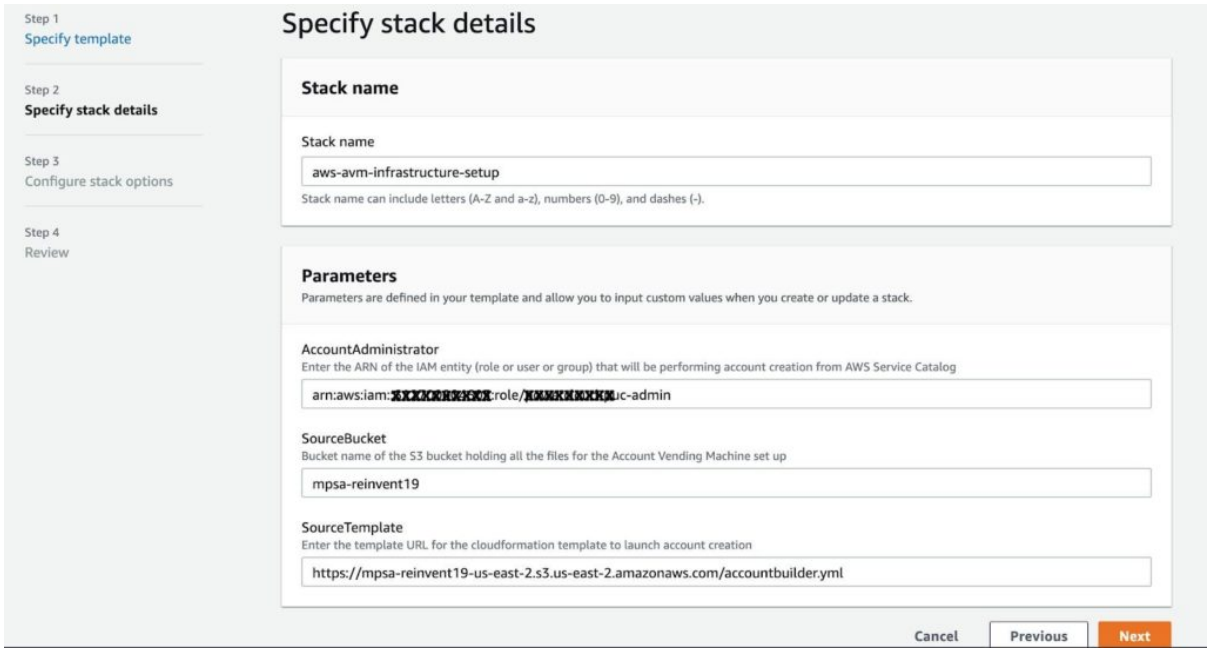


Create a CF stack using the "01AccountCreationLambdaSetup-cfn.yaml" template in Master Account.

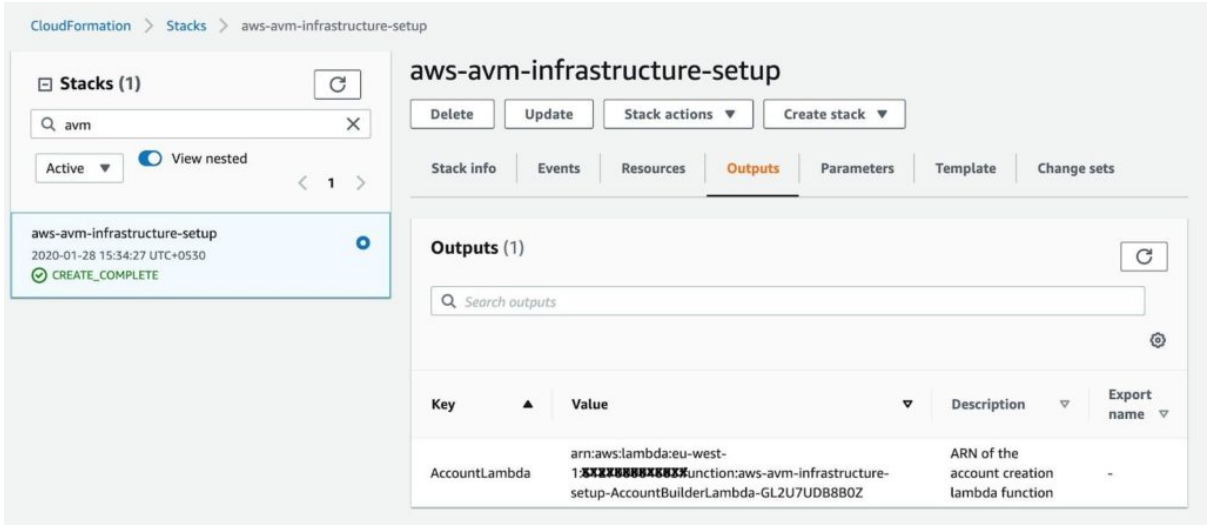


Provide the following parameters on the next page:

- **AccountAdministrator:** The ARN of IAM User/Group/Role which will be performing the account creation through Service Catalog.
- **SourceBucket:** Either keep the default value or provide the existing S3 Bucket Name in the Master account where the CF templates are uploaded.
- **SourceTemplate:** Name of the account builder template i.e. 02accountbuilder.yml.



