SSIP-MSK PRODUCT ONBOARDING

SitadConsulting
ssip@sitadconsulting.com

Table of Contents

1.0 Introduction 1

Prerequisites 2

2.0 Software Bill of Material 3

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

3.0 Product Internal IAM resources 5

4.0 Product Personas 6

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

5.0 Post Provisioning tasks 22

Appendix A Resource Links 37

Appendix B Customer Managed Policy 38

Appendix C Service Availability Regions 41

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 other 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_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.

S/N	***Group Display Name***	***User Name***
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	https://docs.aws.amazon.com/msk/?icmpid=docs_homepage_analytics
2	Amazon Managed Grafana	https://docs.aws.amazon.com/grafana/?icmpid=docs_homepage_mgmtgov
3	AWS Private Certificate Authority	https://docs.aws.amazon.com/privateca/?icmpid=docs_homepage_crypto
4	AWS IAM Identity Center	https://docs.aws.amazon.com/singlesignon/?icmpid=docs_homepage_security
5	Amazon EC2	https://docs.aws.amazon.com/ec2/?icmpid=docs_homepage_featuredsvcs
6	Amazon CloudWatch Logs	https://docs.aws.amazon.com/cloudwatch/
7	AWS Key Management Service	https://docs.aws.amazon.com/kms/

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

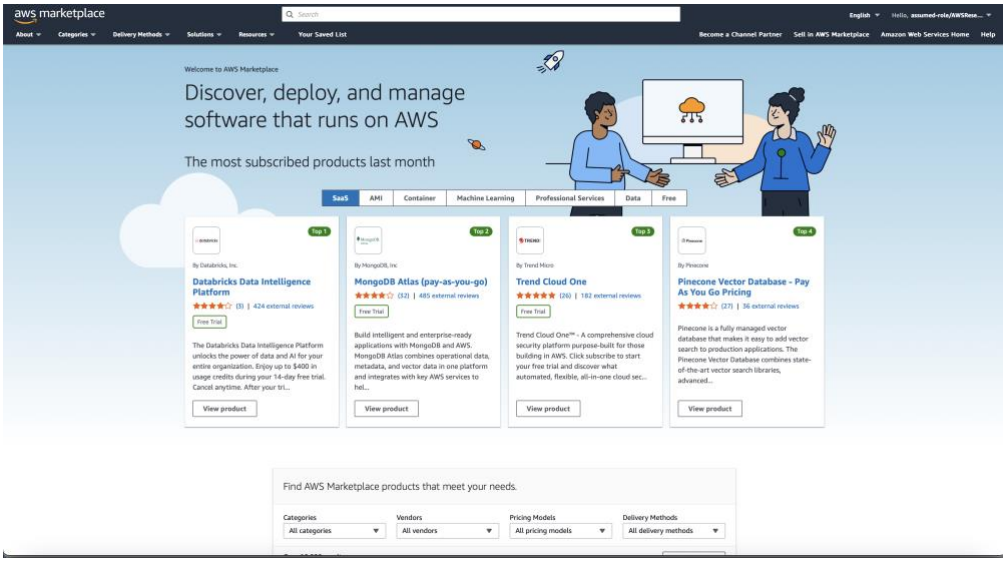
There are mainly two product personas. The product Owner and the product Enduser. These are designated IAM users already existing within the customer account. The table below set out their function and permission association.

S/N	***Persona***	***Responsible for***	***Permission Assignment***
1	Owner	1. Subscribing to the product on AWS marketplace 2. Launching CloudFormation template that deploys product dependent IAM resources into customer's account 3. Adding product to Service Catalog Portfolio. 4. Sharing product to Endusers	1. Designated user to be assigned the following AWS Managed policy: ***AWSMarketplaceManageSubscriptions*** 2. In addition, ***a customer managed policy with content provided in Appendix B must be attached to the user*** (this policy allows the deployment of product dependent IAM resources into customers account)
2	Enduser	1. Launching the product.	Designated user ***must be added to IAM group – ssipmskgrp*** (this ***IAM group- ssipmskgrp*** 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.

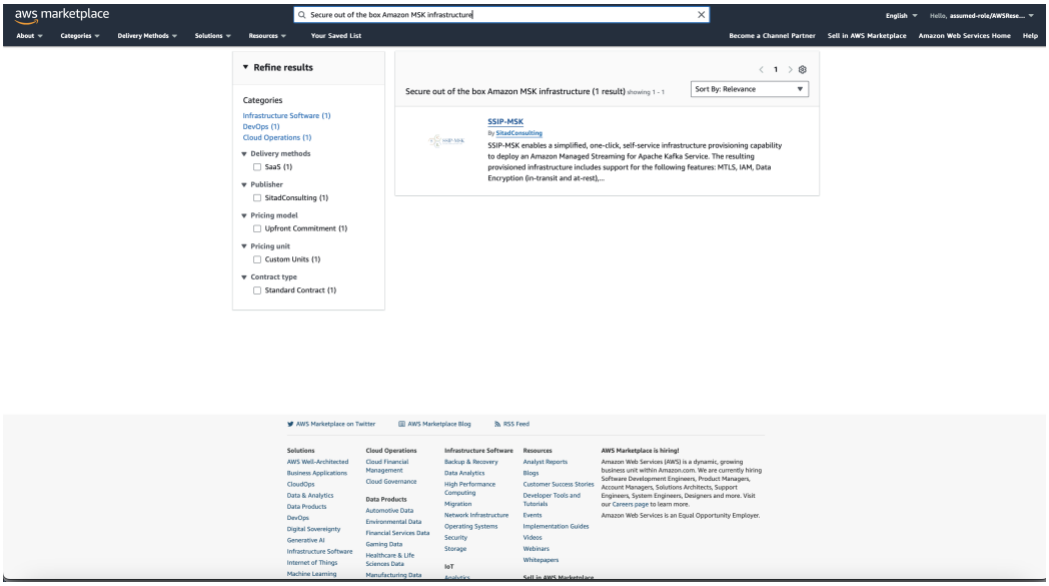
Please note that the product is going to be shared with the subscribing account, so please ensure that this is the account you intend to have the product deploy into.

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:

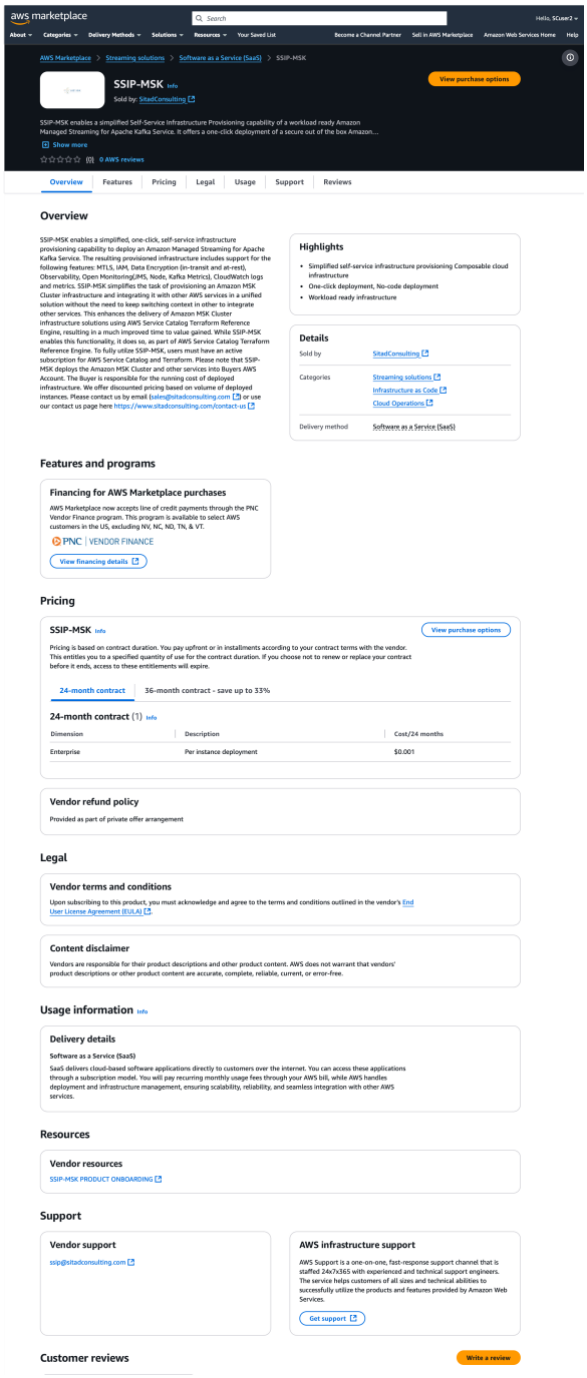


3. At the displayed Product Owner logon to ***AWS Marketplace***, in the search box, type in any of the following search phrase to discover our service offering:
   1. Secure out of the box Amazon MSK infrastructure
   2. Workload ready Amazon Managed Streaming for Apache Kafka service
   3. Simplified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

