



# SSIP-MSK PRODUCT ONBOARDING

SitadConsulting  
SSIP@sitadconsulting.com

SITADCONSULTING

0

## Table of Contents

<b>1.0 Introduction .....</b>	<b>1</b>
Prerequisites .....	2
<b>2.0 Software Bill of Material .....</b>	<b>3</b>
2.1 Amazon MSK.....	3
2.2 Amazon Managed Grafana.....	3
2.3 AWS Private Certificate Authority .....	3
2.4 AWS IAM Identity Center .....	3
2.5 Amazon EC2 .....	4
<b>3.0 Product Internal IAM resources .....</b>	<b>5</b>
<b>4.0 Product Personas .....</b>	<b>6</b>
4.0.1 Subscribing to product and launching CloudFormation template. ....	6
4.0.2 Adding product to Service Catalog Portfolio .....	15
4.0.3 Sharing the product .....	15
4.0.4 Launching the product. ....	16
<b>5.0 Post Provisioning tasks .....</b>	<b>22</b>
<b>Appendix A Resource Links.....</b>	<b>37</b>
<b>Appendix B Customer Managed Policy .....</b>	<b>38</b>
<b>Appendix C Service Availability Regions .....</b>	<b>41</b>

## 1.0 Introduction

This document provides description of AWS services used by our product – **SSIP-MSK**, and also outlines the required steps for onboarding unto the product. SSIP-MSK is an acronym for “Self-Service Infrastructure Provisioning for Amazon Managed Streaming for Apache Kafka”. This product will provision a secure by default, highly available MSK Cluster with the following features enabled out of the box:

1. Authentication & Authorization
  - MTLs
  - IAM
2. Data Encryption
  - In transit and at rest
3. Open Monitoring, Observability and Logging
  - Prometheus (JMX, Node and Kafka Metrics)
  - LinkedIn CruiseControl
  - Amazon Managed Grafana
  - Amazon CloudWatch
4. An EC2 instance configured with required tools for cluster interaction
5. Effective resource tagging

***We are using both Open Source Terraform and AWS service Catalog as the core element of this product. As part of our responsibility to ensure compliance and fairness in the use of Terraform Open Source in a commercial product, we will require proof that you have the appropriate license in place in order to use our product. In addition, the following products which we have incorporated as part of this product require license to access full functionality, these are; LinkedIn CruiseControl and Amazon Managed Grafana. Also, note that you are responsible for the running cost of AWS Services that would be provisioned as part of deploying this product. This cost is separate from your AWS Marketplace transaction charges.***

***\*Please note that all provisioned resources will be tagged with metadata supplied by customer during product launch for easy identification.***

#### Prerequisites

1. Ensure that AWS Organization has been enabled and a Member Account that will host the **SSIP-MSK** product has been designated. Please refer - [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_org\\_create.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_org_create.html)  
[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_tutorials\\_basic.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_tutorials_basic.html)
2. Ensure that IAM Identity Centre has been enabled (required for single sign-on experience into Amazon Managed Grafana Console). Please refer - <https://docs.aws.amazon.com/singlesignon/latest/userguide/get-set-up-for-idc.html>
3. You have a mobile authenticator app installed on a mobile device (required to provide authentication code for single sign-on experience to Amazon Managed Grafana)
4. Ensure that no internal network access policy blocks internet access via VPC Internet Gateways (internet access is required to install MSK Cluster interaction tools)

## 2.0 Software Bill of Material

### 2.1 Amazon MSK

The product will provision a secure by default highly available Amazon MSK cluster with support for the following:

1. private broker nodes spread across three availability zones
2. Kafka versions – 3.5.1 – 3.7.x.kraft Kraft Mode
3. MTLS and IAM authentication with certificate issued by AWS Private CA
4. Encryption in transit and at rest enabled through AWS KMS and AWS Private CA respectively.
5. Broker logging via CloudWatch logs
6. Open monitoring through Prometheus JMX and Node exporter

### 2.2 Amazon Managed Grafana

The product will provision a secure by default highly available Grafana workspace with support for the following:

1. VPC based connectivity to data sources via private-link. The data sources in use include; Prometheus (available on provisioned EC2 instance), CloudWatch logs and metrics
2. Public and private access to Grafana workspace enabled via EC2 prefix-list and private-link respectively.
3. Grafana version 10.4
4. Single sign-on authentication via AWS IAM Identity Center

### 2.3 AWS Private Certificate Authority

The product will provision a private certificate (CA) authority. The ARN of CA certificate generated by the PCA is used to enable MTLS support for Amazon MSK.

### 2.4 AWS IAM Identity Center

The product will provision a group, user and permission set for use by Grafana for single sign-on authentication into Grafana console, managing Grafana workspace and Identity Center users.

<i>S/N</i>	<i>Group Display Name</i>	<i>User Name</i>
1	GrafanaAdmins	grafanaAdmin

## 2.5 Amazon EC2

The product will provision an EC2 instance configured with console access in addition to remote access via SSH. Links to all the tooling built together with the provisioned instance will be provided in [Appendix A](#). The provisioned instance is configured with the following:

1. Linux users – **kafka, kafkadev, prometheus and cruisecontrol**. These users are allowed to switch users via sudo without password. We recommend that each user should have a password set and the configured sudo access reviewed to reflect company standard as required.
2. Client.properties and producer.properties files – populated with configuration to support both IAM and TLS authentication (all files located in kafka conf path - /etc/kafka)
3. Apache Kafka – installed into kafka\_home\_dir (/opt/apps/kafka)
4. IAM-Auth jar library – aws-msk-iam-auth-2.1.1-all.jar added to Apache kafka lib path
5. Client Auth tool for MTLS – cloned and built (AuthMSK-1.0-SNAPSHOT.jar)
6. Prometheus instance – configured to retrieve both JMX and Node Metrics from MSK Cluster. These metrics are then polled by Grafana for visualization once the Prometheus data source has been setup in Grafana.
7. LinkedIn CruiseControl – cloned, built and configured including access to webui.
8. Both console and SSH access are enabled. Please note that for SSH access, a default public key is presented during product launch, customer should provide their own public key so they can gain access to the instance via SSH once deployed, alternatively, customer can gain access via console.

S/N	AWS Services in use	Link to Documentation
1	Amazon MSK	<a href="https://docs.aws.amazon.com/msk/?icmpid=docs_homepage_analytics">https://docs.aws.amazon.com/msk/?icmpid=docs_homepage_analytics</a>
2	Amazon Managed Grafana	<a href="https://docs.aws.amazon.com/grafana/?icmpid=docs_homepage_mgmtgov">https://docs.aws.amazon.com/grafana/?icmpid=docs_homepage_mgmtgov</a>
3	AWS Private Certificate Authority	<a href="https://docs.aws.amazon.com/privateca/?icmpid=docs_homepage_crypto">https://docs.aws.amazon.com/privateca/?icmpid=docs_homepage_crypto</a>
4	AWS IAM Identity Center	<a href="https://docs.aws.amazon.com/singlesignon/?icmpid=docs_homepage_security">https://docs.aws.amazon.com/singlesignon/?icmpid=docs_homepage_security</a>
5	Amazon EC2	<a href="https://docs.aws.amazon.com/ec2/?icmpid=docs_homepage_featuredsvcs">https://docs.aws.amazon.com/ec2/?icmpid=docs_homepage_featuredsvcs</a>
6	Amazon CloudWatch Logs	<a href="https://docs.aws.amazon.com/cloudwatch/">https://docs.aws.amazon.com/cloudwatch/</a>
7	AWS Key Management Service	<a href="https://docs.aws.amazon.com/kms/">https://docs.aws.amazon.com/kms/</a>

### 3.0 Product Internal IAM resources

These IAM resources are internal to the product and will be provisioned when the product is launched by the customer. All provisioned resources will have their names prefixed (supplied when launching product) and tagged for easy identification.

S/N	Name	Description
1	<prefix>KafkaClientInstanceRole	Assumable role by KafkaAdmin user and members of KafkaAdminGroup
2	<prefix>KafkaAuthorizationPolicy	Policy granting access to Kafka data plane operations. Attached to KafkaAdminRole below.
3	<prefix>KafkaAdminRole	Assumable role by KafkaAdmin user and members of KafkaAdminGroup
4	<prefix>KafkaAdminGroup	Group for KafkaAdmins
5	<prefix>KafkaAdminPolicy	Policy attached to KafkaAdminGroup for assuming roles above
6	<prefix>KafkaAdmin	KafkaAdmin user. Console access should be enabled for this user with password set. This will allow the user to be able to assume the KafkaAdminRole.
7	<prefix>GrafanaAdminRole	Associated with Grafana workspace

## 4.0 Product Personas

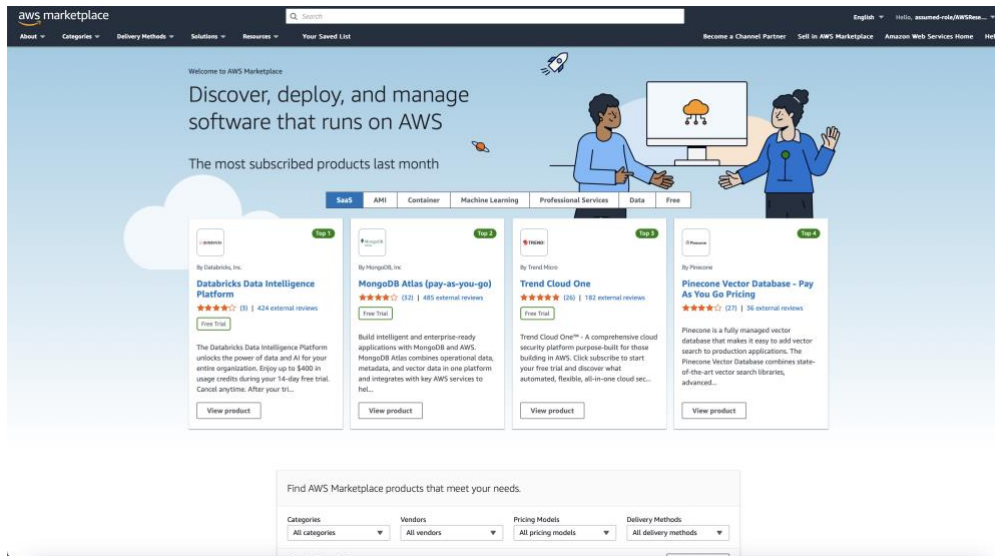
There are mainly two product personas. The product Owner and the product Enduser. These are designated IAM users already existing within the customer account. The table below set out their function and permission association.

<b>S/N</b>	<b>Persona</b>	<b>Responsible for</b>	<b>Permission Assignment</b>
1	Owner	<ol style="list-style-type: none"> <li>1. Subscribing to the product on AWS marketplace</li> <li>2. Launching CloudFormation template that deploys product dependent IAM resources into customer's account</li> <li>3. Adding product to Service Catalog Portfolio.</li> <li>4. Sharing product to Endusers</li> </ol>	<ol style="list-style-type: none"> <li>1. Designated user to be assigned the following AWS Managed policy: <b><i>AWSMarketplaceManageSubscriptions</i></b></li> <li>2. In addition, <b><i>a customer managed policy with content provided in <a href="#">Appendix B</a> must be attached to the user</i></b> (this policy allows the deployment of product dependent IAM resources into customers account)</li> </ol>
2	Enduser	<ol style="list-style-type: none"> <li>1. Launching the product.</li> </ol>	Designated user <b><i>must be added to IAM group – ssipmskgrp</i></b> (this <b><i>IAM group- ssipmskgrp</i></b> will be created into customers account once the CloudFormation template is Launched by Product Owner.)