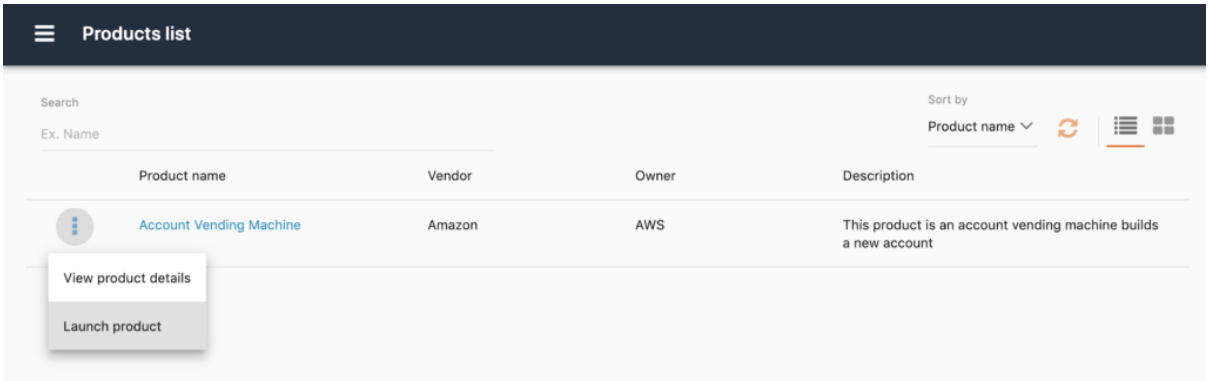
Create the Stack. Save the Lambda ARN from the outputs.



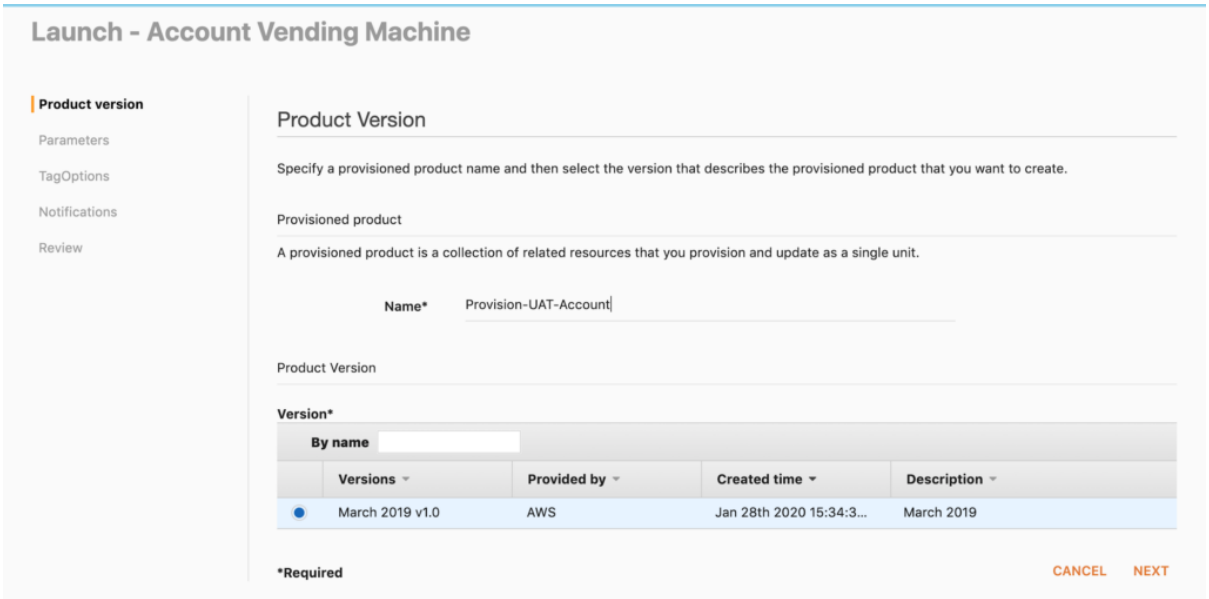
Use the same IAM ARN as provided in the CF parameters to log into the account and switch to Service Catalog Products.