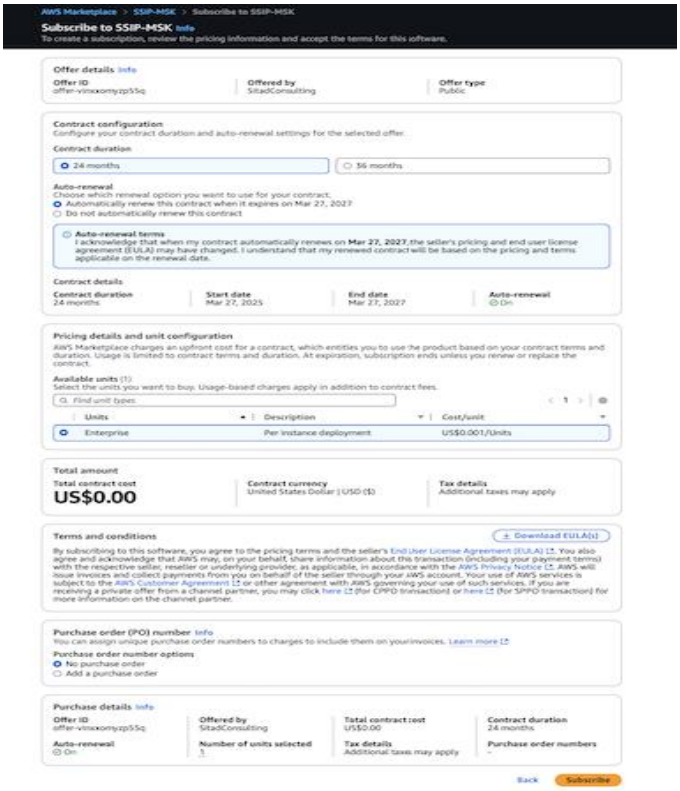
   Our service offering ***SSIP-MSK*** is displayed as shown below:



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:



5. 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:



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 Inbox - Yahoo! 14:49

You accepted an AWS Marketplace offer

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: SitadConsulting

Product details
Product name: SSIP-MSK
Product ID: prod-vhdrvzlia6rt2

Offer details
Offer name: Offer created on 2024-10-29T15:20:33.498Z
Offer ID: offer-vinxxomyzp55q

Agreement details
Agreement ID: agmt-c234s222mrsfaqh1lyt3k16vq
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)

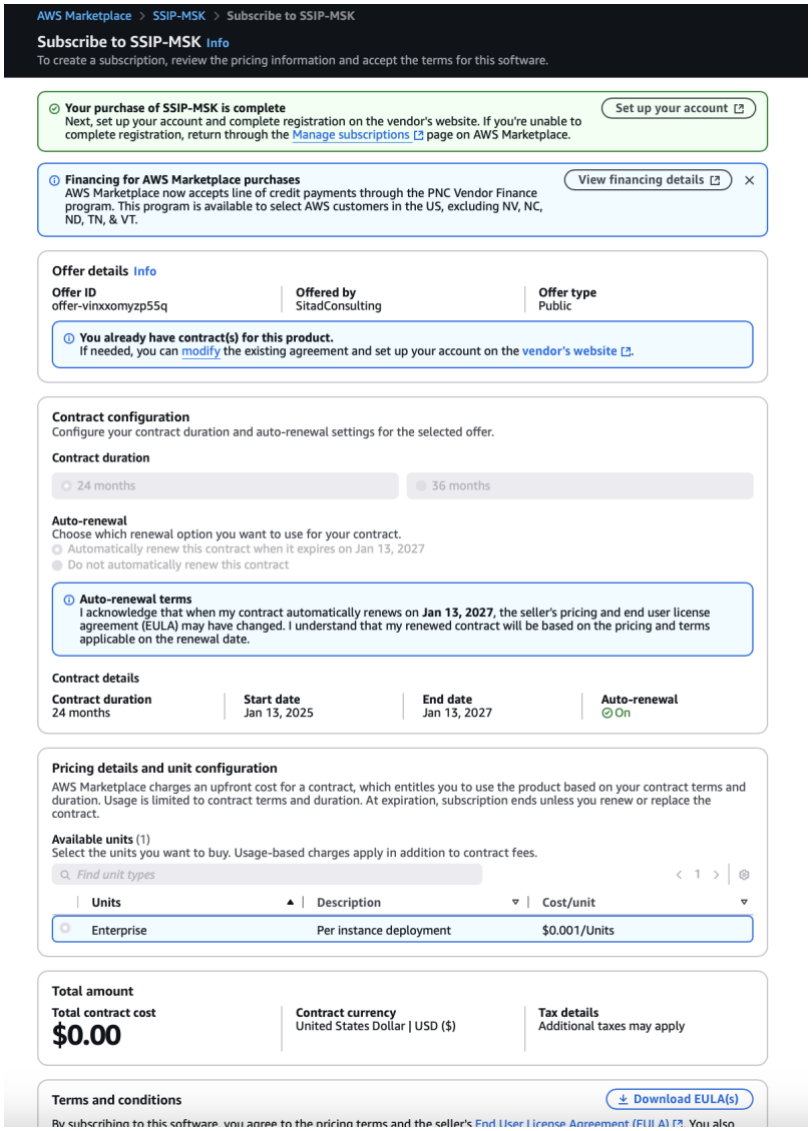
For SaaS products, register with the seller's website by visiting the procurement page to set up your account and start using the product. For more details, review our Buyers guide.

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.

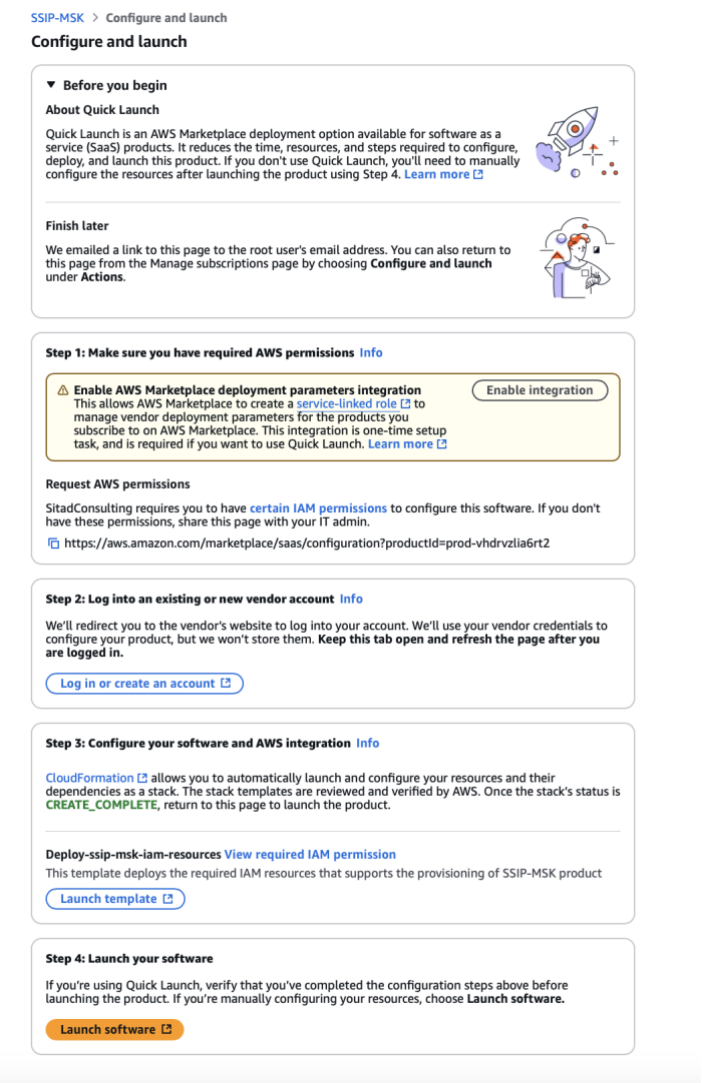
To review details of your agreement, visit the Manage subscriptions page. For agreements on data products, visit the AWS Data Exchange console.