### 4.0.1 Subscribing to product and launching CloudFormation template.

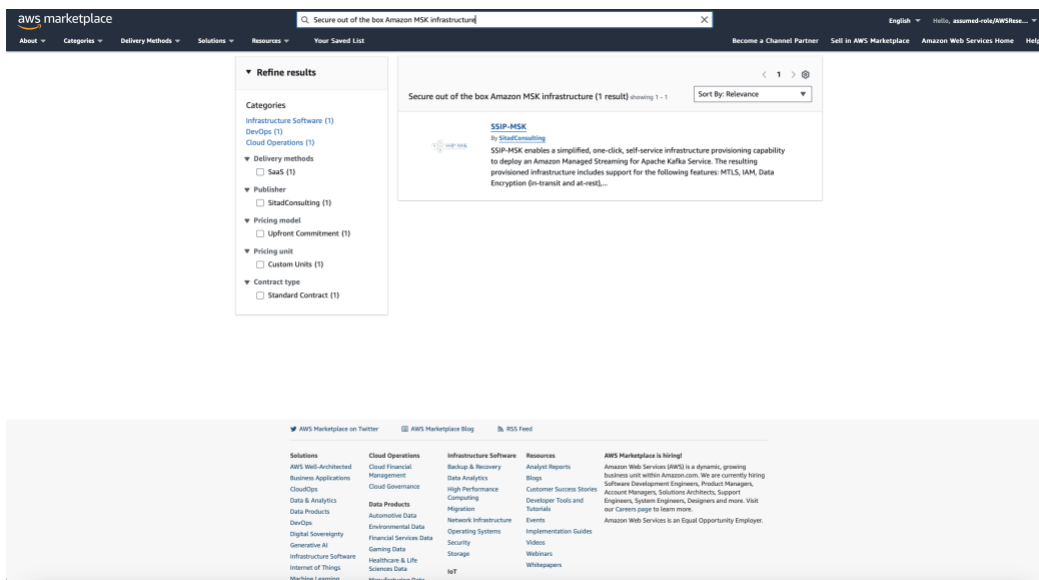
***Please note that the product is going to be shared with the subscribing account, so please ensure that this is the account you intend to have the product deploy into.***

1. As designated Product Owner logon to ***AWS Marketplace***. ***Please ensure that the managed policy “AWSMarketplaceManageSubscriptions” and the customer managed policy in Appendix B has been attached to the designated Product Owner.***
2. The Product Owner logon to ***AWS Marketplace*** is as shown below:



3. At the displayed Product Owner logon to **AWS Marketplace**, in the search box, type in any of the following search phrase to discover our service offering:
  1. Secure out of the box Amazon MSK infrastructure
  2. Workload ready Amazon Managed Streaming for Apache Kafka service
  3. Simplified self-service MSK infrastructure
  4. Simplified self-service infrastructure provisioning capability

Our service offering **SSIP-MSK** is displayed as shown below:



4. On the displayed service offering product page shown above, click on **SSIP-MSK**, you will be redirected to the product subscription page as shown below:

The screenshot displays the AWS Marketplace product page for SSIP-MSK. The page is structured as follows:

- Header:** Includes the AWS Marketplace logo, search bar, and navigation links like 'About', 'Categories', 'Delivery Methods', 'Solutions', 'Resources', and 'Your Saved List'.
- Product Card:** Features the product name 'SSIP-MSK', a 'View purchase options' button, and a brief description: 'SSIP-MSK enables a simplified Self-Service Infrastructure Provisioning capability of a workload ready Amazon Managed Streaming for Apache Kafka Service. It offers a one-click deployment of a secure out of the box Amazon...'.
- Overview:** A detailed paragraph explaining the product's capabilities and features, including MTL, IAM, Data Encryption, and integration with other AWS services.
- Highlights:** A list of key features: 'Simplified self-service infrastructure provisioning Composable cloud infrastructure', 'One-click deployment, No-code deployment', and 'Workload ready infrastructure'.
- Details:** A section providing metadata such as 'Sold by: SitadConsulting', 'Categories: Streaming solutions, Infrastructure as Code, Cloud Operations', and 'Delivery method: Software as a Service (SaaS)'.
- Financing for AWS Marketplace purchases:** A section mentioning the PNC Vendor Finance program.
- Pricing:** A section showing pricing based on contract duration (24-month and 36-month) and a table for the '24-month contract (1)' with columns for Dimension, Description, and Cost/24 months.
- Vendor refund policy:** A section stating 'Provided as part of private offer arrangement'.
- Legal:** A section for 'Vendor terms and conditions' with a link to the 'User License Agreement (ULA)'.
- Content disclaimer:** A section stating 'Vendor is responsible for their product descriptions and other product content. AWS does not warrant that vendor product descriptions or other product content are accurate, complete, reliable, current, or error-free'.
- Usage information:** A section for 'Delivery details' explaining the SaaS model and recurring monthly usage fees.
- Resources:** A section for 'Vendor resources' with a link to 'SSIP-MSK PRODUCT ONBOARDING'.
- Support:** A section for 'Vendor support' with a link to 'ssp@sitadconsulting.com' and 'AWS infrastructure support' with a 'Get support' button.
- Customer reviews:** A section at the bottom with a 'Write a review' button.

- At the displayed product subscription page above, at the top of the page on the right, click on **View purchase options** button, you will be redirected to **Purchase options** page as shown below:

[AWS Marketplace](#) > [SSIP-MSK](#) > [Subscribe to SSIP-MSK](#)  
**Subscribe to SSIP-MSK** [Info](#)  
 To create a subscription, review the pricing information and accept the terms for this software.

**Offer details** [Info](#)  
 Offer ID: offer-vmsxomyzps5sq | Offered by: SitadConsulting | Offer type: Public

**Contract configuration**  
 Configure your contract duration and auto-renewal settings for the selected offer.

**Contract duration**  
 24 months |  36 months

**Auto-renewal**  
 Choose which renewal option you want to use for your contract.  
 Automatically renew this contract when it expires on Mar 27, 2027.  
 Do not automatically renew this contract.

**Auto-renewal terms**  
 I acknowledge that when my contract automatically renews on Mar 27, 2027, the seller's pricing and end user license agreement (EULA) may have changed. I understand that my renewed contract will be based on the pricing and terms applicable on the renewal date.

**Contract details**  
 Contract duration: 24 months | Start date: Mar 27, 2025 | End date: Mar 27, 2027 | Auto-renewal:  On

**Pricing details and unit configuration**  
 AWS Marketplace charges an upfront cost for a contract, which entitles you to use the product based on your contract terms and duration. Usage is limited to contract terms and duration. At expiration, subscription ends unless you renew or replace the contract.

**Available units (1)**  
 Select the units you want to buy. Usage-based charges apply in addition to contract fees.

Units	Description	Cost/unit
<input checked="" type="radio"/> Enterprise	Per Instance deployment	US\$0.001/units

**Total amount**  
 Total contract cost: **US\$0.00** | Contract currency: United States Dollar (USD) (\$) | Tax details: Additional taxes may apply

**Terms and conditions** [Download EULA\(s\)](#)  
 By subscribing to this software, you agree to the pricing terms and the seller's End User License Agreement (EULA). You also agree and acknowledge that AWS may, on your behalf, share information about the transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services is subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services. If you are receiving a private offer from a channel partner, you may click here for EPPD transaction or here for SPPD transaction for more information on the channel partner.

**Purchase order (PO) number** [Info](#)  
 You can assign unique purchase order numbers to charges to include them on your invoices. [Learn more](#)

**Purchase order number options**  
 No purchase order  
 Add a purchase order

**Purchase details** [Info](#)  
 Offer ID: offer-vmsxomyzps5sq | Offered by: SitadConsulting | Total contract cost: US\$0.00 | Contract duration: 24 months  
 Auto-renewal:  On | Number of units selected: 1 | Tax details: Additional taxes may apply | Purchase order numbers: -

[Back](#) [Subscribe](#)

6. At the displayed **Purchase options** page, click on **Contract duration** of your choice, next, click on **Enterprise**, scroll down to the end of the page and click on **Subscribe** button, after a few minutes, your purchase is complete, you will receive an email with details of the product purchased. A sample email and **purchase complete** page are shown below:

**AWS Marketplace**

You accepted an AWS Marketplace offer

Inbox - Yahoo! 14:49

To: [REDACTED]



This message is from a mailing list.

Unsubscribe



Greetings from AWS Marketplace,

An AWS Marketplace offer has been accepted by AWS account [REDACTED] on January, 13 2025 02:47 PM UTC, and an agreement was created.

Review the following details:

Seller details**Seller name:** SitadConsultingProduct details**Product name:** SSIP-MSK**Product ID:** prod-vhdrvzlia6rt2Offer details**Offer name:** Offer created on 2024-10-29T15:20:33.498Z**Offer ID:** offer-vinxomyzp55qAgreement details**Agreement ID:** agmt-c234s222mrsfaqh1yt3k16vq**Agreement start Date:** January, 13 2025 02:47 PM UTC**Agreement end Date:** January, 13 2027 02:47 PM UTC**Purchase amount:** 0.001 (USD)

For SaaS products, register with the seller's website by visiting the procurement page to set up your account and start using the product. For more details, review our [Buyers guide](#).

The subscriber will receive entitlements to the product on the January, 13 2025 02:47 PM UTC. If there are processing issues, they will be notified in a separate email.

To review details of your agreement, visit the [Manage subscriptions page](#). For agreements on data products, visit the [AWS Data Exchange console](#).

If you have any questions about your agreement or need assistance, visit [AWS Support](#).

Regards,

The AWS Marketplace Team

AWS Marketplace > SSIP-MSK > Subscribe to SSIP-MSK

**Subscribe to SSIP-MSK** [Info](#)  
 To create a subscription, review the pricing information and accept the terms for this software.

✔ **Your purchase of SSIP-MSK is complete** [Set up your account](#)

Next, set up your account and complete registration on the vendor's website. If you're unable to complete registration, return through the [Manage subscriptions](#) page on AWS Marketplace.

ⓘ **Financing for AWS Marketplace purchases** [View financing details](#)

AWS Marketplace now accepts line of credit payments through the PNC Vendor Finance program. This program is available to select AWS customers in the US, excluding NV, NC, ND, TN, & VT.

**Offer details** [Info](#)

<b>Offer ID</b> offer-vinxomyzp55q	<b>Offered by</b> SitadConsulting	<b>Offer type</b> Public
---------------------------------------	--------------------------------------	-----------------------------

ⓘ **You already have contract(s) for this product.**  
 If needed, you can [modify](#) the existing agreement and set up your account on the [vendor's website](#).

**Contract configuration**  
 Configure your contract duration and auto-renewal settings for the selected offer.

**Contract duration**

24 months  36 months

**Auto-renewal**  
 Choose which renewal option you want to use for your contract.

Automatically renew this contract when it expires on Jan 13, 2027  
 Do not automatically renew this contract

ⓘ **Auto-renewal terms**  
 I acknowledge that when my contract automatically renews on **Jan 13, 2027**, the seller's pricing and end user license agreement (EULA) may have changed. I understand that my renewed contract will be based on the pricing and terms applicable on the renewal date.

**Contract details**

<b>Contract duration</b> 24 months	<b>Start date</b> Jan 13, 2025	<b>End date</b> Jan 13, 2027	<b>Auto-renewal</b> <input checked="" type="radio"/> On
---------------------------------------	-----------------------------------	---------------------------------	--

**Pricing details and unit configuration**  
 AWS Marketplace charges an upfront cost for a contract, which entitles you to use the product based on your contract terms and duration. Usage is limited to contract terms and duration. At expiration, subscription ends unless you renew or replace the contract.

**Available units (1)**  
 Select the units you want to buy. Usage-based charges apply in addition to contract fees.

Units	Description	Cost/unit
<input checked="" type="radio"/> Enterprise	Per instance deployment	\$0.001/Units

**Total amount**

<b>Total contract cost</b> <b>\$0.00</b>	<b>Contract currency</b> United States Dollar   USD (\$)	<b>Tax details</b> Additional taxes may apply
---	---	--

**Terms and conditions** [Download EULA\(s\)](#)

By subscribing to this software, you agree to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You also

- At the displayed **Purchase completion** page, in the green box, click on **Set up your account** button, you will be redirected to Quick Launch page as shown below:

SSIP-MSK &gt; Configure and launch

## Configure and launch

## ▼ Before you begin

## About Quick Launch

Quick Launch is an AWS Marketplace deployment option available for software as a service (SaaS) products. It reduces the time, resources, and steps required to configure, deploy, and launch this product. If you don't use Quick Launch, you'll need to manually configure the resources after launching the product using Step 4. [Learn more](#)



## Finish later

We emailed a link to this page to the root user's email address. You can also return to this page from the Manage subscriptions page by choosing **Configure and launch** under **Actions**.

Step 1: Make sure you have required AWS permissions [Info](#)

**Enable AWS Marketplace deployment parameters integration**  
This allows AWS Marketplace to create a [service-linked role](#) to manage vendor deployment parameters for the products you subscribe to on AWS Marketplace. This integration is one-time setup task, and is required if you want to use Quick Launch. [Learn more](#)

## Request AWS permissions

SitadConsulting requires you to have [certain IAM permissions](#) to configure this software. If you don't have these permissions, share this page with your IT admin.

<https://aws.amazon.com/marketplace/saas/configuration?productId=prod-vhdrvzia6rt2>

Step 2: Log into an existing or new vendor account [Info](#)

We'll redirect you to the vendor's website to log into your account. We'll use your vendor credentials to configure your product, but we won't store them. **Keep this tab open and refresh the page after you are logged in.**

Step 3: Configure your software and AWS integration [Info](#)

[CloudFormation](#) allows you to automatically launch and configure your resources and their dependencies as a stack. The stack templates are reviewed and verified by AWS. Once the stack's status is `CREATE_COMPLETE`, return to this page to launch the product.