Creating a New Account

Launch AVM Product to create a new account with the security baseline.

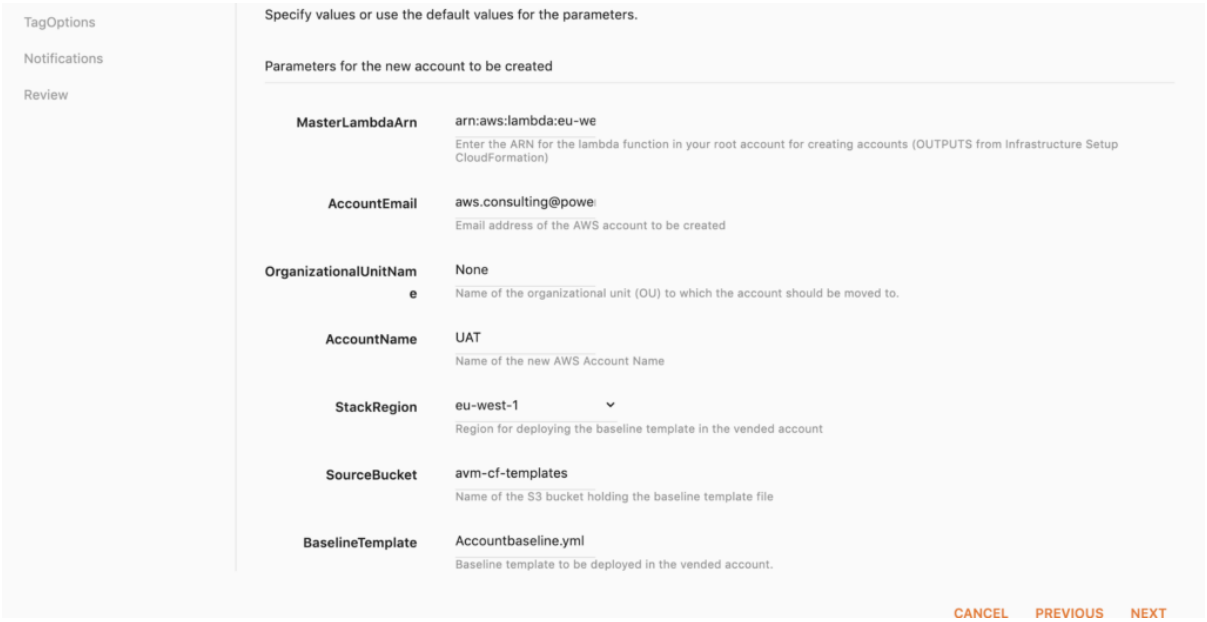


Give a relevant name for the product to be provisioned.