If you have any questions about your agreement or need assistance, visit AWS Support.

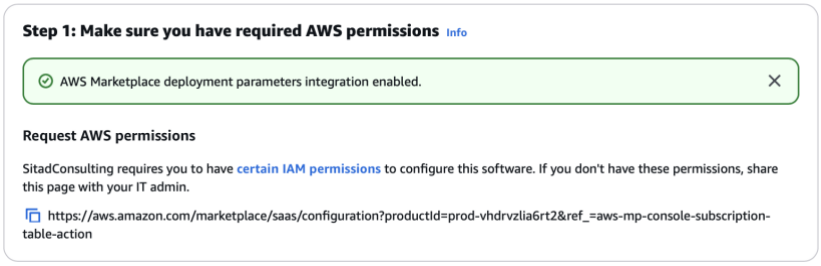
Regards,
The AWS Marketplace Team



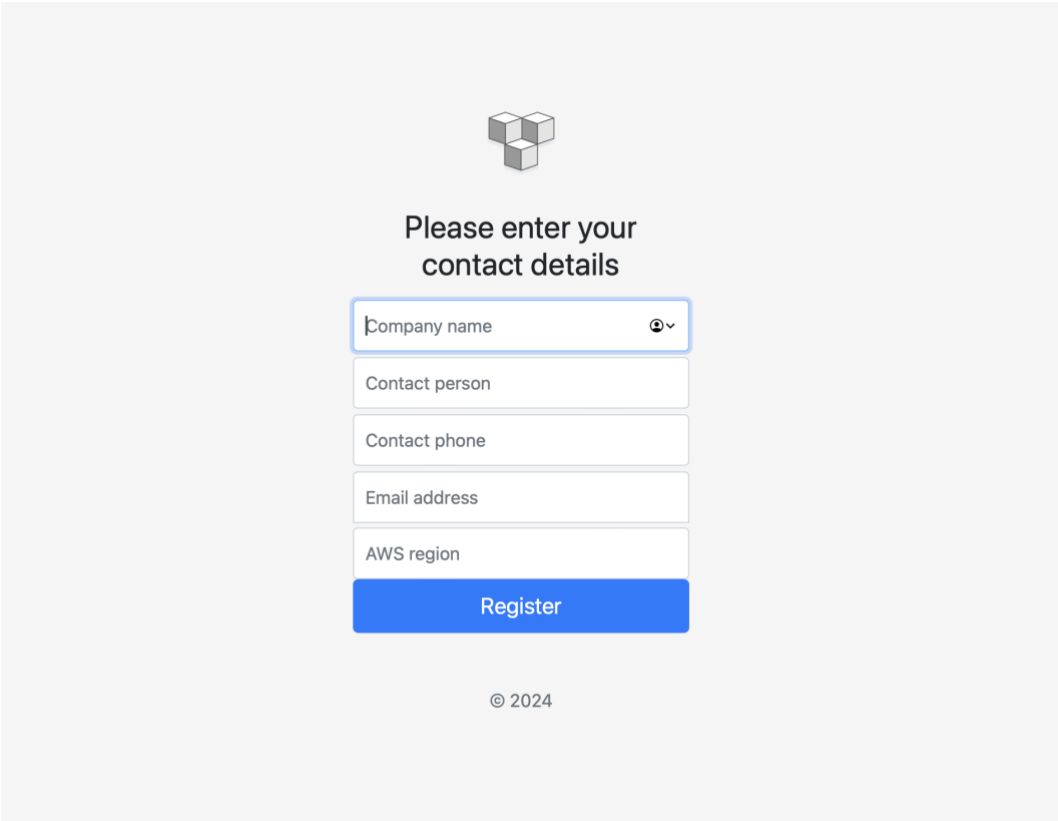
7. At the displayed ***Purchase completion*** page, in the green box, click on ***Set up your account*** button, you will be redirected to Quick Launch page as shown below:



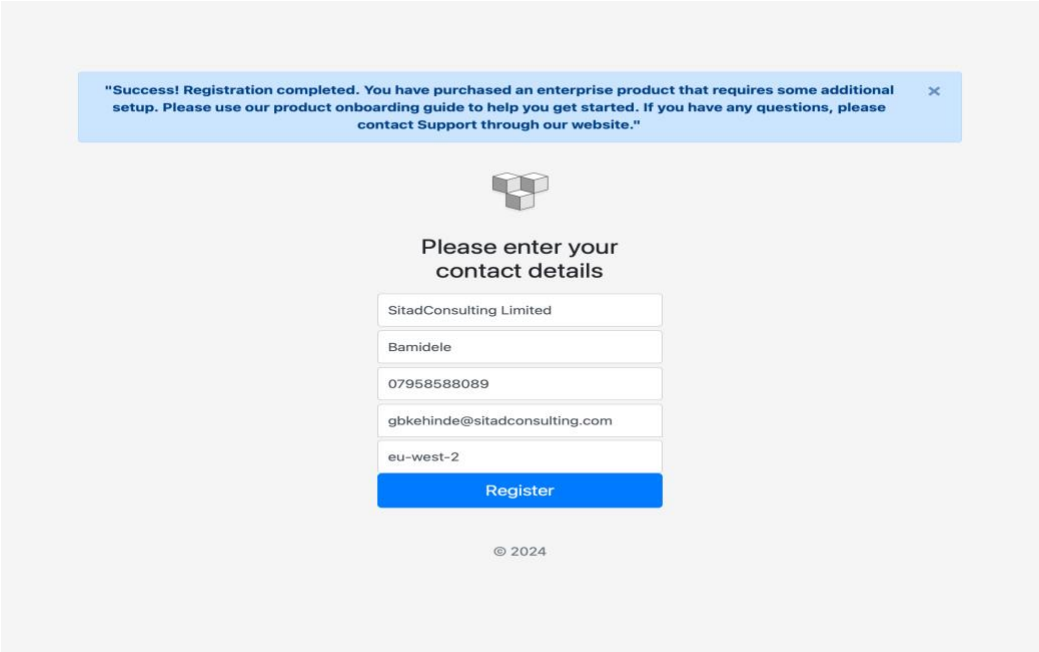
8. At the displayed ***Configure and launch*** page, follow the on-screen instruction and complete Step 1, 2 and 3
9. Step 1, click on ***Enable integration,*** once integration is enabled you see in a green bar the statement ***AWS Marketplace deployment parameters integration enabled***, as shown below:



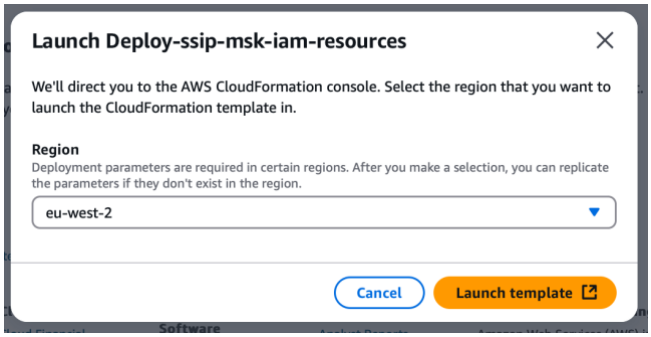
10. Step 2, click on ***Log in or create account***, you will be redirected to the account creation page as shown below:



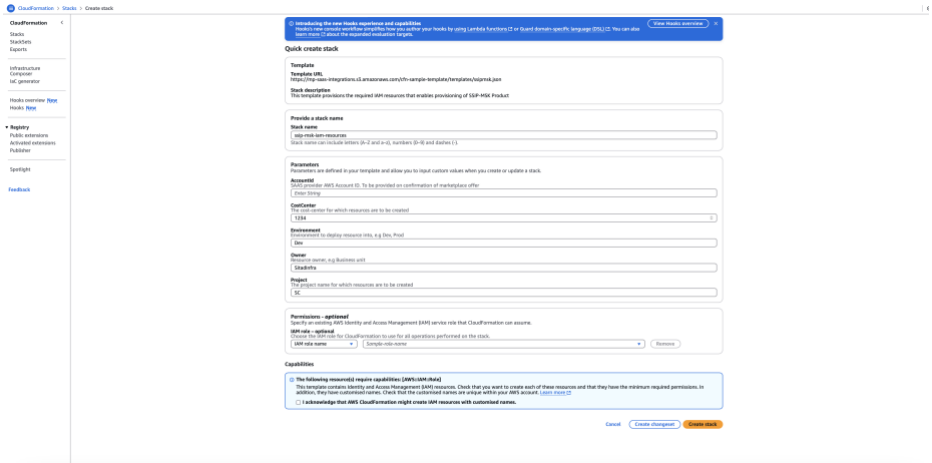
11. At the displayed account creation page, ***please note that each field must be filled in with correct information to capture the details of the product Owner (We can only grant access to the product when all fields have been entered correctly)*** and click ***Register*** button, a successful registration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