Deploy-ssip-msk-iam-resources [View required IAM permission](#)

This template deploys the required IAM resources that supports the provisioning of SSIP-MSK product

## Step 4: Launch your software

If you're using Quick Launch, verify that you've completed the configuration steps above before launching the product. If you're manually configuring your resources, choose **Launch software**.

8. At the displayed **Configure and launch** page, follow the on-screen instruction and complete Step 1, 2 and 3
9. Step 1, click on **Enable integration**, once integration is enabled you see in a green bar the statement **AWS Marketplace deployment parameters integration enabled**, as shown below:

**Step 1: Make sure you have required AWS permissions** [Info](#)

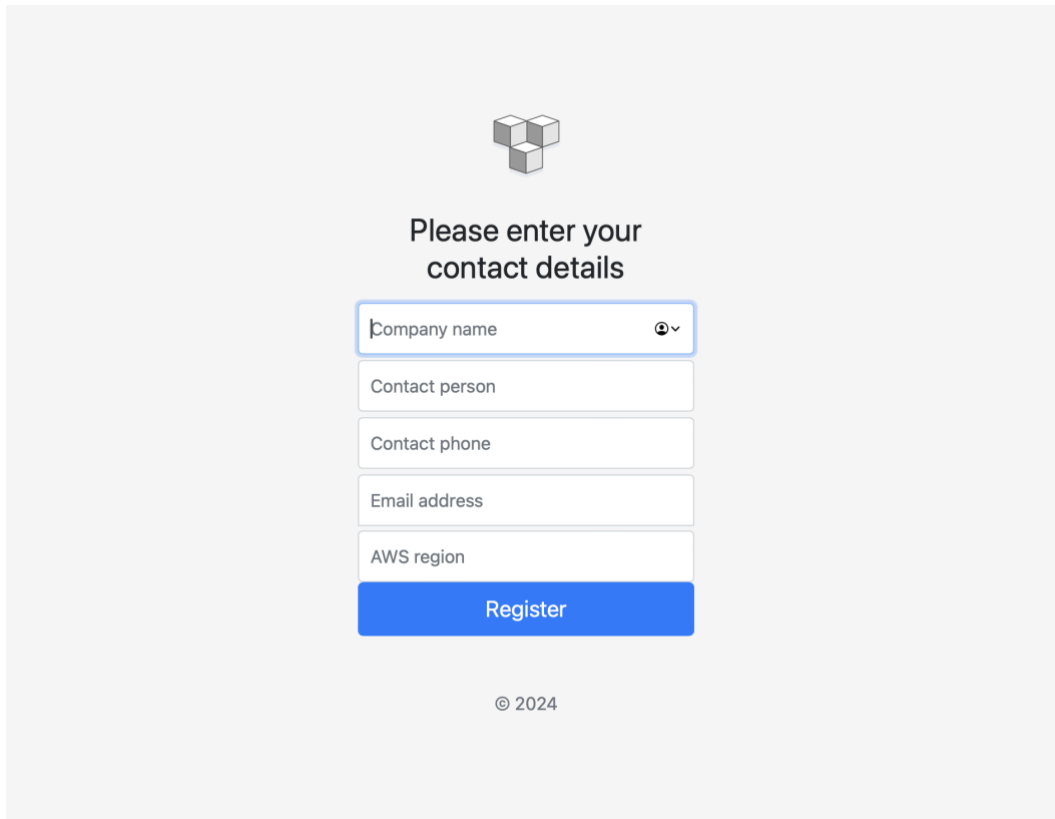
✔ AWS Marketplace deployment parameters integration enabled. ✕

**Request AWS permissions**

SitadConsulting requires you to have [certain IAM permissions](#) to configure this software. If you don't have these permissions, share this page with your IT admin.

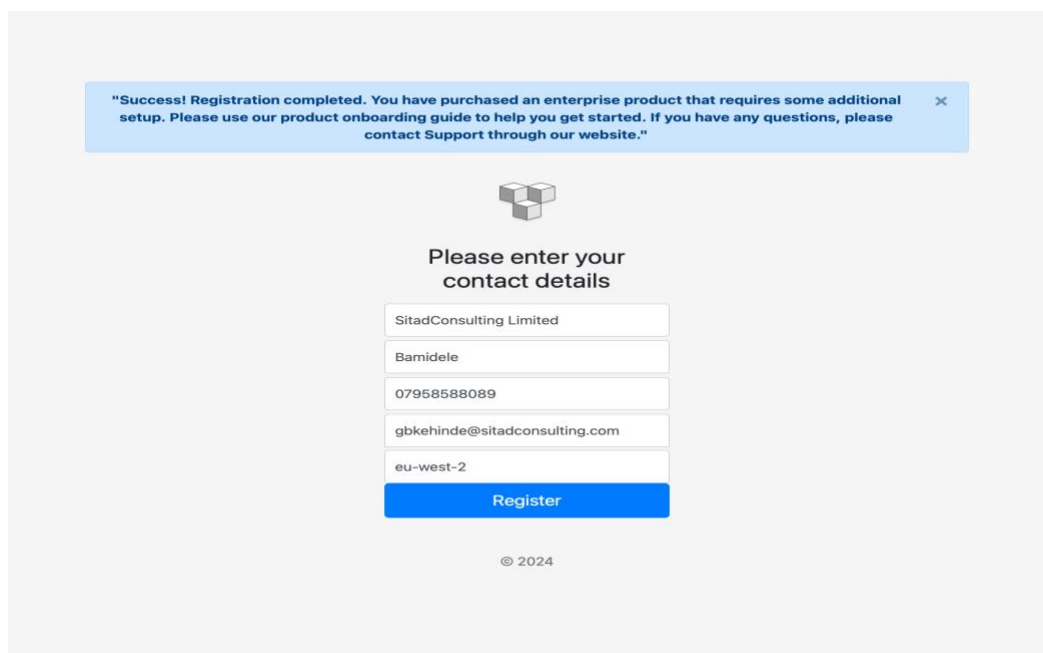
[https://aws.amazon.com/marketplace/saas/configuration?productId=prod-vhdrvzia6rt2&ref\\_=aws-mp-console-subscription-table-action](https://aws.amazon.com/marketplace/saas/configuration?productId=prod-vhdrvzia6rt2&ref_=aws-mp-console-subscription-table-action)

10. Step 2, click on **Log in or create account**, you will be redirected to the account creation page as shown below:



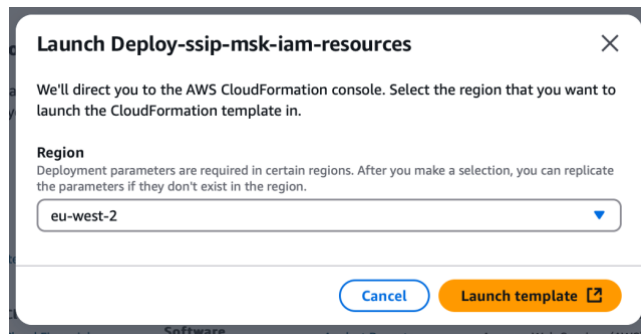
The screenshot shows a registration form on a light gray background. At the top center is a logo consisting of three interlocking cubes. Below the logo is the text "Please enter your contact details". The form consists of five input fields stacked vertically: "Company name" (with a dropdown arrow), "Contact person", "Contact phone", "Email address", and "AWS region". Below these fields is a blue "Register" button. At the bottom center, there is a copyright notice "© 2024".

11. At the displayed account creation page, ***please note that each field must be filled in with correct information to capture the details of the product Owner (We can only grant access to the product when all fields have been entered correctly)*** and click **Register** button, a successful registration banner is displayed as shown below:

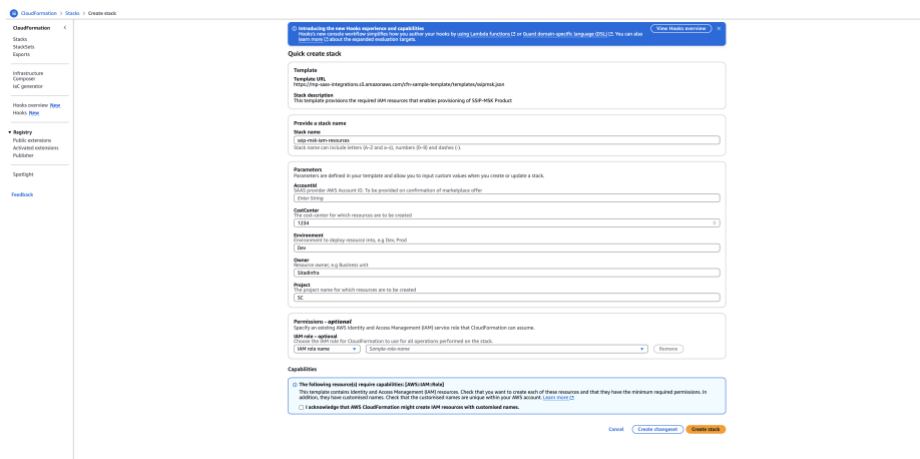


The screenshot shows the same registration form as in the previous image, but now it is filled with data. Above the form is a blue success banner with a close button (X) on the right. The banner text reads: "Success! Registration completed. You have purchased an enterprise product that requires some additional setup. Please use our product onboarding guide to help you get started. If you have any questions, please contact Support through our website." The form fields are filled with: "SitadConsulting Limited", "Bamidele", "07958588089", "gbkehinde@sitadconsulting.com", and "eu-west-2". The blue "Register" button is still visible at the bottom. The copyright notice "© 2024" is at the bottom center.

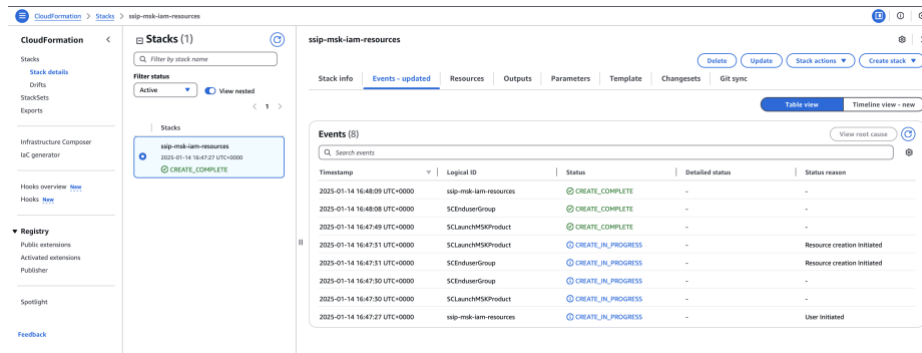
12. Step 3, click on **Launch template** button to deploy product dependent IAM resources, follow the on-screen prompts, at the displayed Launch **Deploy-ssip-msk-iam-resources** screen, shown below, use the drop-down arrow to choose the AWS region you specified in step 12 above, click Launch template, you will be redirected to the CloudFormation console



13. At the displayed **CloudFormation console** screen, on the right-pane, under parameter section, fill-in the pertinent details, tick **I acknowledge that AWS CloudFormation might create IAM resources with customised names**, and click on **Create stack** button. The **AccountID** parameter is provided via AWS Secret Manager deployed into customer account after product subscription is complete. Retrieve the **AccountID** from Secret Manager.

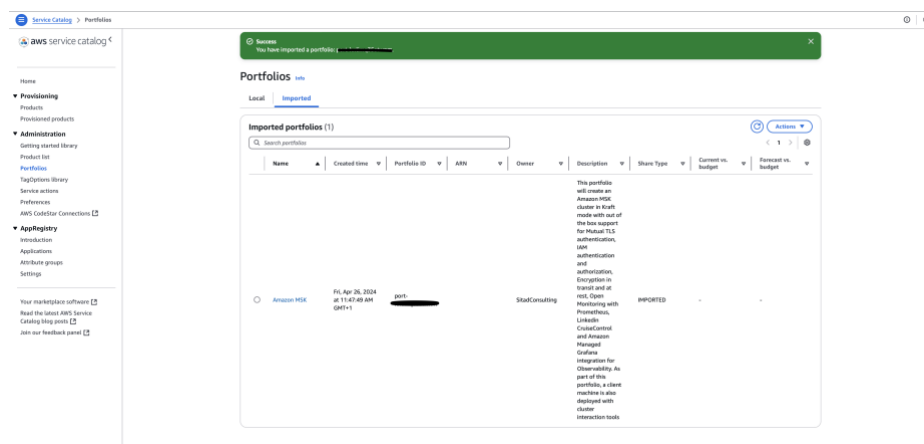


14. After a few minutes the stack is created as shown below:



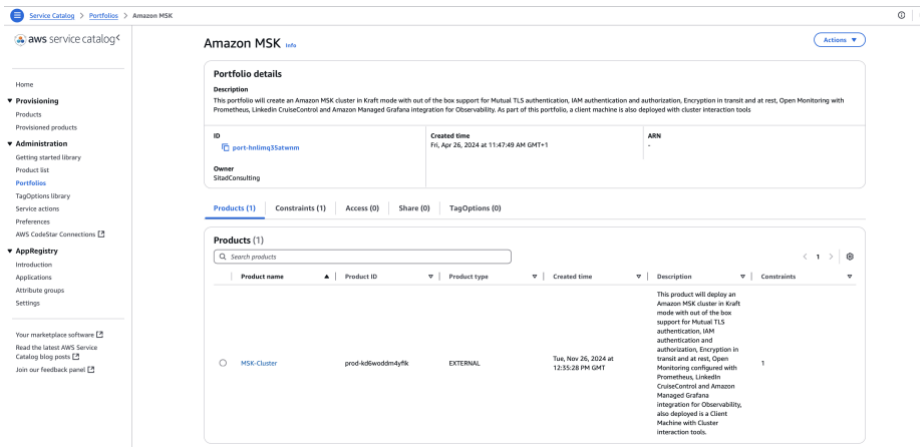
#### 4.0.2 Adding product to Service Catalog Portfolio.