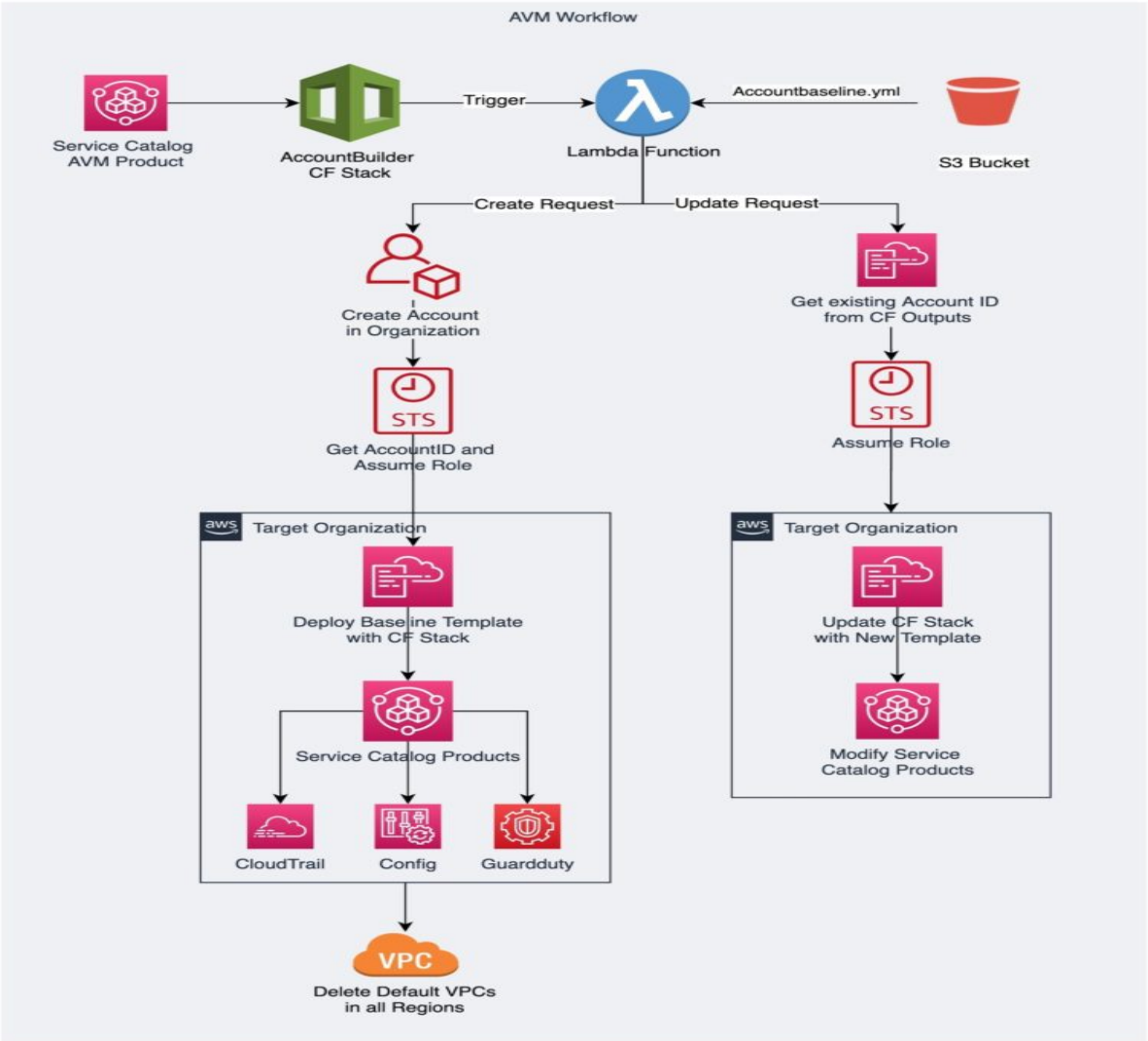


Provide the following parameters:

- **MasterLambdaArn:** ARN of the Lambda function which was saved from the CF Outputs.
- **Account Email:** Email address to be associated with the new Organization.
- **OrganizationalUnitName:** Keep default for placing the organization at the root level.
- **AccountName:** Proper Name for the New organization account.
- **StackRegion:** Region where the CF stack will be created in the target account.
- **SourceBucket:** This is the S3 bucket where you have kept your Baseline CF template. In our case, we have created a new S3 bucket in the same master account with the baseline template stored in it.
- **BaselineTemplate:** Enter the Baseline CF template name which exists in the SourceBucket i.e. 03accountbaseline.yml.

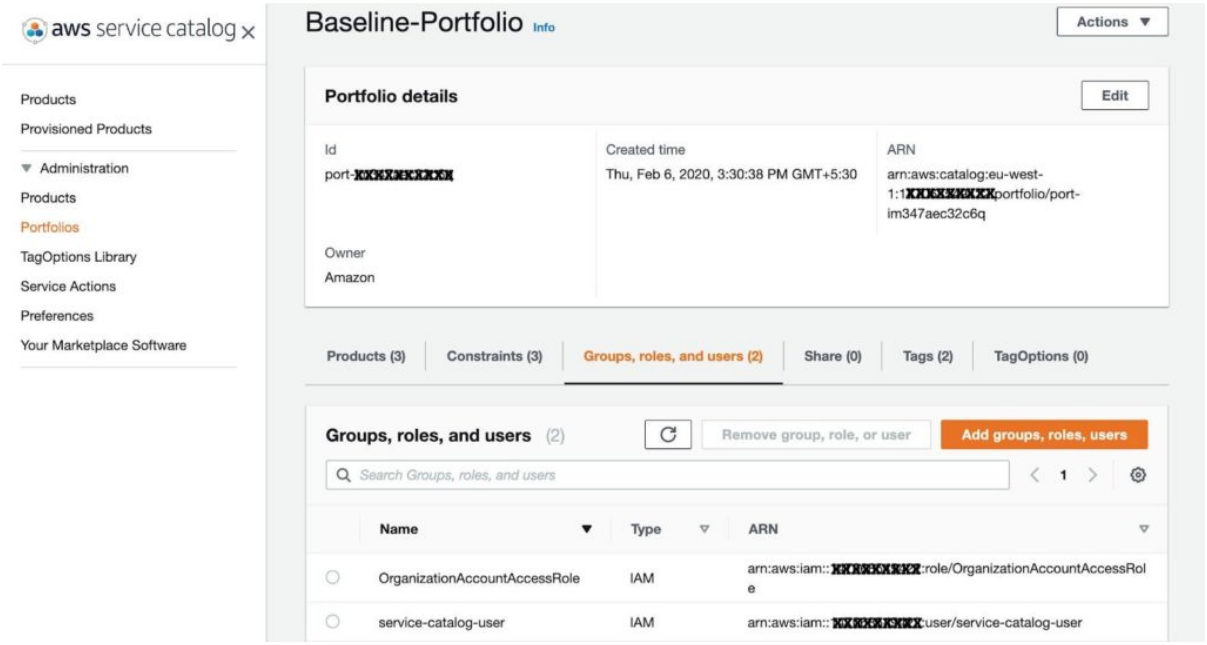


Click Next, Review and Launch the Product.