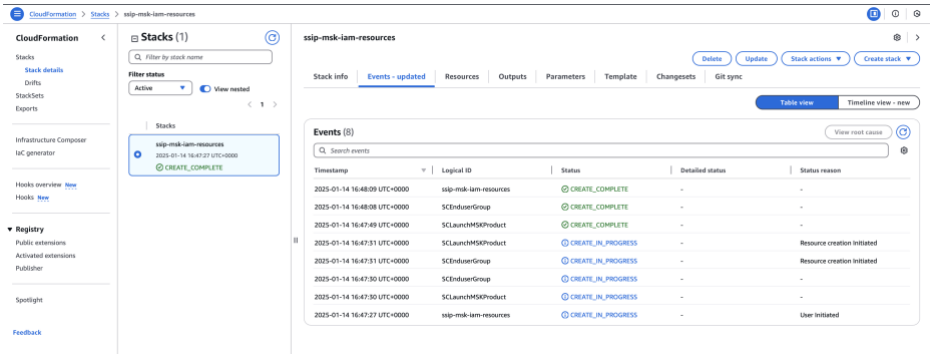
12. Step 3, click on ***Launch template*** button to deploy product dependent IAM resources, follow the on-screen prompts, at the displayed Launch ***Deploy-ssip-msk-iam-resources*** screen, shown below, use the drop-down arrow to choose the AWS region you specified in step 12 above, click Launch template,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

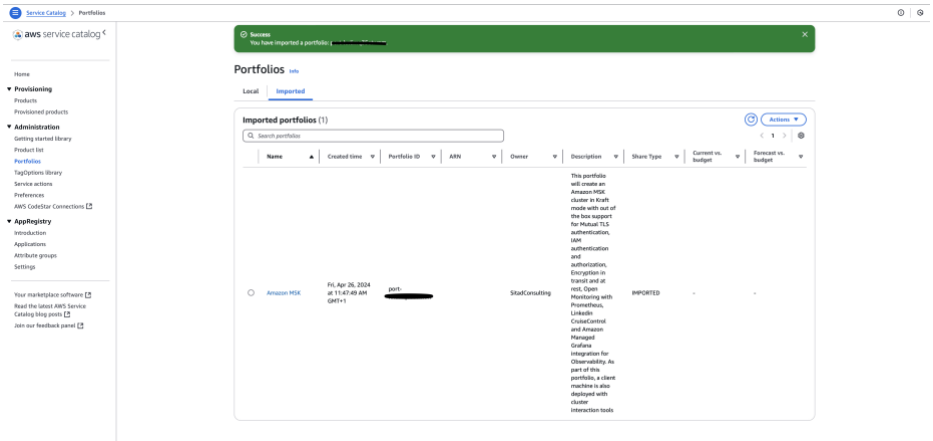


14. After a few minutes the stack is created as shown below:



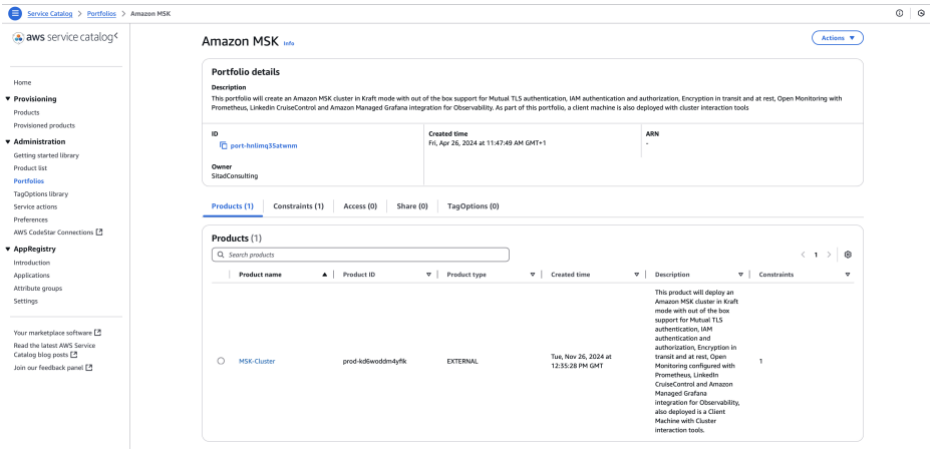
4.0.2 Adding product to Service Catalog Portfolio.

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:

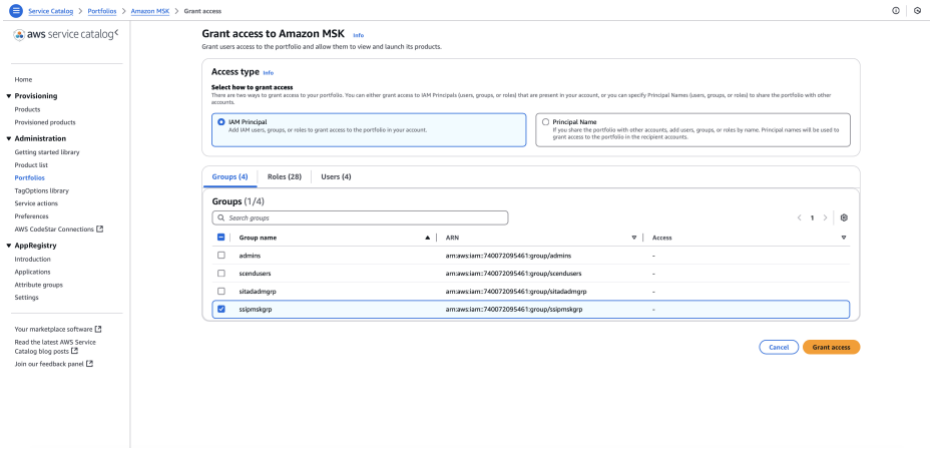


4.0.3 Sharing the product

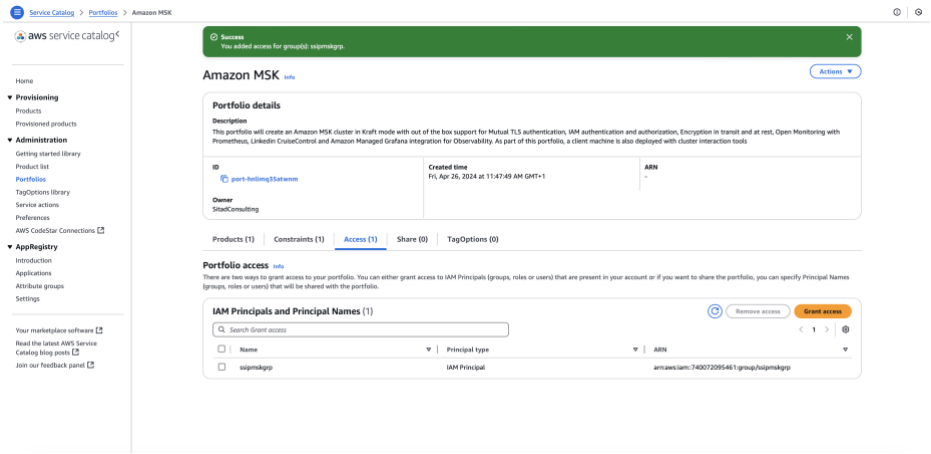
1. As the product Owner, and logon on to Service Catalog, on the left-pane under ***Administration***, click on ***Portfolios***, at the displayed right-pane ***Portfolios*** page click on the Imported tab, next click on ***Amazon MSK*** portfolio, the portfolio will be displayed as shown below:



2. 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:



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

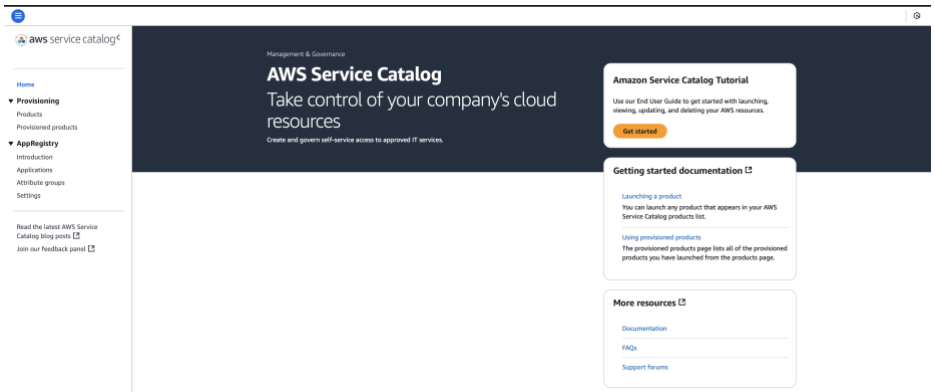


4.0.4 Launching the product.

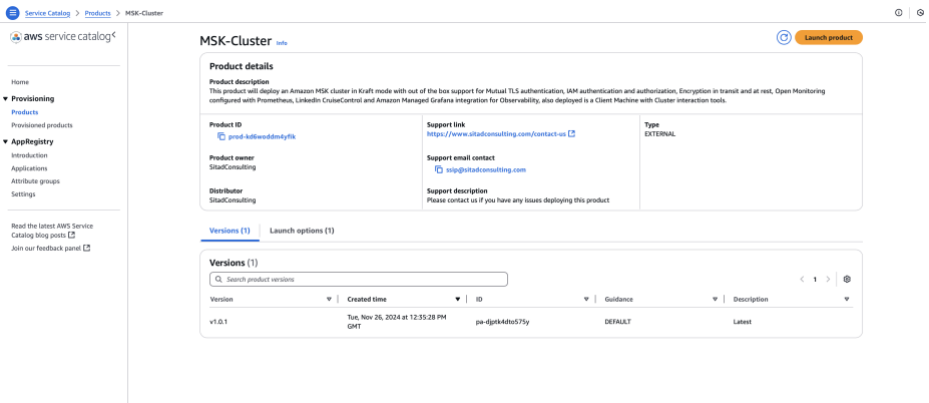
Before attempting to launch the product, please ensure that the product Owner has completed section 4.0.1, 4.0.2 and 4.0.3 above. In section 4.0.1, the CloudFormation template deploys the dependent IAM resources required to ensure a successful product launch. The table below describes the IAM resources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

S/N	***IAM Resources***	***Name***	***Usage***
1	IAM Group	ssipmskgrp	Designated ***product Enduser must be added to this group by the customer,*** 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

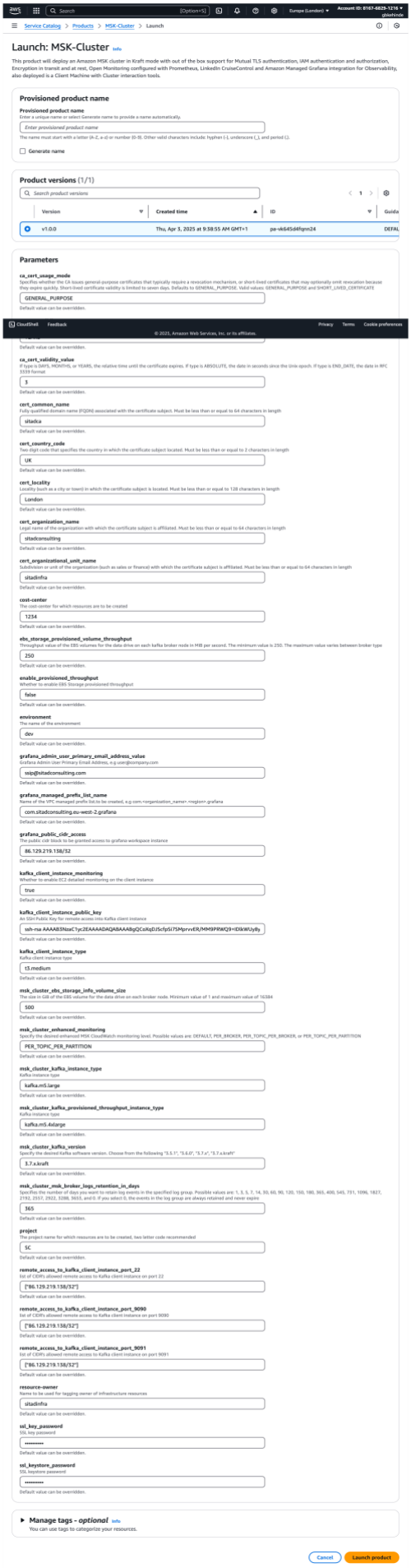
1. As product Enduser, logon to AWS console and search for *Service Catalog*, then click on the displayed Service Catalog, you will be redirected to the page shown below



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:



Service Catalog > Products > MSK-Cluster > Launch

Launch: MSK-Cluster Info

This product will deploy an Amazon MSK cluster in Krafft 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, LinkedIn CruiseControl and Amazon Managed Grafana integration for Observability, also deployed is a Client Machine with Cluster interaction tools.

Provisioned product name

Provisioned product name
Enter a unique name or select Generate name to provide a name automatically.

Enter provisioned product name

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)

Search product versions

Version	Created time	ID	Guida
v1.0.0	Thu, Apr 3, 2025 at 9:58:55 AM GMT+1	pa-vk645d4fqnm24	DEFAU

Parameters

ca_cert_usage_mode
Specifies whether the CA issues general-purpose certificates that typically require a revocation mechanism, or short-lived certificates that may optionally omit revocation because they expire quickly. Short-lived certificate validity is limited to seven days. Defaults to GENERAL_PURPOSE. Valid values: GENERAL_PURPOSE and SHORT_LIVED_CERTIFICATE
GENERAL_PURPOSE
Default value can be overridden.

CloudShell Feedback Privacy Terms Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.

Default value can be overridden.

ca_cert_validity_value
If type is DAYS, MONTHS, or YEARS, the relative time until the certificate expires. If type is ABSOLUTE, the date in seconds since the Unix epoch. If type is END_DATE, the date in RFC 3339 format.
3
Default value can be overridden.

cert_common_name
Fully qualified domain name (FQDN) associated with the certificate subject. Must be less than or equal to 64 characters in length
sitadca
Default value can be overridden.

cert_country_code
Two digit code that specifies the country in which the certificate subject located. Must be less than or equal to 2 characters in length
UK
Default value can be overridden.

cert_locality
Locality (such as a city or town) in which the certificate subject is located. Must be less than or equal to 128 characters in length
London
Default value can be overridden.

cert_organization_name
Legal name of the organization with which the certificate subject is affiliated. Must be less than or equal to 64 characters in length
sitadconsulting
Default value can be overridden.

cert_organizational_unit_name
Subdivision or unit of the organization (such as sales or finance) with which the certificate subject is affiliated. Must be less than or equal to 64 characters in length
sitadinfra
Default value can be overridden.

cost-center
The cost-center for which resources are to be created
1234
Default value can be overridden.

ebs_storage_provisioned_volume_throughput
Throughput value of the EBS volumes for the data drive on each kafka broker node in MB per second. The minimum value is 250. The maximum value varies between broker type
250
Default value can be overridden.

enable_provisioned_throughput
Whether to enable EBS Storage provisioned throughput
false
Default value can be overridden.

environment
The name of the environment
dev
Default value can be overridden.

grafana_admin_user_primary_email_address_value
Grafana Admin User Primary Email Address, e.g user@company.com
ssip@sitadconsulting.com
Default value can be overridden.

grafana_managed_prefix_list_name
Name of the VPC managed prefix list.to be created, e.g com.<organization_name>.<region>.grafana
com.sitadconsulting.eu-west-2.grafana
Default value can be overridden.

grafana_public_cidr_access
The public cidr block to be granted access to grafana workspace instance
86.129.219.158/32
Default value can be overridden.

kafka_client_instance_monitoring
Whether to enable EC2 detailed monitoring on the client instance
true
Default value can be overridden.

kafka_client_instance_public_key
An SSH Public Key for remote access into Kafka client instance
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCcXqDJSc/pSi75MprrvER/MM9PRWQ9+tDlkWUy8y
Default value can be overridden.

kafka_client_instance_type
Kafka client instance type
t3.medium
Default value can be overridden.