1. As product Owner logon to AWS console and search for **Service Catalog** service and click on **Service Catalog**
2. At the displayed Service Catalog console, on the left-pane, under **Administration** click on **Portfolios**.
3. At the displayed Portfolios page, click on the tab **Imported**, next, on the right end, click **Action** button, then click **Import portfolio**, leave the default choice of **AWS account**, next, enter the **Portfolio ID** (provided via AWS Secret Manager deployed into customer account after product subscription is complete. Retrieve the **Portfolio ID** from Secret Manager) and click **Import**, the portfolio is imported as shown below:

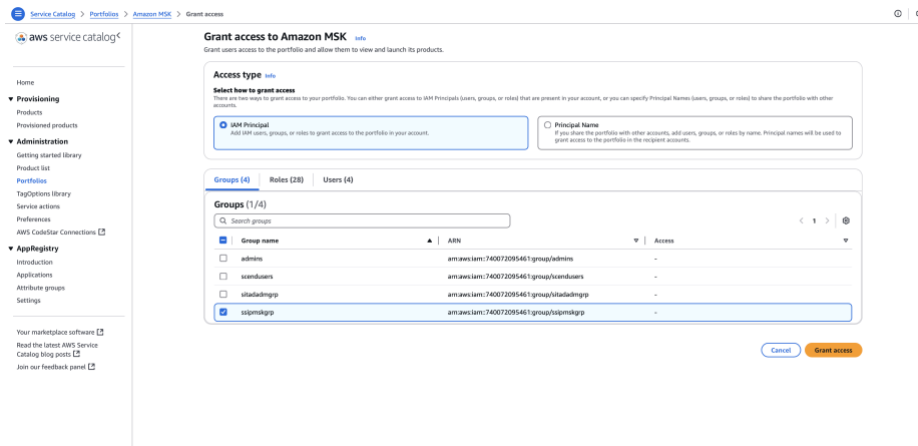


#### 4.0.3 Sharing the product

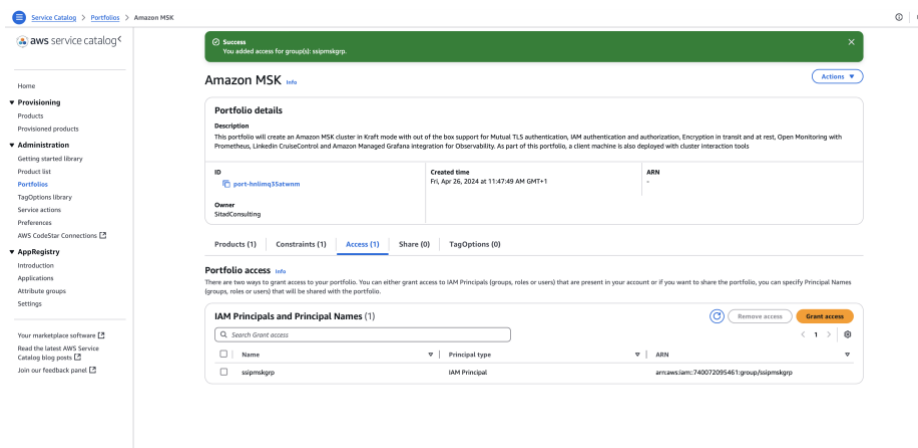
1. As the product Owner, and logon on to Service Catalog, on the left-pane under **Administration**, click on **Portfolios**, at the displayed right-pane **Portfolios** page click on the Imported tab, next click on **Amazon MSK** portfolio, the portfolio will be displayed as shown below:



- At the displayed **Amazon MSK** portfolio, click on the **Access** tab, at the displayed **Portfolio access** section, click on **Grant access** button, the **Grant access to Amazon MSK** page, select the group **ssipmskgrp**, as shown below:



- After selecting the group **ssipmskgrp**, click on **Grant access** button, access is granted as shown below:

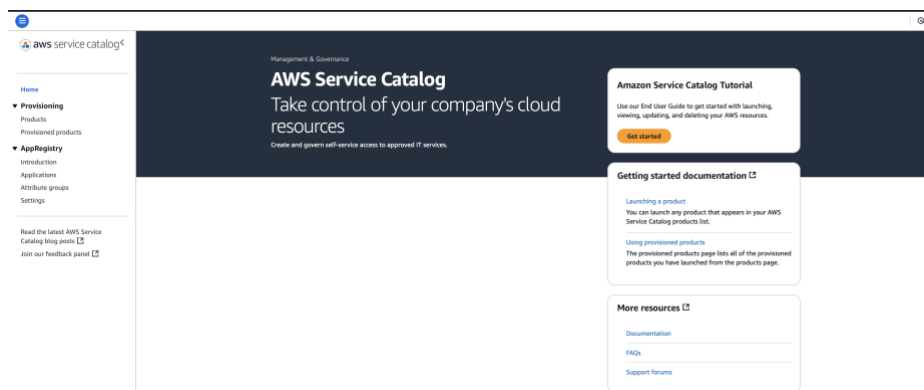


#### 4.0.4 Launching the product.

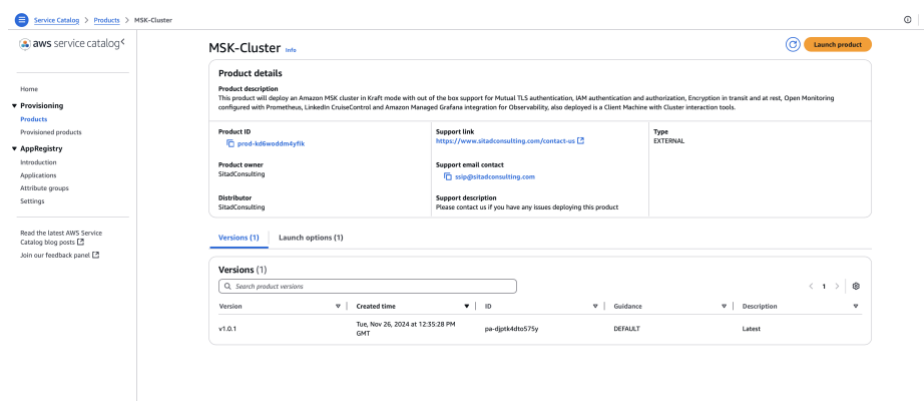
Before attempting to launch the product, please ensure that the product Owner has completed section 4.0.1, 4.0.2 and 4.0.3 above. In section 4.0.1, the CloudFormation template deploys the dependent IAM resources required to ensure a successful product launch. The table below describes the IAM resources deployed by CloudFormation template.

S/N	IAM Resources	Name	Usage
1	IAM Group	ssipmskgrp	Designated <b>product Enduser must be added to this group by the customer</b> , after which the user can proceed with executing the steps outlined in this section
2	IAM Role	SCLaunch-MSKProducts	This role is assumed by Service Catalog, it contains all dependent IAM permission to support launching of the product

1. As product Enduser, logon to AWS console and search for *Service Catalog*, then click on the displayed Service Catalog, you will be redirected to the page shown below



2. At the displayed **Service Catalog** console menu items, under **Provisioning**, click on **Products**, on the displayed right-pane **Products** page, click on the **MSK-Cluster** product, the **MSK-Cluster**, product details page is displayed as shown below:



3. At the displayed **MSK-Cluster** product details page, click on **Launch product** button, the **Launch: MSK-Cluster** page is displayed as shown below:

Launch: MSK-Cluster [info](#)

This product will deploy an Amazon MSK cluster in Kraft mode with out of the box support for Mutual TLS authentication, IAM authentication and authorization, Encryption in transit and at rest, Open Monitoring configured with Prometheus, LinuxEBS CloudControl and Amazon Managed Grafana integration for Observability, also deployed is a Client Machine with Cluster Interaction tools.

**Provisioned product name**  
 Enter a unique name or select Generate name to provide a name automatically.  
  
 The name must start with a letter (A-Z, a-z) or number (0-9). Other valid characters include hyphen (-), underscore (\_), and period (.).  
 Generate name

**Product versions (1/1)**  
 < 1 >  

Version	Created time	ID	Guid
v1.0.0	Thu, Apr 3, 2025 at 9:58:55 AM GMT+1	pe-nb6G6thgm24	DEFAULT

**Parameters**  
 ca\_cert\_usage\_mode  
 ca\_cert\_validity\_value  
 cert\_common\_name  
 cert\_country\_code  
 cert\_location  
 cert\_organization\_name  
 cert\_organizational\_unit\_name  
 env-center  
 msk\_storage\_provisioned\_volume\_throughput  
 msk\_provisioned\_throughput  
 env-namespace  
 grafana\_admin\_user\_primary\_email\_address\_value  
 grafana\_managed\_grafana\_list\_name  
 grafana\_public\_cdk\_access  
 kafka\_client\_instance\_monitoring  
 kafka\_client\_instance\_public\_key  
 kafka\_client\_instance\_type  
 msk\_cluster\_efs\_storage\_life\_volume\_size  
 msk\_cluster\_enhanced\_monitoring  
 msk\_cluster\_kafka\_instance\_type  
 msk\_cluster\_kafka\_instance\_size  
 msk\_cluster\_kafka\_provisioned\_throughput\_instance\_type  
 msk\_cluster\_kafka\_version  
 msk\_cluster\_msk\_broker\_logs\_retention\_in\_days  
 project  
 remote\_access\_to\_kafka\_client\_instance\_port\_22  
 remote\_access\_to\_kafka\_client\_instance\_port\_3000  
 remote\_access\_to\_kafka\_client\_instance\_port\_3001  
 resource-owner  
 s3\_key\_password  
 s3\_keystore\_password

**Manage tags - optional**  
 You can use tags to categorize your resources.

[Cancel](#) [Launch product](#)

4. At the displayed **Launch: MSK-Cluster** page, assign a name to the deployment or click the **Generate name**, next review the **Parameters section, ensure pertinent details are entered for the following:**
  - a. Please update certificate related parameters (cert\_common\_name, cert\_country\_code, cert\_organization\_name, cert\_organizational\_unit\_name, cert\_locality), **with pertinent details**.
  - b. Tagging parameters (cost-center, environment, project(a 2 letter code), resource-owner)
  - c. Please update remote access parameters **to reflect pertinent details**.
  - d. Kafka\_Client\_instance\_public\_key parameter (please note that a value for SSH public key **must be provided, customer must set a dummy SSH key value if they are not providing a real SSH public key**)
  - e. Please update Grafana parameters (grafana\_managed\_prefix\_list\_name, grafana\_public\_cidr\_access, grafana\_admin\_user\_primary\_email\_address\_value), **with pertinent details**.
  - f. Kafka parameters (if enabling provisioned throughput, then ensure the supported Kafka instance type is specified)
  - g. Update value for ssl\_keystore\_password and ssl\_key\_password

After updating parameters **with pertinent details**, click on **Launch product** button at the end of the page, after successful deployment of the product the screen shown below is displayed

The screenshot displays the AWS Service Catalog console for the 'deploy-ssipmsk' product. At the top, a green success message states: 'Successfully launched deploy-ssipmsk. You can now view the events and outputs associated with this product below.' The product details section includes a description of an Amazon MSK cluster in Kraft mode with Mutual TLS authentication, IAM authentication, and encryption. It also lists key attributes: Provisioned product ID (pp-ows2kqf72py), User name (SCUser1), Status (Available), Product name (MSK-Cluster), User ARN (arn:aws:iam::740072095461:user/SCUser1), Created (Tue, Feb 4, 2025 at 10:54:41 AM GMT), Provisioned product ARN (arn:aws:servicecatalog:us-east-1:740072095461:stack/deploy-ssipmsk/pp-ows2kqf72py), Version name (v1.0.1), and Product type (EXTERNAL).