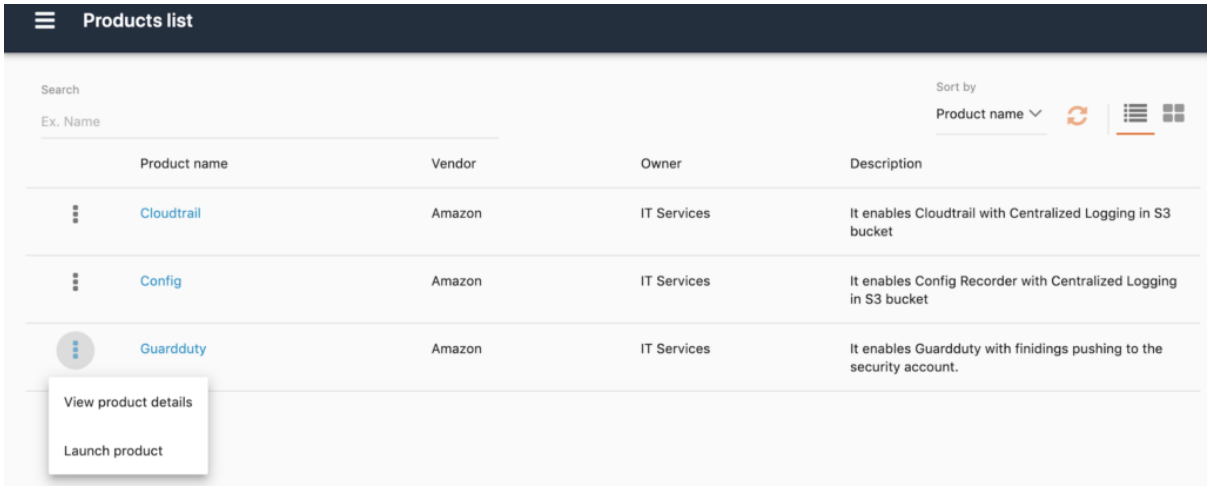
The AVM Product executes the following actions in the new target account:

- Triggers the Lambda Function which uses Organization APIs to create the new account based on the user inputs provided.
- Assumes the OrganizationAccountAccessRole in the new account and executes the below actions:
    - Creates an IAM user service-catalog-user with the default password service-catalog-2019. The password will be asked to change at the first login.
    - Creates a IAM group ServiceCatalogUserGroup with the least privilege permissions to access AWS Service Catalog. Adds the service-catalog-user to the group.
    - Creates CF stack with the **Accountbaseline.yml** template which creates the below Service Catalog Products.
        - Enable-CloudTrail
        - Enable-Config
        - Enable-Guardduty
    - Deleting the default VPCs in all AWS Regions.
    - Adds the IAM user as principal to the Service Catalog portfolio. If you login with any other IAM User/Group/Role, add the respective ARN as the principal in the Baseline Portfolio in the target account as shown below.

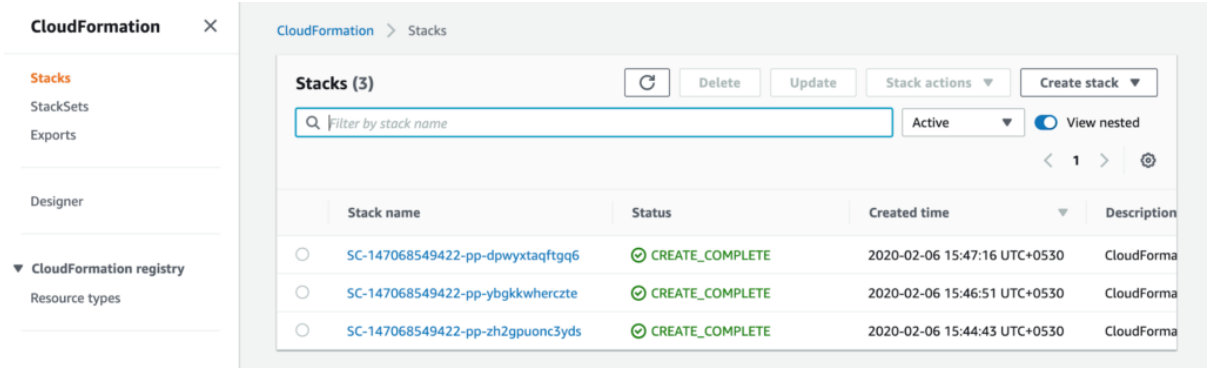


Launch Baseline Service Catalog Products in the Newly Created Account

Once the AVM product is launched, Go to Service Catalog Products in the target account.