msk_cluster_ebs_storage_info_volume_size
The size in GiB of the EBS volume for the data drive on each broker node. Minimum value of 1 and maximum value of 16384
500
Default value can be overridden.

msk_cluster_enhanced_monitoring
Specify the desired enhanced MSK CloudWatch monitoring level. Possible values are: DEFAULT, PER_BROKER, PER_TOPIC_PER_BROKER, or PER_TOPIC_PER_PARTITION
PER_TOPIC_PER_PARTITION
Default value can be overridden.

msk_cluster_kafka_instance_type
Kafka instance type
kafka.m5.large
Default value can be overridden.

msk_cluster_kafka_provisioned_throughput_instance_type
Kafka instance type
kafka.m5.4xlarge
Default value can be overridden.

msk_cluster_kafka_version
Specify the desired Kafka software version. Choose from the following '3.5.1", '3.6.0", '3.7.x", '3.7.x.kraft'
3.7.x.kraft
Default value can be overridden.

msk_cluster_msk_broker_logs_retention_in_days
Specifies the number of days you want to retain log events in the specified log group. Possible values are: 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1096, 1827, 2192, 2557, 2922, 3288, 3653, and 0. If you select 0, the events in the log group are always retained and never expire
365
Default value can be overridden.

project
The project name for which resources are to be created, two letter code recommended
SC
Default value can be overridden.

remote_access_to_kafka_client_instance_port_22
list of CIDR's allowed remote access to Kafka client instance on port 22
["86.129.219.158/32"]
Default value can be overridden.

remote_access_to_kafka_client_instance_port_9090
list of CIDR's allowed remote access to Kafka client instance on port 9090
["86.129.219.158/32"]
Default value can be overridden.

remote_access_to_kafka_client_instance_port_9091
list of CIDR's allowed remote access to Kafka client instance on port 9091
["86.129.219.158/32"]
Default value can be overridden.

resource-owner
Name to be used for tagging owner of Infrastructure resources
sitadinfra
Default value can be overridden.

ssl_key_password
SSL key password
••••••••••
Default value can be overridden.

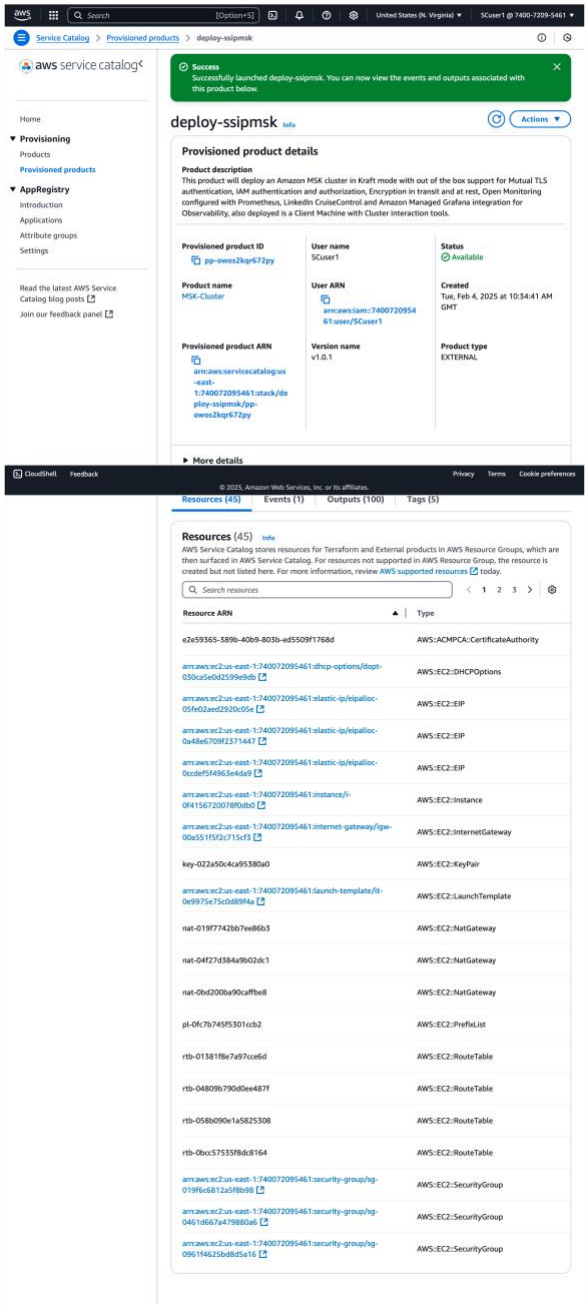
ssl_keystore_password
SSL keystore password
••••••••••
Default value can be overridden.

▸ **Manage tags - *optional*** Info
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


Service Catalog > Provisioned products > deploy-ssipmsk
aws service catalog
Home
Provisioning
Products
Provisioned products
AppRegistry
Introduction
Applications
Attribute groups
Settings
Read the latest AWS Service Catalog blog posts
Join our feedback panel
Success
Successfully launched deploy-ssipmsk. You can now view the events and outputs associated with this product below.
deploy-ssipmsk
Actions
Provisioned product details
Product description
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, LinkedIn CruiseControl and Amazon Managed Grafana integration for Observability, also deployed is a Client Machine with Cluster interaction tools.
Provisioned product ID
pp-owos2kqr672py
User name
SCuser1
Status
Available
Product name
MSK-Cluster
User ARN
arn:aws:iam::740072095461:user/SCuser1
Created
Tue, Feb 4, 2025 at 10:34:41 AM GMT
Provisioned product ARN
arn:aws:servicecatalog:us-east-1:740072095461:stack/deploy-ssipmsk/pp-owos2kqr672py
Version name
v1.0.1
Product type
EXTERNAL
More details
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2025, Amazon Web Services, Inc. or its affiliates.
Resources (45)
Events (1)
Outputs (100)
Tags (5)
Resources (45)
AWS Service Catalog stores resources for Terraform and External products in AWS Resource Groups, which are then surfaced in AWS Service Catalog. For resources not supported in AWS Resource Group, the resource is created but not listed here. For more information, review AWS supported resources today.
Search resources
Resource ARN
Type
e2e5936S-389b-40b9-803b-ed5509f1768d
AWS::ACMPCA::CertificateAuthority
arn:aws:ec2:us-east-1:740072095461:dhcp-options/dopt-030ca5e0d2599e9db
AWS::EC2::DHCPOptions
arn:aws:ec2:us-east-1:740072095461:elastic-ip/eipalloc-05fe02aed2920c05e
AWS::EC2::EIP
arn:aws:ec2:us-east-1:740072095461:elastic-ip/eipalloc-0a48e6709f2571447
AWS::EC2::EIP
arn:aws:ec2:us-east-1:740072095461:elastic-ip/eipalloc-0ccdef5f4963e4da9
AWS::EC2::EIP
arn:aws:ec2:us-east-1:740072095461:instance/i-0f415672007f80db0
AWS::EC2::Instance
arn:aws:ec2:us-east-1:740072095461:internet-gateway/igw-00a551f5f2c715cf3
AWS::EC2::InternetGateway
key-022a50c4ca95380a0
AWS::EC2::KeyPair
arn:aws:ec2:us-east-1:740072095461:launch-template/lt-0e9975e75c0d89f4a
AWS::EC2::LaunchTemplate
nat-019f7742bb7ee86b3
AWS::EC2::NatGateway
nat-04f27d384a9b02dc1
AWS::EC2::NatGateway
nat-0bd200ba90caffbe8
AWS::EC2::NatGateway
pl-0fc7b745f5301ccb2
AWS::EC2::PrefixList
rtb-01381f8e7a97cce6d
AWS::EC2::RouteTable
rtb-04809b790d0ee487f
AWS::EC2::RouteTable
rtb-058b090e1a5825308
AWS::EC2::RouteTable
rtb-0bcc57535f8dc8164
AWS::EC2::RouteTable
arn:aws:ec2:us-east-1:740072095461:security-group/sg-019f6c6812a5f8b98
AWS::EC2::SecurityGroup
arn:aws:ec2:us-east-1:740072095461:security-group/sg-0461d667a479880a6
AWS::EC2::SecurityGroup
arn:aws:ec2:us-east-1:740072095461:security-group/sg-0961f4625bd8d5a16
AWS::EC2::SecurityGroup