Below the details, the 'Resources (45)' section is visible, listing various AWS resources created by the product. The resources are categorized by type and include:

- AWS-ACMPCA-CertificateAuthority**: e2e59365-389b-4069-803b-ad5509f1766d
- AWS-EC2-DHCPOptions**: amawsnc2-us-east-1:740072095461:dhcp-options/dopt-030ca5e0d2599e9db
- AWS-EC2-EIP**: amawsnc2-us-east-1:740072095461:elastic-ip/elipalloc-05fe02aed2920c05e, amawsnc2-us-east-1:740072095461:elastic-ip/elipalloc-0a48e709f2371447, amawsnc2-us-east-1:740072095461:elastic-ip/elipalloc-0c0ef5f4963e4da9
- AWS-EC2-Instance**: amawsnc2-us-east-1:740072095461:instance/i-0f4156720078040b0
- AWS-EC2-InternetGateway**: amawsnc2-us-east-1:740072095461:internet-gateway/igw-00a551f52c715af3
- AWS-EC2-KeyPair**: key-022a50c4c995380a0
- AWS-EC2-LaunchTemplate**: amawsnc2-us-east-1:740072095461:launch-template/lt-0c9975475c0d89f4a
- AWS-EC2-NatGateway**: nat-019f742bb7ee8b05, nat-04f27d3584a9b02d61, nat-0bd200ba90ca9fb68
- AWS-EC2-PrefixList**: pl-0f7b745f5301cbb2
- AWS-EC2-RouteTable**: rtb-01381f8a7a97cce6d, rtb-04809b790d0ee487f, rtb-058b090e1a5825308, rtb-0bc5733f8b6b164
- AWS-EC2-SecurityGroup**: amawsnc2-us-east-1:740072095461:security-group/sg-019f6c812a5f8b98, amawsnc2-us-east-1:740072095461:security-group/sg-04e1d667a479880a6, amawsnc2-us-east-1:740072095461:security-group/sg-09e1f6a235d885a16

## 5.0 Post Provisioning tasks

Logon to the Kafka client instance to start LinkedIn CruiseControl service and access the WebUI

**Please note that the customer is required to replace the default SSH public key provided during product launch to be able to gain access to the instance after deployment.**

Start a remote ssh sessions to the instance, example shown below:

```
ssh -i "SCKafkaClientInstancePubkey.pem" ec2-user@ec2-54-234-163-97.compute-1.amazonaws.com
```

```
Warning: Identity file SCKafkaClientInstancePubkey.pem not accessible: No such file or directory.
```

```
, #_
~\ ####_ Amazon Linux 2023
~~ \#####\
~~ |###|
~~ |#/___ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '->
~~~ /
~~_._ \
/_/_/
_/m/'
```

```
Last login: Fri Oct 18 16:28:11 2024 from 86.133.201.101
```

```
[ec2-user@ip-10-0-49-224 ~]$
```

At the \$ prompt displayed above, switch user to cruisecontrol as shown below:

```
[ec2-user@ip-10-0-49-224 ~]$ sudo su – cruisecontrol
```

Press the return key so that the cruisecontrol user session is displayed as shown below:

```
[cruisecontrol@ip-10-0-49-224 ~]$
```

At the display cruisecontrol user prompt, change into “cruise-control” directory as show below:

```
[cruisecontrol@ip-10-0-49-224 ~]$ cd cruise-control
```

Press the return key, the “cruise-control” directory is displayed as shown below:

```
[cruisecontrol@ip-10-0-49-224 cruise-control]$
```

At the displayed “cruise-control” directory prompt, start the CruiseControl service as show below:

```
[cruisecontrol@ip-10-0-49-224 cruise-control]$ ./kafka-cruise-control-start.sh -  
daemon config/cruisecontrol.properties 9091
```

Press the enter key.

Next, check that the CruiseControl service is running, execute the command below:

```
[cruisecontrol@ip-10-0-49-224 cruise-control]$ ps -ef | grep cruise | grep java  
cruisec+ 29724 1 11 17:09 pts/1 00:00:17 java -Xmx1G -server -XX:+UseG1GC -  
XX:MaxGCPauseMillis=20 -XX:InitiatingHeapOccupancyPercent=35 -  
XX:+DisableExplicitGC -Djava.awt.headless=true -Dcom.sun.management.jmxremote  
-Dcom.sun.management.jmxremote.authenticate=false -  
Dcom.sun.management.jmxremote.ssl=false -Dkafka.logs.dir=./logs -  
Dlog4j.configurationFile=file:./config/log4j.properties -cp ./cruise-  
control/build/dependant-libs/*:./cruise-control/build/libs/*:./cruise-control-metrics-  
reporter/build/libs/* com.linkedin.kafka.cruisecontrol.KafkaCruiseControlMain  
config/cruisecontrol.properties 9091  
cruisec+ 29927 29605 0 17:12 pts/1 00:00:00 grep --color=auto java
```

The output shows that the CruiseControl service started ok.

Next, access CruiseControl Web UI to visualize the state of your Kafka Clusters.

Setup a remote ssh tunnel into your Kafka Client Instance as shown below:

```
sitadconsulting@sitads-MBP ~ % ssh -L 9091:127.0.0.1:9091 -i ssh -i  
"SCKafkaClientInstancePubkey.pem" ec2-user@ec2-54-234-163-97.compute-  
1.amazonaws.com
```

Press the return key, a tunnel session is established as shown below:

```
Warning: Identity file ssh not accessible: No such file or directory.  
Warning: Identity file SCKafkaClientInstancePubkey.pem not accessible: No such file  
or directory.  
The authenticity of host 'ec2-54-234-163-97.compute-1.amazonaws.com  
(54.234.163.97)' can't be established.  
ED25519 key fingerprint is  
SHA256:vGP++ny3ABPIpyO1iSJH5W718kqVxQMeqtBShBM4gsg.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-54-234-163-97.compute-1.amazonaws.com'  
(ED25519) to the list of known hosts.  
, #_  
~\ ####_ Amazon Linux 2023  
~~ \#####\
```

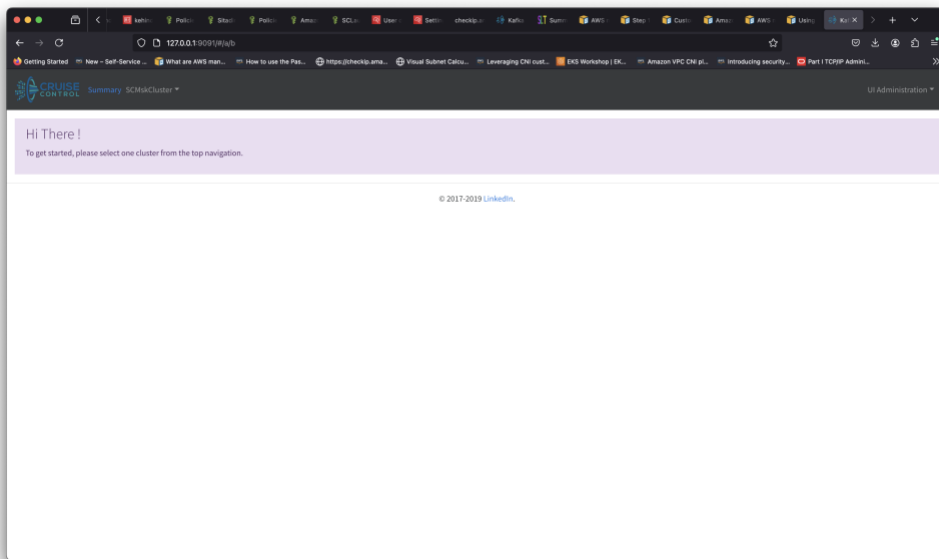
```