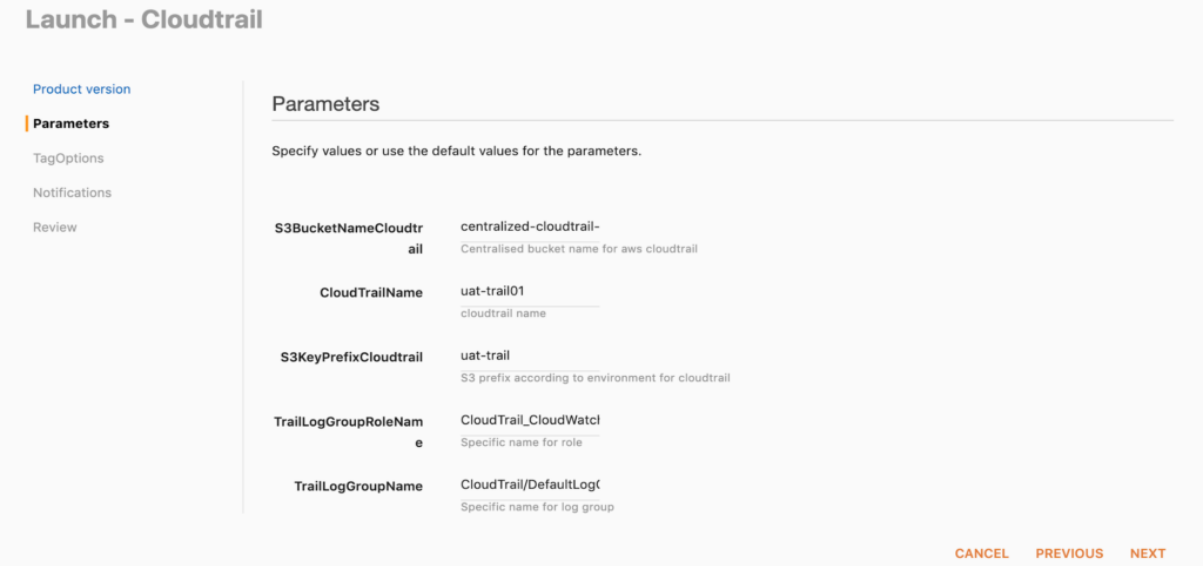


When launching each product, Service Catalog provisions the CloudFormation Stack in the backend.



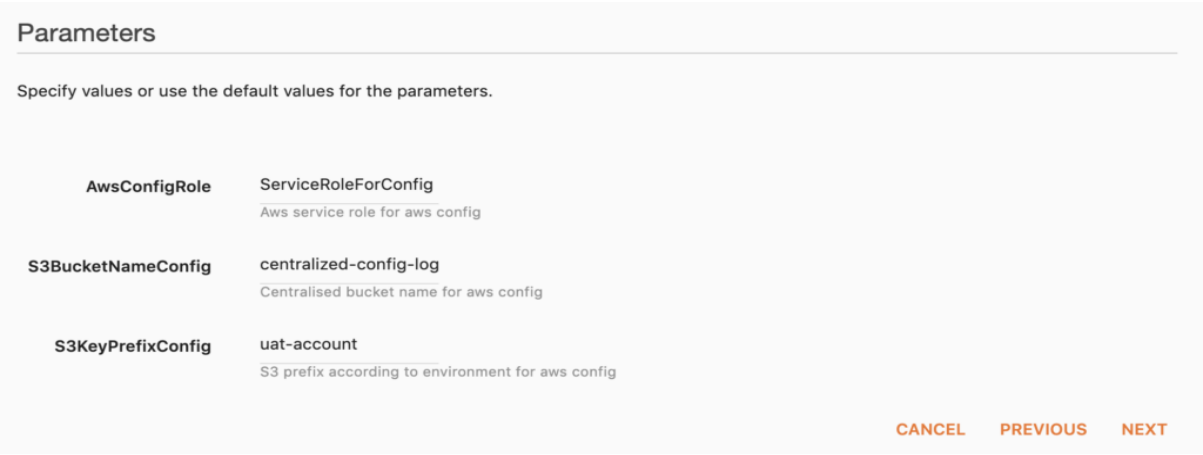
For Enabling CloudTrail in the new account, Provide the below parameters:

- **S3BucketNameCloudtrail:** Since we have implemented the Landing zone concept, we have enabled the CloudTrail logs in the centralized Logging account. Ensure the existing S3 bucket in the logging account is allowed for Cross Account CloudTrail Logs.
- **CloudTrailName:** Name of the Trail.
- S3KeyPrefixCloudtrail: Prefix in the S3 Bucket for the new account.
- **TrailLogGroupRoleName:** The CF stack creates the IAM Role which pushes the trail logs to CloudWatch as well.
- **TrailLogGroupName:** CloudWatch Log Group Name.

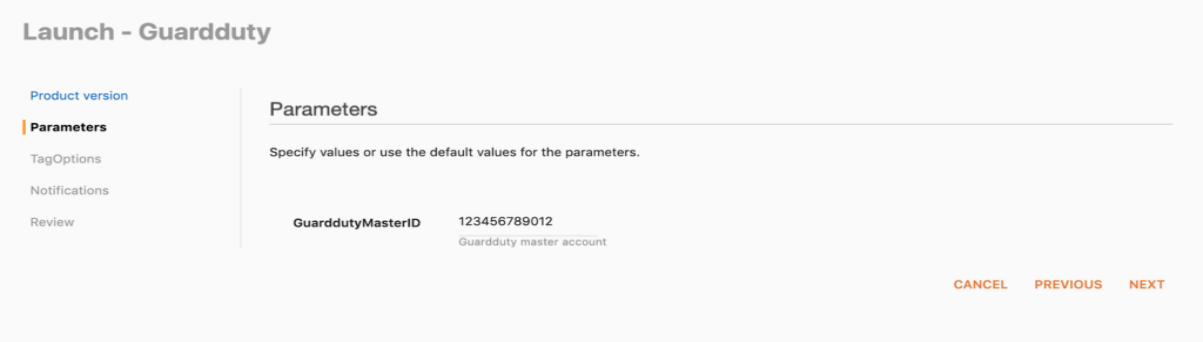


Similarly, to enable Config from the Service Catalog Product, provide the following parameters:

- **AwsConfigRole:** Name of the Config Service Role. The IAM Role will be created by the CF stack.
- **S3BucketNameConfig:** Centralized S3 bucket name for the Config Logs. We have provided the centralized bucket which exists in the Logging Account.
- **S3KeyPrefixConfig:** Prefix in the S3 bucket.



For the GuardDuty, it asks for a single parameter GuarddutyMasterID which is the AccountID of the security Account which acts as a master for the Guardduty since all the findings will be pushed to the security account.

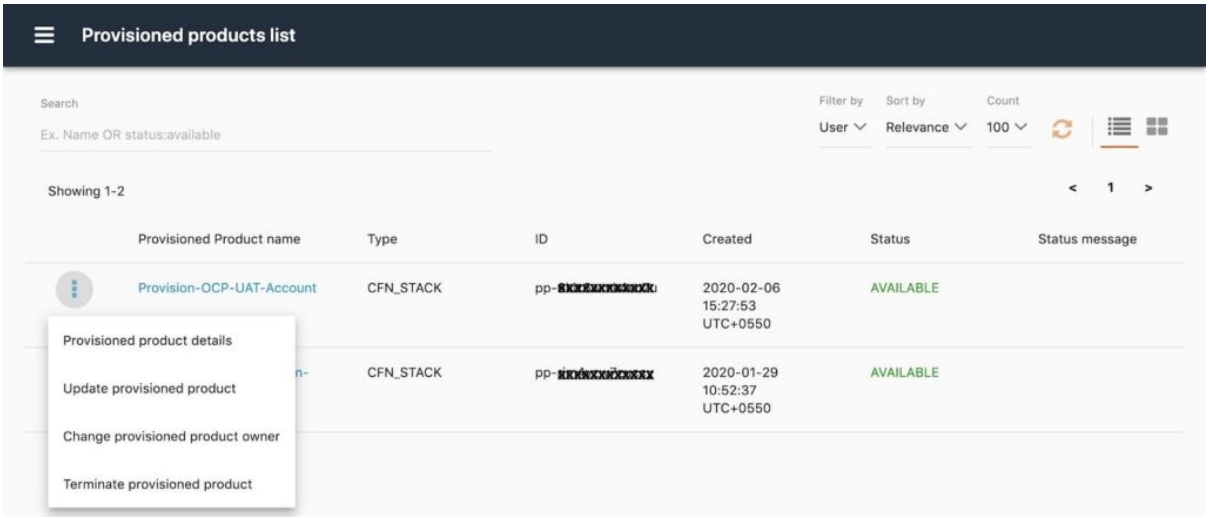


And this is how we can achieve the security practices by default with the account creation itself.