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

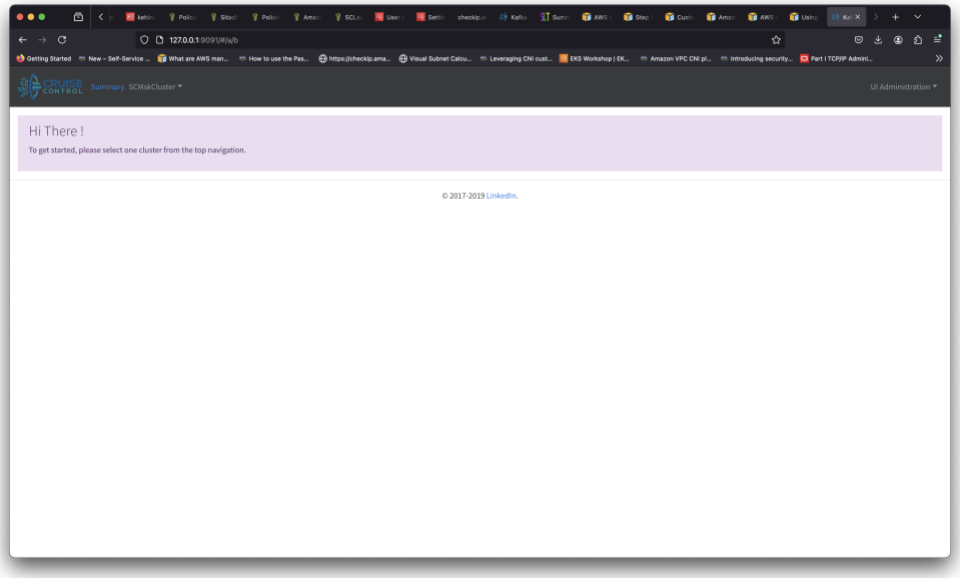
Press the return key, a tunnel session is established as shown below:

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.