~ ~ \###|
~ ~ \#/___ https://aws.amazon.com/linux/amazon-linux-2023
~ ~ V~' !->
~ ~ ~ /
~ ~ ~. /
~ ~ ~ /
~ ~ ~ /m/'

```

Last login: Fri Oct 18 16:41:52 2024 from 86.133.201.101  
[ec2-user@ip-10-0-49-224 ~]\$

Next, fire up a browser of your choosing and enter in the address bar this localhost url – <http://127.0.0.1:9091>



At the left-hand side of the page, click on your Cluster name and navigate to the Kafka Cluster Load Tab, the page below is displayed.

The screenshot displays the Cruise Control console for an SCMSkCluster. It features a navigation bar with tabs for Kafka Cluster State, Kafka Cluster Load, Kafka Partition Load, Cruise Control State, Cruise Control Proposals, Cruise Control Tasks, Resource distributions, Peer Reviews, and Kafka Cluster Administration. A 'Flags: Allow Capacity Estimation' section is visible, along with a 'Refresh Kafka Cluster Load' button. Below this, two tables provide detailed load information:

**Kafka Server Load**

Host	Topic/Partition		Disk/Cpu		Network Rate					
	#Replicas	#Leaders	Disk	CPU	Leader In	Follower In	Network Out	Potential Out	LF Ratio	IO Ratio
b-1.scmskcluster.7eg2za.c13.kafka.us-east-1	94	40	359.24 KB	4.16 %	39 Bps	23 Bps	89 Bps	138 Bps	0.5800	0.4431
b-3.scmskcluster.7eg2za.c13.kafka.us-east-1	95	39	370.90 KB	1.26 %	0 Bps	59 Bps	0 Bps	135 Bps		
b-2.scmskcluster.7eg2za.c13.kafka.us-east-1	98	38	383.81 KB	6.81 %	26 Bps	38 Bps	52 Bps	140 Bps	1.4564	0.5071

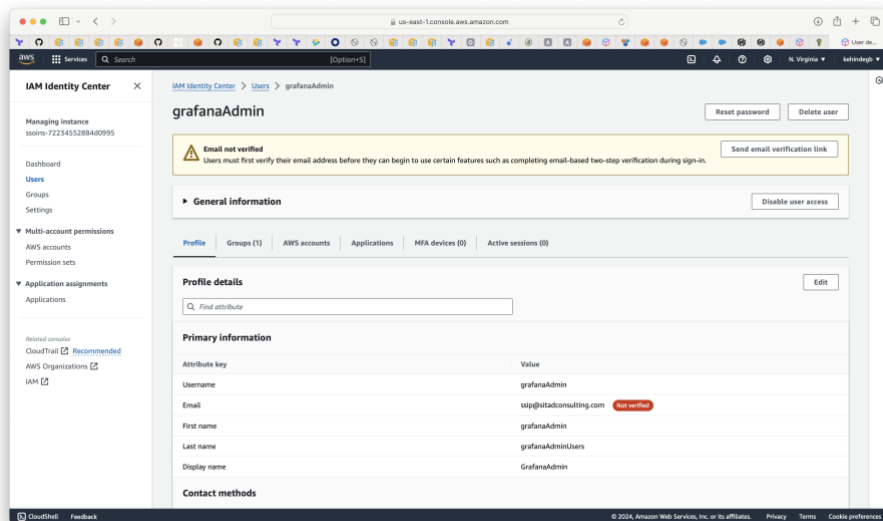
**Kafka Broker Load**

ID	State	Host	Topic/Partition		Disk/Cpu		Network Rate					
			#Replicas	#Leaders	Disk Used	CPU Used	Leader In	Follower In	Network Out	Potential Out	LF Ratio	IO Ratio
1	ALIVE	b-1.scmskcluster.7eg2za.c13.kafka.us-east-1	94	40	359.24 KB	4.16 %	39 Bps	23 Bps	89 Bps	138 Bps	0.5800	0.4431
3	ALIVE	b-3.scmskcluster.7eg2za.c13.kafka.us-east-1	95	39	370.90 KB	1.26 %	0 Bps	59 Bps	0 Bps	135 Bps		
2	ALIVE	b-2.scmskcluster.7eg2za.c13.kafka.us-east-1	98	38	383.81 KB	6.81 %	26 Bps	38 Bps	52 Bps	140 Bps	1.4564	0.5071

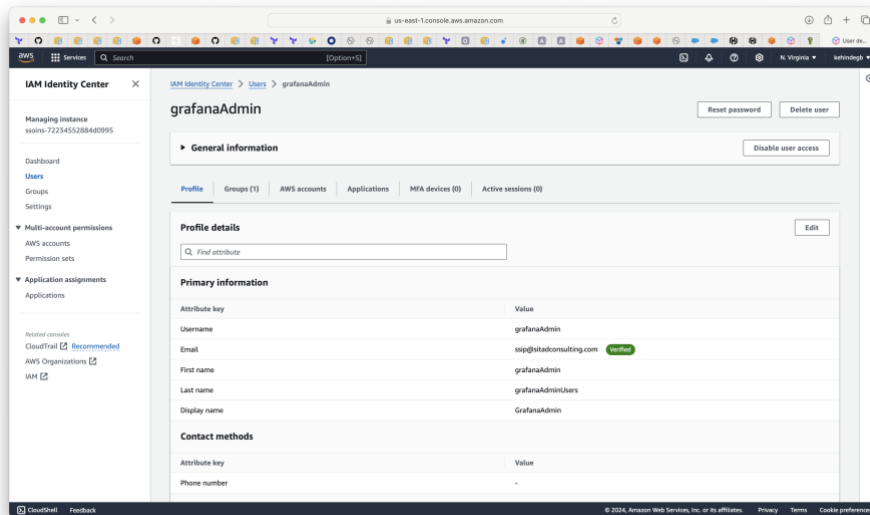
© 2017-2019 LinkedIn.

## Accessing Amazon Managed Grafana Console

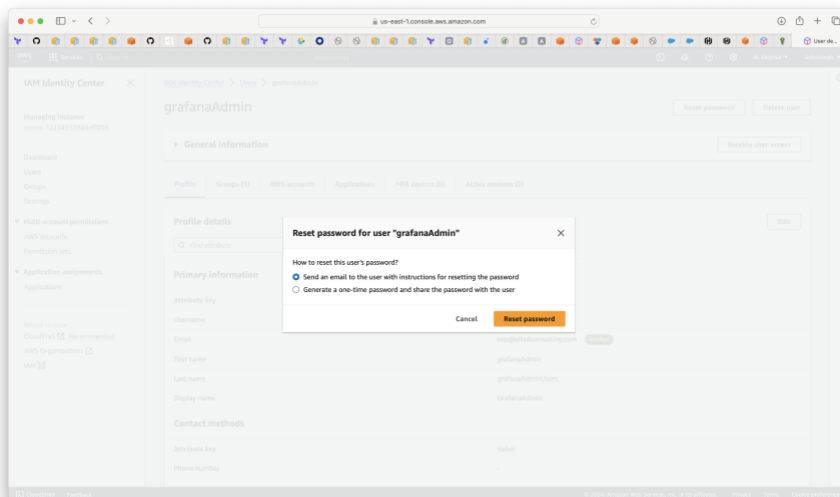
- 4.0.1 Logon to IAM Identity Center Console
- 4.0.2 On the left pane displayed IAM Identity Center window, click on Users
- 4.0.3 On the right pane displayed window, click on the grafanaAdmin user
- 4.0.4 On the right pane displayed window, click on the “send email verification link” button you will receive an email to verify your specified email address as shown below:



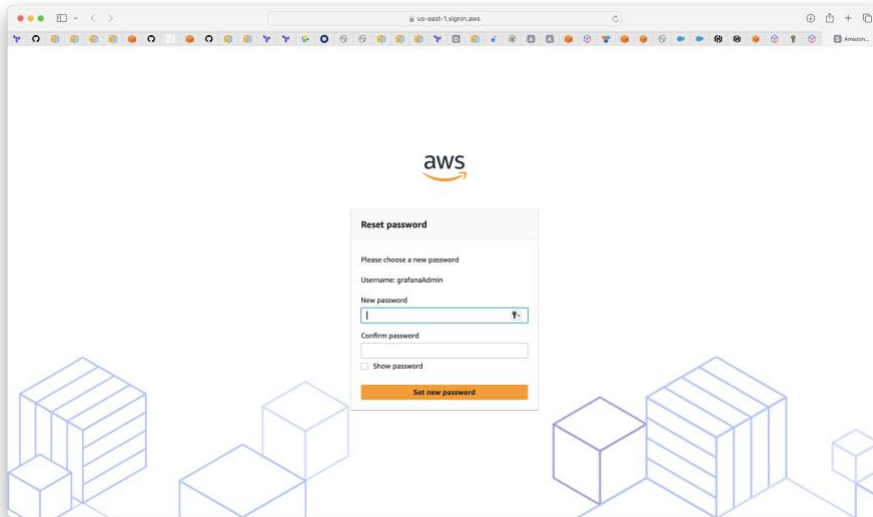
- 4.0.5 In the mail sent to your specified email address, click the button “Verify your email address”
- 4.0.6 Next, return to IAM identity Center Console, on the right pane, refresh your browser session to confirm your email address has been verified as shown below:



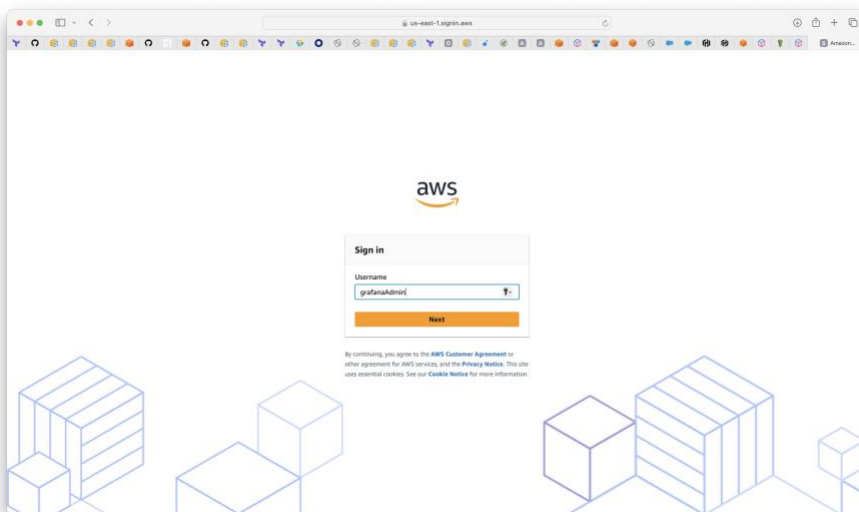
4.0.7 Next, in the same window on the right pane, click on “Reset password” button, a dialog box is displayed as show below, click on the “Reset password” button to send an email with instructions for resetting the user’s password



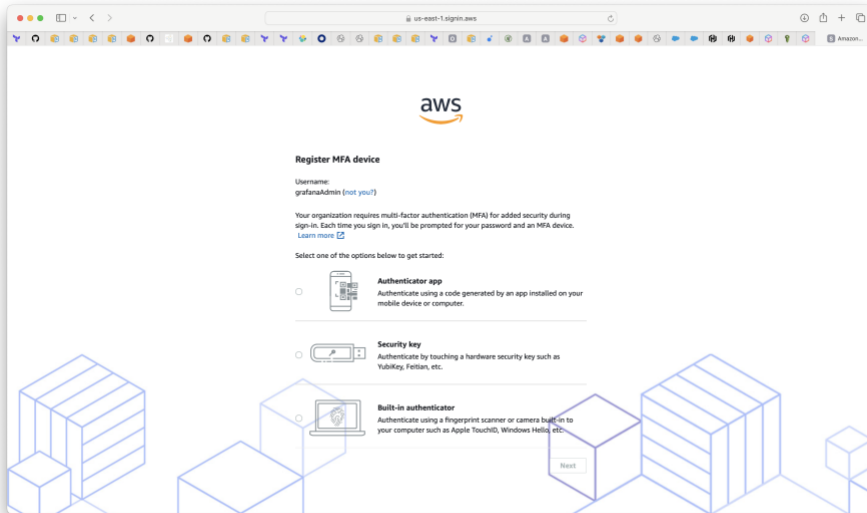
4.0.8 In the mail you received, click on the “Rest password” button, you will be redirected to a new browser page to set you password as shown below:



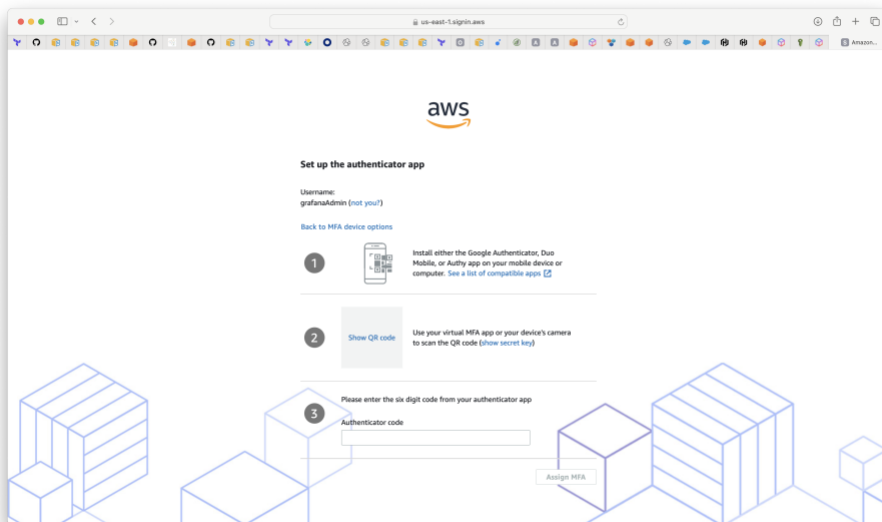
4.0.9 After setting your password, you will be redirected to sign-in page as shown below:



4.0.10 Click next and enter your new password, after entering your new password, you will be redirected to Register an MFA device as shown below:

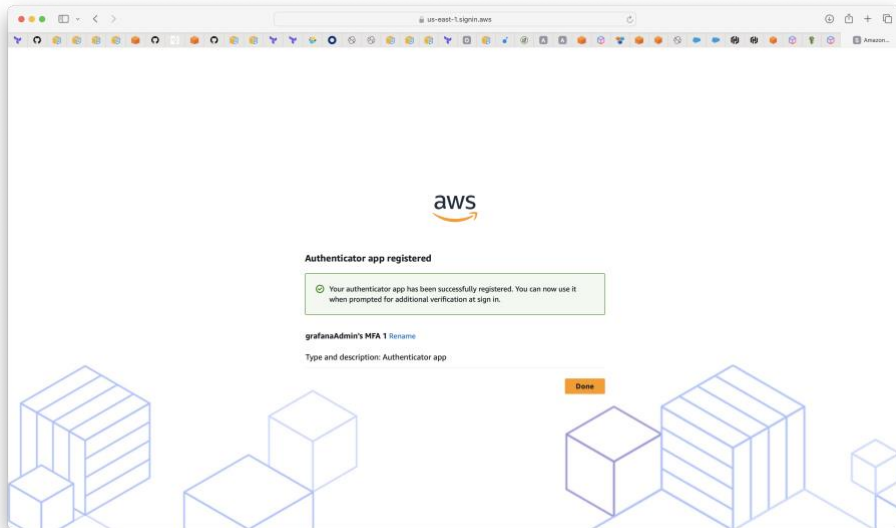


4.0.11 select the “Authenticator app” option and click next, a new page to Setup the authenticator app is displayed as shown below:

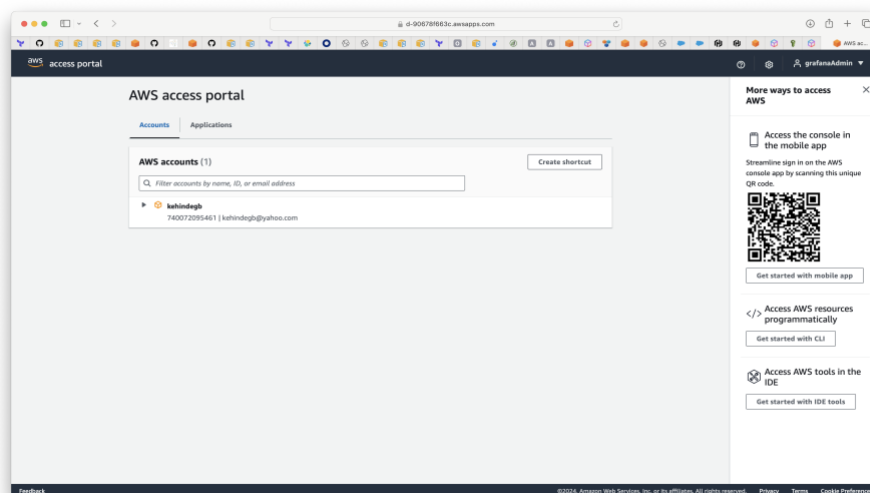


4.0.12 If you already have a virtual MFA device, then click option 2 to reveal the QR code. Scan the code using your virtual MFA device. The grafanaAdmin use will be configure.

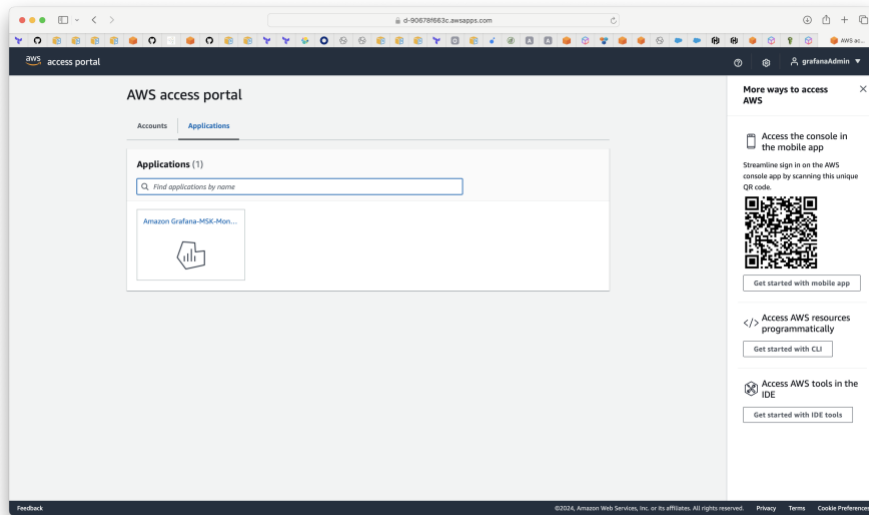
4.0.13 Next, enter the code provided by your virtual MFA device in the box, a new page is display indicating your Authenticator app is registered as shown below



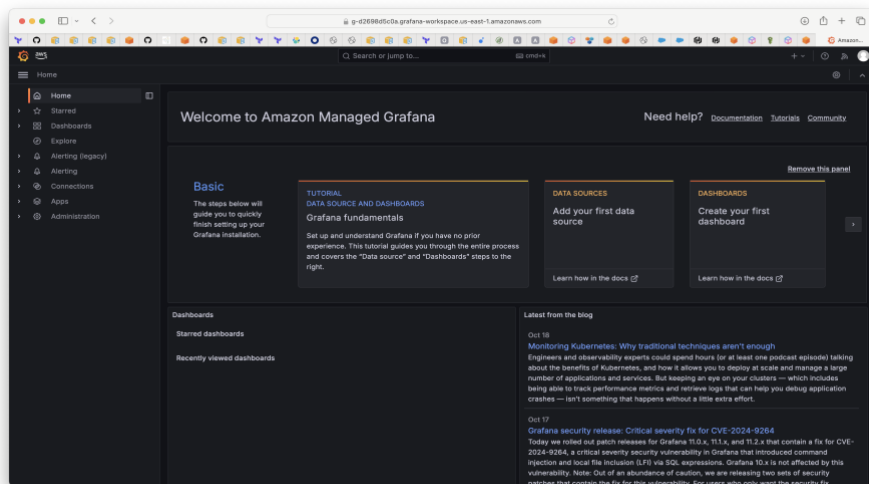
4.0.14 Next, click done and you will be redirected to the sign-in. Sign-in as “grafanaAdmin” user, after entering your password, you will be prompted to authenticate with MFA code. Once you supply the code, you will be redirected to “AWS Access Portal” page as shown below:



4.0.15 Next, click on the Applications tab, you will see your registered application as shown below:

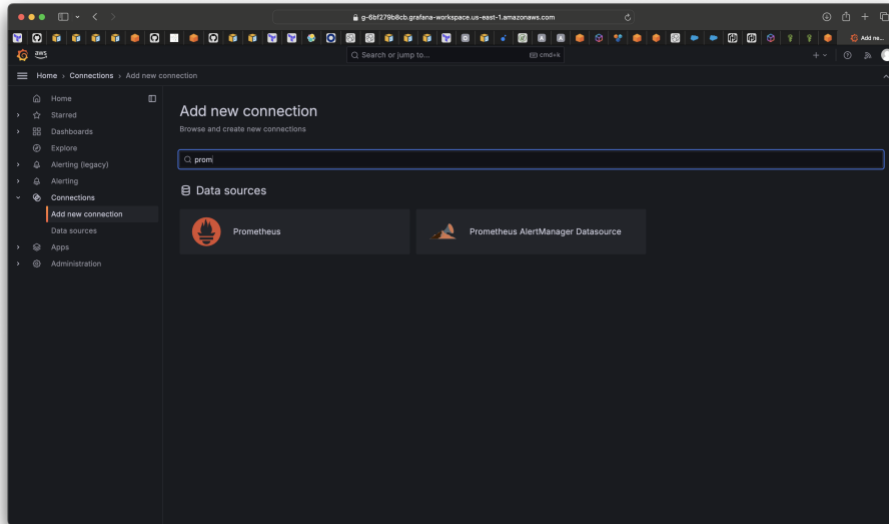


4.0.16 Next, click on your configured application and you will be redirected to the Amazon Managed Grafana Console as shown below:

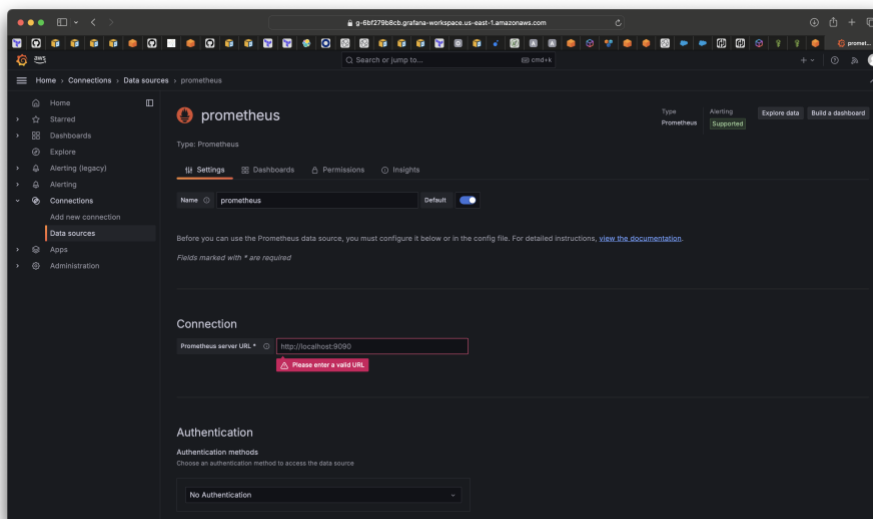


#### 4.0.17 Configure Prometheus Data Source Connection

At the displayed Grafana Web UI console, on the left pane, click on “Connections” and then click “Add new connection”, in the display “Add new connection” window on the right pane, start typing “prom” and the Prometheus data source is displayed as show below:



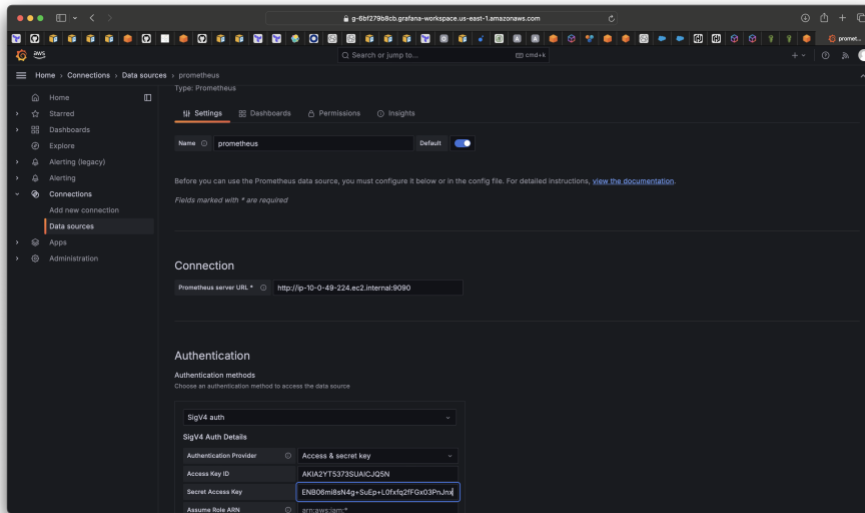
Click on Prometheus, and on the displayed window, click on “Add new data source button”, the window below is displayed



At the displayed window, under Connection, Prometheus server URL box, enter the private DNS name of your Kafka Client instance including the port at which Prometheus is running – 9090

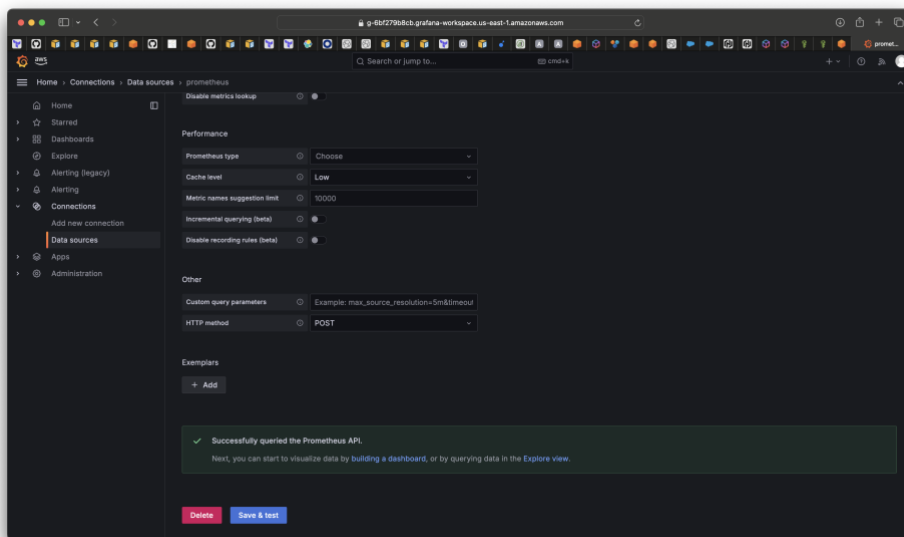
Still, in the same window above, under Authentication section, click on the drop-down list and select SigV4Auth, in the Authentication Provider drop down list, select Access & Secret Key. Next enter the value for Access Key ID and Secret Access Key (to get these values, logon to your Kafka Client Instance. The values are obtainable under the kafka user account AWS credentials)

Once these values have been populated, as show below:

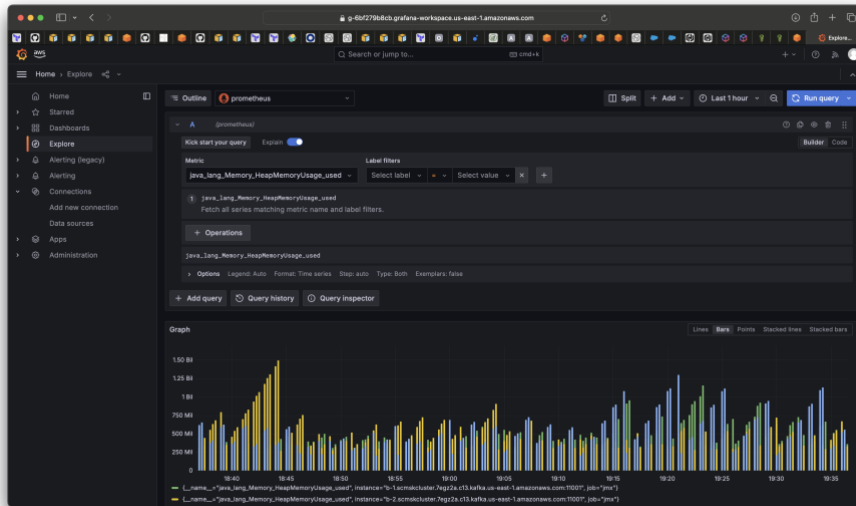


Next, scroll down to the bottom of the page and click on the button “Save & Test”

The window shown below is displayed, indicating a successful query of the Prometheus API



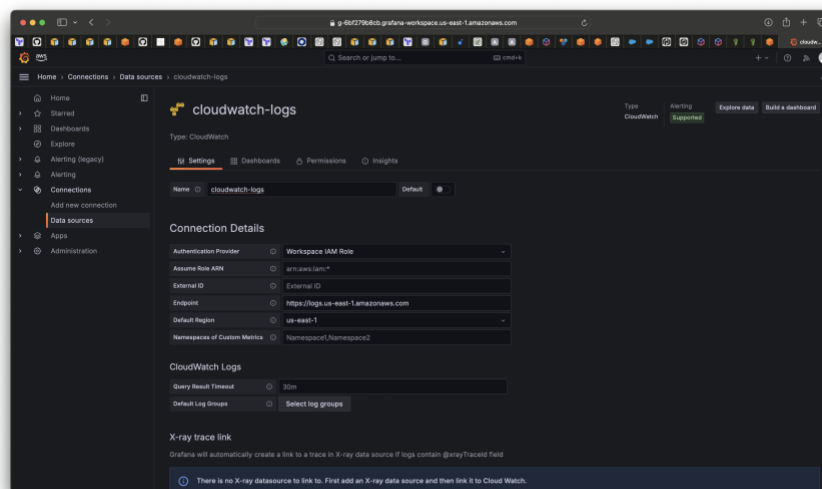
Next, on the left pane, click on Explore, on the displayed window, on the right pane, Prometheus is selected in the Outline section, under Metric, select are metric of your choosing and click on run query to display the visuals for that metric as shown below:



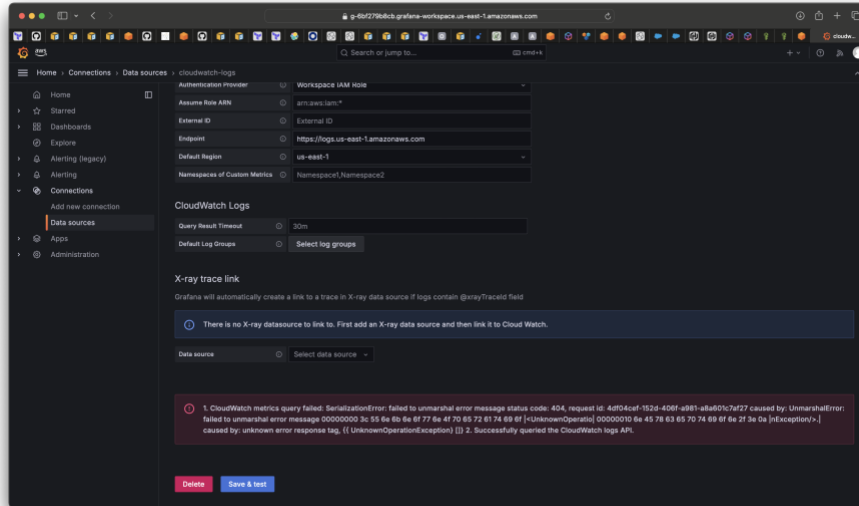
### Configure CloudWatch Data Source Connection

Follow the same process for Prometheus above but search for CloudWatch Data Source.

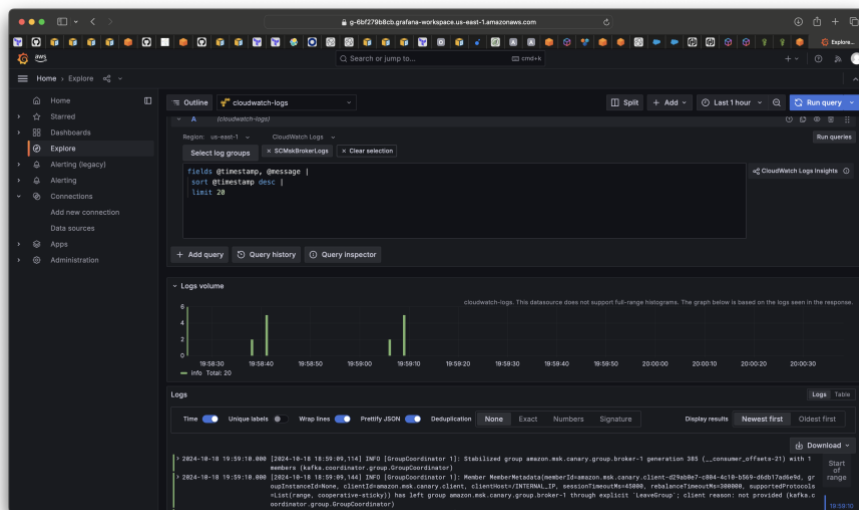
Setup CloudWatch logs Data Source as shown below:



Once the Connection Details section has been filled in, scroll down to bottom of the page and click on the 'Save & test' button. The window below shows that the Logs endpoint has been queried successfully

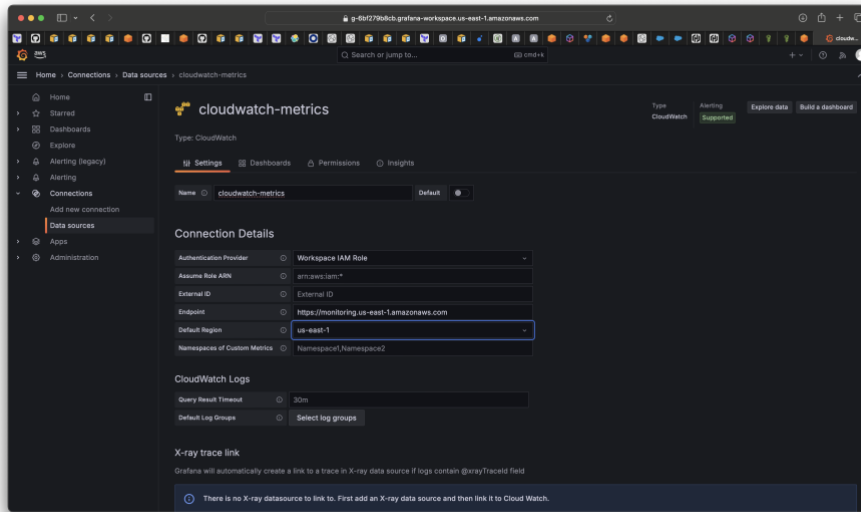


Next, Explore Logs, using the same process as before. Sample Log visualization is displayed as show below:

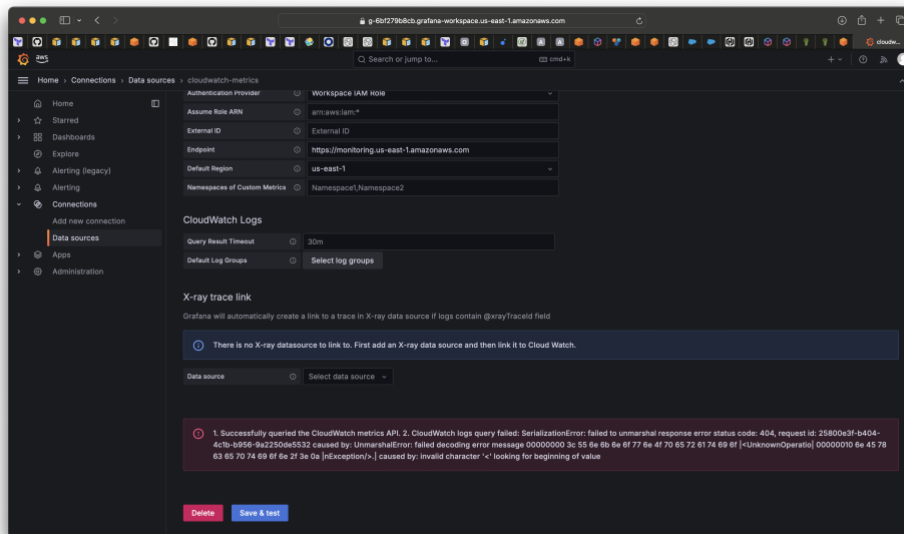


Next, repeat this same process for the monitoring end point to capture CloudWatch Metrics.

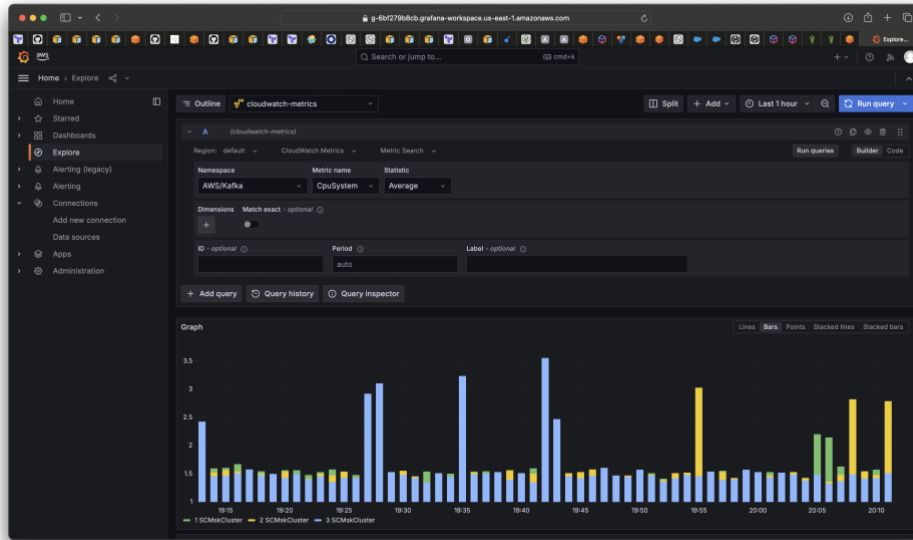
Setup CloudWatch Metrics Data Source as shown below:



Once the Connection Details section has been filled in, scroll down to bottom of the page and click on the "Save & test" button. The window below shows that the Metrics endpoint has been queried successfully



Next, explore Metric, Sample Kafka Metrics is displayed as shown below:



## Appendix A Resource Links

- \* <https://github.com/linkedin/cruise-control>
- \* <https://github.com/linkedin/cruise-control-ui>
- \* <https://github.com/prometheus/prometheus/releases>
- \* <https://github.com/aws-samples/amazon-msk-client-authentication>
- \* <https://github.com/adoptium/temurin8-binaries/releases>
- \* <https://dlcdn.apache.org/maven/maven-3/3.9.5/binaries/>
- \* <https://github.com/aws/aws-msk-iam-auth/releases>
- \* <https://archive.apache.org/dist/kafka/3.7.0/>

\*These represent the links from which all the tooling built together with the provisioned EC2 instance were sourced.

## Appendix B Customer Managed Policy

Below is the IAM policy to attach to the designated product Owner user.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iam:Get*", "iam:List*", "cloudformation:ValidateTemplate" ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateGroup",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:*GroupPolicy",
      "Resource": "arn:aws:iam::*:group/ssip*",
      "Condition": { "ArnLike": { "iam:PolicyARN": "arn:aws:iam::aws:policy/AWSMarketplace*" } }
    },
    {
      "Effect": "Allow",
      "Action": "iam:*GroupPolicy",
      "Resource": "arn:aws:iam::*:group/ssip*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:*Group",
      "Resource": "arn:aws:iam::*:group/ssip*"
    },
    {
      "Effect": "Allow",
      "Action": [ "iam:CreatePolicy", "iam:CreateRole", "iam:Tag*" ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:*RolePolicy",
      "Resource": "*",
      "Condition": { "ArnLike": { "iam:PolicyARN":
"arn:aws:iam::*:policy/SCLaunch*ManagedPolicy" } }
    },
    {
      "Effect": "Allow",
      "Action": "iam:Delete*",