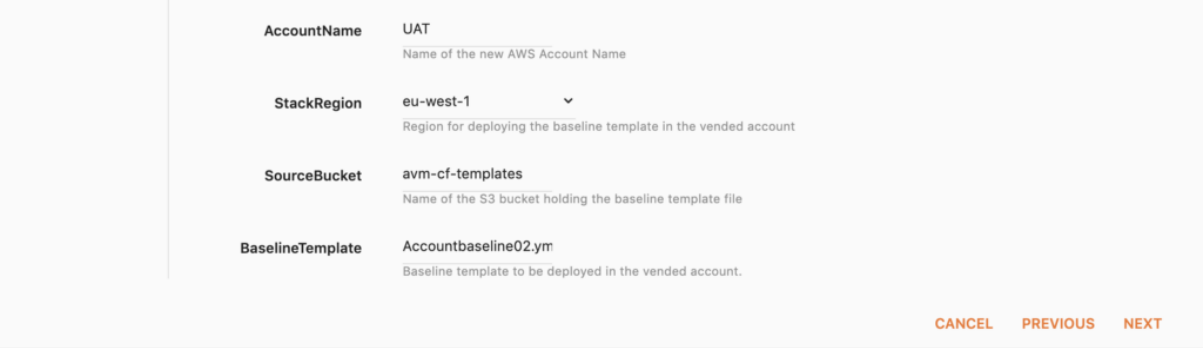
Updating an existing account

Till now we have covered the one-time setup of the baseline settings. What if you want to configure more services as the baseline settings in the existing AWS organization launched through AVM? By default, the Lambda script provided by AWS doesn't support the Update feature of the Baseline Template. We have modified the python script and uploaded it here. Update the Lambda script in the Master account with the modified script.
A valid use case can be, let's say, after enabling CloudTrail, Config, and Guardduty, now you also want to enable SecurityHub through the Baseline Setup. Below steps should be followed for the update feature to work:

- Ensure the Lambda function has the update functionality as specified in the script.
- Update the AccountBaseline template and add the Service Catalog Product for SecurityHub in it. Ensure not to delete the existing resources. Upload the updated Baseline template, e.g AccountBaseline02.yml in the S3 bucket.
- Go to the Provisioned Products List in the Service Catalog in the Master account.



- Click Update provisioned product and provide the updated Baseline template name in the BaselineTemplate parameter.



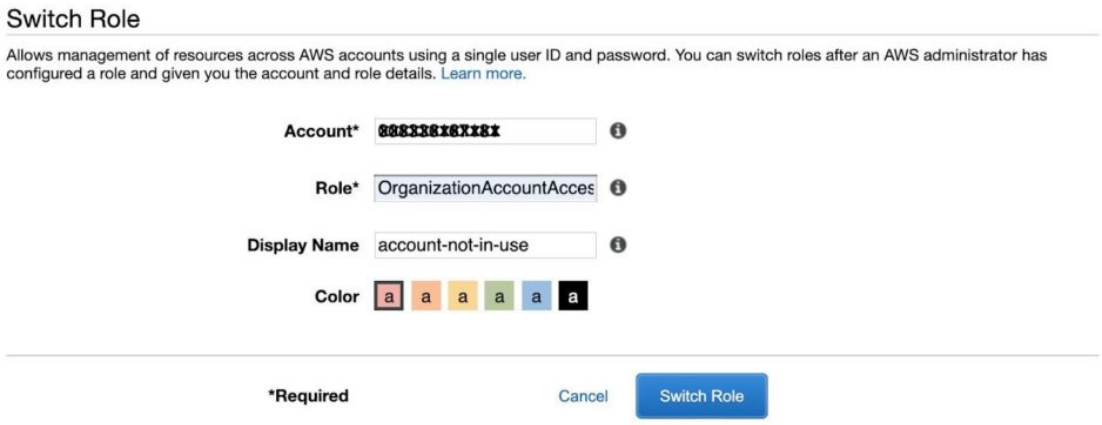
Click Next and update the product. It triggers the Lambda Script and updates the existing CloudFormation Stack in the Target account to add one more Service Catalog product.

Deleting an account

The deletion of an account includes manual efforts. To leave organisation, the account must be updated with valid billing information. Ensure you have a valid Email address for the account.

Steps to follow for account deletion:

- Switch to the account which you want to delete using the AccountID and RoleOrganizationAccountAccessRole.



- Update the Billing information.
- Switch to the AWS Organizations. Click on “Leave organisation”.