```

```

    "Resource": [ "arn:aws:iam::*:policy/SCLaunch*ManagedPolicy",
"arn:aws:iam::*:role/SCLaunch-MSK*"]
  },
  {
    "Effect": "Allow",
    "Action": [ "cloudformation:CreateStack" ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [ "cloudformation:De*", "cloudformation:Get*", "cloudformation:List*" ],
    "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
  },
  {
    "Effect": "Allow",
    "Action": "cloudformation:CreateUploadBucket",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "cloudformation>DeleteStack",
    "Resource": "arn:aws:cloudformation:*:*:stack/ssip*/*"
  },
  {
    "Effect": "Allow",
    "Action": [ "cloudformation:Get*", "servicecatalog:Describe*", "servicecatalog:List*",
"servicecatalog:*Product*", "ssm:Describe*", "ssm:Get*", "config:Describe*" ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [ "servicecatalog:Describe*", "servicecatalog:List*",
"servicecatalog:*ProvisionedProduct*" ],
    "Resource": "*",
    "Condition": { "StringEquals": { "servicecatalog:userLevel": "self"}}
  },
  {
    "Effect": "Allow",
    "Action": "servicecatalog:*Portfolio*",
    "Resource": "arn:aws:catalog:*:*:portfolio/*"
  },
  {
    "Effect": "Allow",
    "Action": "s3:CreateBucket",
    "Resource": "arn:aws:s3:::cf-templates-*"
  },
  {
    "Effect": "Allow",
    "Action": "s3:List*",
    "Resource": "*"
  },
}

```

```

{
  "Effect": "Allow",
  "Action": [ "s3:List*", "s3:Get*" ],
  "Resource": "arn:aws:s3:::cf-templates-*"
},
{
  "Effect": "Allow",
  "Action": [ "s3:Put*", "s3:Get*", "s3:Delete*" ],
  "Resource": "arn:aws:s3:::cf-templates-*/*"
},
{
  "Effect": "Allow",
  "Action": [ "iam:CreateServiceLinkedRole", "iam:GetServiceLinkedRoleDeletionStatus",
"iam>DeleteServiceLinkedRole" ],
  "Resource": [ "arn:aws:iam::*:role/aws-service-
role/deployment.marketplace.amazonaws.com/AWSServiceRoleForMarketplaceDeployment" ],
  "Condition": { "StringLike": { "iam:AWSServiceName":
[ "deployment.marketplace.amazonaws.com" ] }}
},
{
  "Effect": "Allow",
  "Action": "account:ListRegions",
  "Resource": [ "arn:aws:account::*:account" ]
},
{
  "Effect": "Allow",
  "Action": [ "ec2:Describe*", "license-manager:Get*", "license-manager:List*", "license-
manager-user-subscriptions:List*", "notifications:List*", "servicecatalog:List*", "sns:List*" ],
  "Resource": "*"
}
]
}

```

## Appendix C Service Availability Regions

Region Name	Region	Available
US East (N. Virginia)	us-east-1	Yes
Europe (London)	eu-west-2	Yes
US West (Oregon)	us-west-2	Coming soon
Europe (Stockholm)	eu-north-1	Coming soon