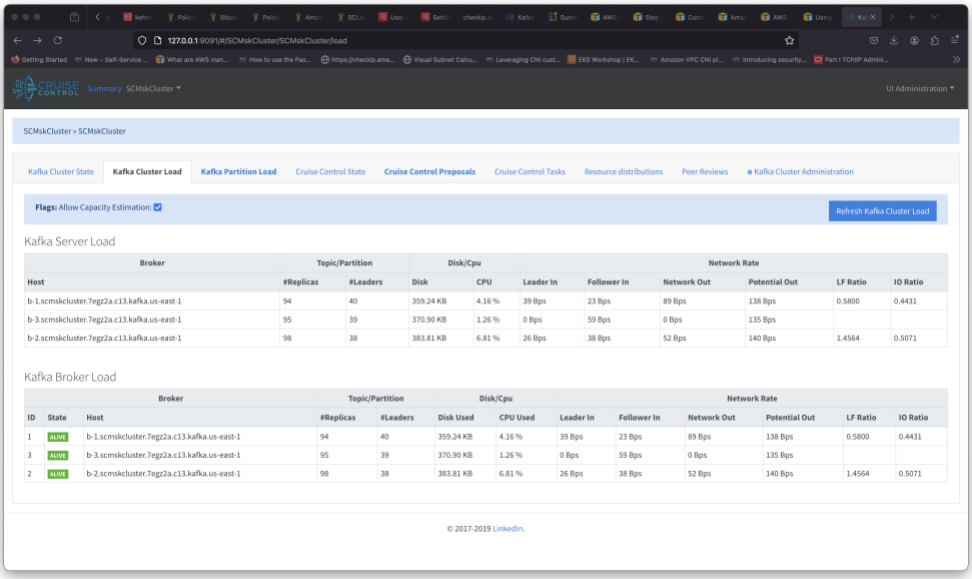
```
  ,     #_
  ~\_  ####_        Amazon Linux 2023
 ~~  \_#####\
```

```
~~    \###|
~~     \#/ ___   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.



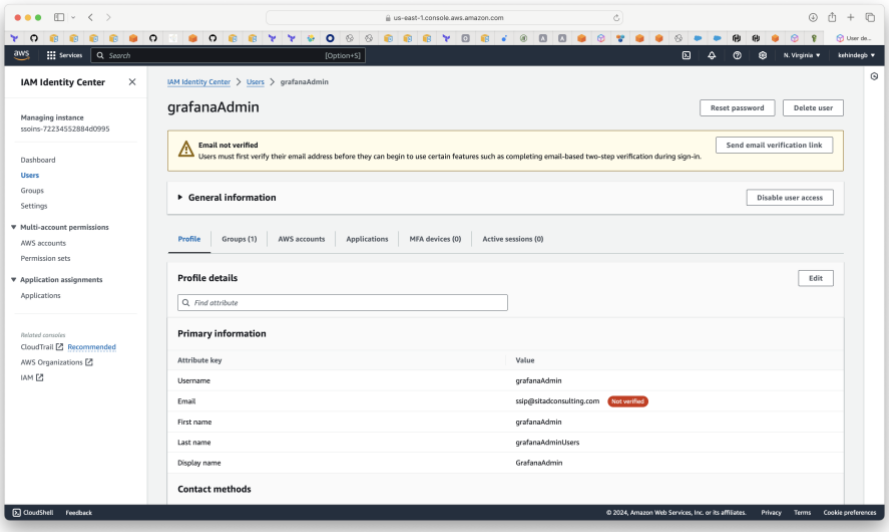
Accessing Amazon Managed Grafana Console

4.0.1 Logon to IAM Identity Center Console

4.0.2 On the left pane displayed IAM Identity Center window, click on Users

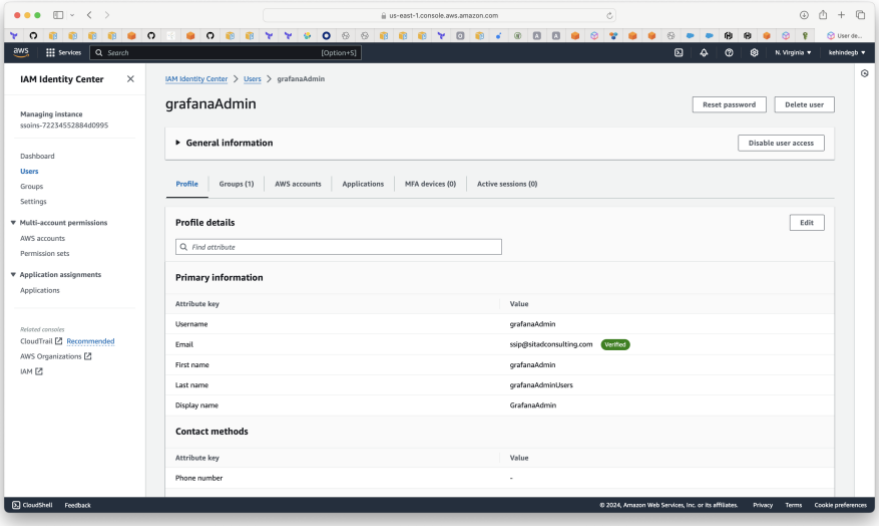
4.0.3 On the right pane displayed window, click on the grafanaAdmin user

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:

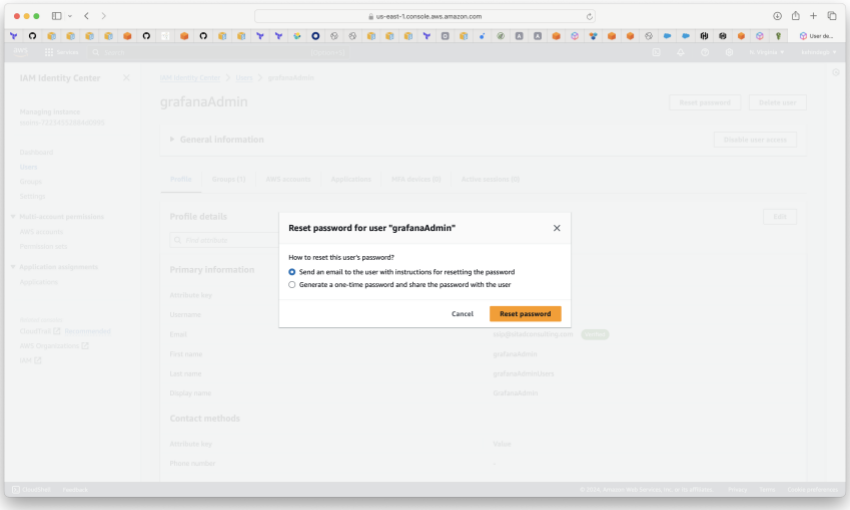


4.0.5 In the mail sent to your specified email address, click the button “Verify your email address”

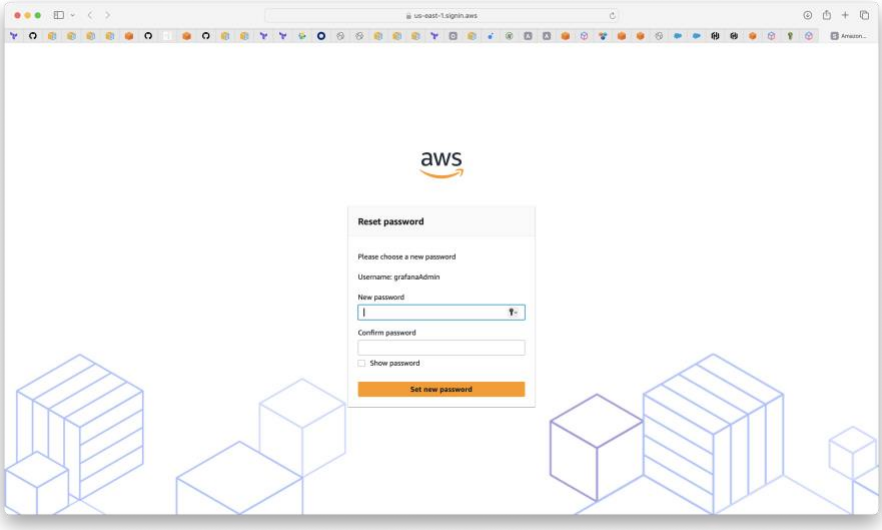
4.0.6 Next, return to IAM identity Center Console, on the right pane, refresh your browser session to confirm your email address has been verified as shown below:



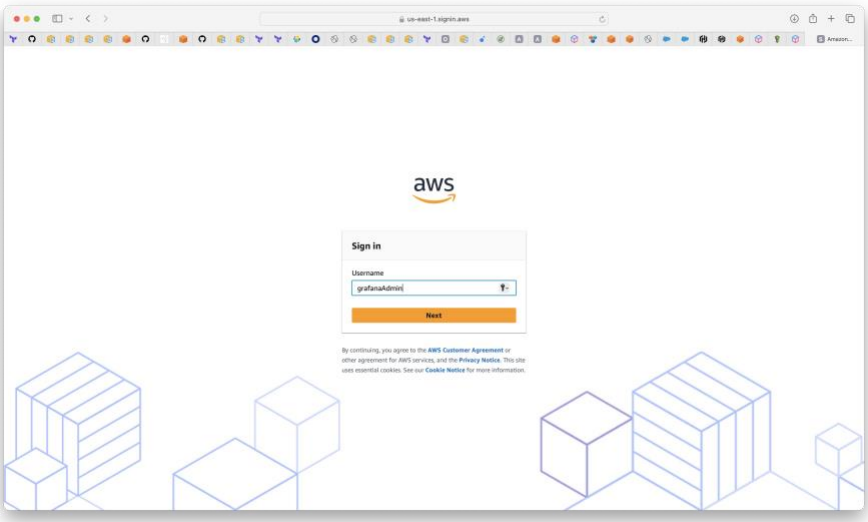
4.0.7 Next, in the same window on the right pane, click on “Reset password” button, a dialog box is displayed as show below, click on the “Reset password” button to send an email with instructions for resetting the user’s password



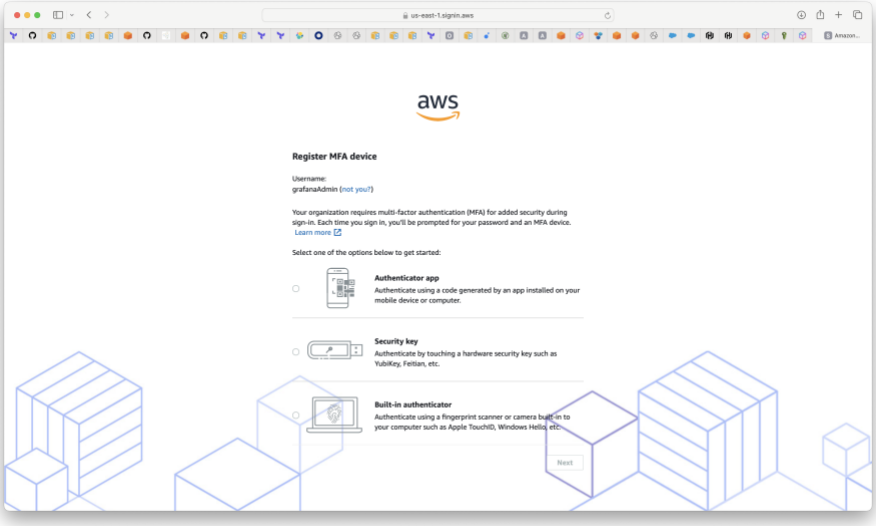
4.0.8 In the mail you received, click on the “Rest password” button, you will be redirected to a new browser page to set you password as shown below:



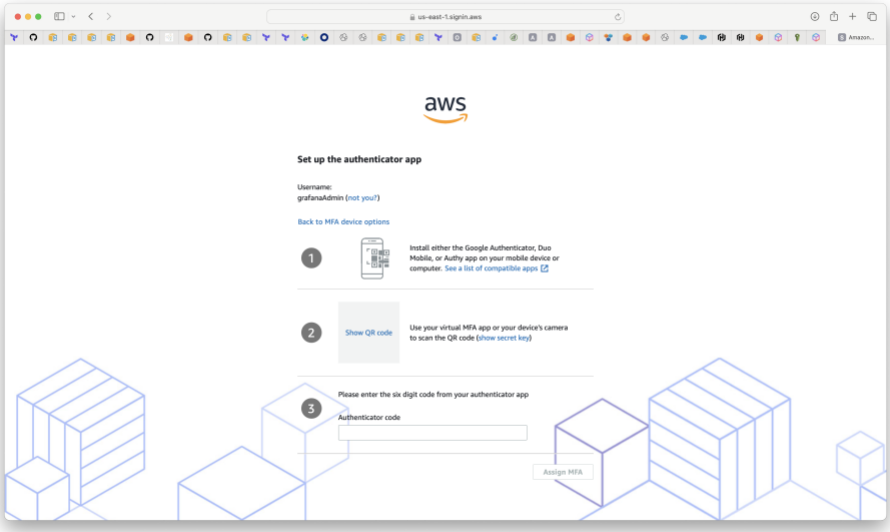
4.0.9 After setting your password, you will be redirect to sign-in page as shown below:



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:

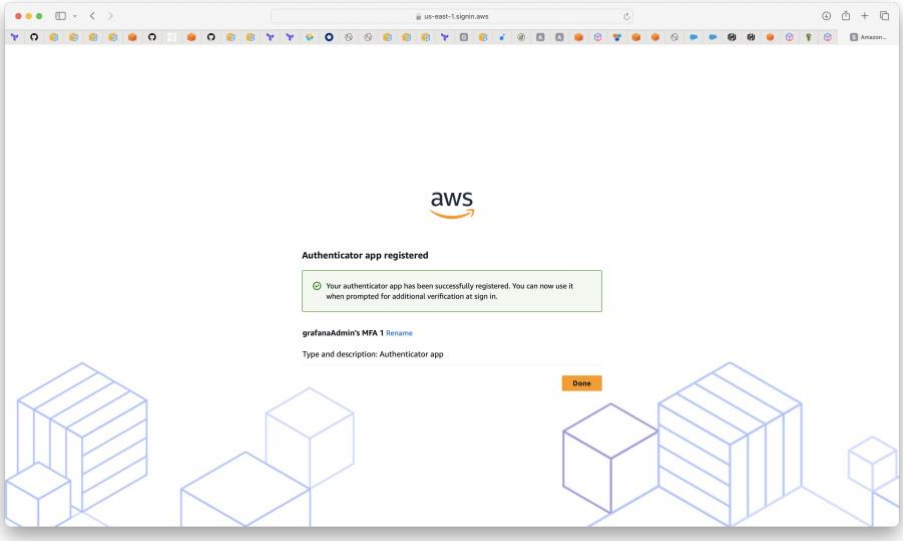


4.0.11 select the “Authenticator app” option and click next, a new page to Setup the authenticator app is displayed as shown below:

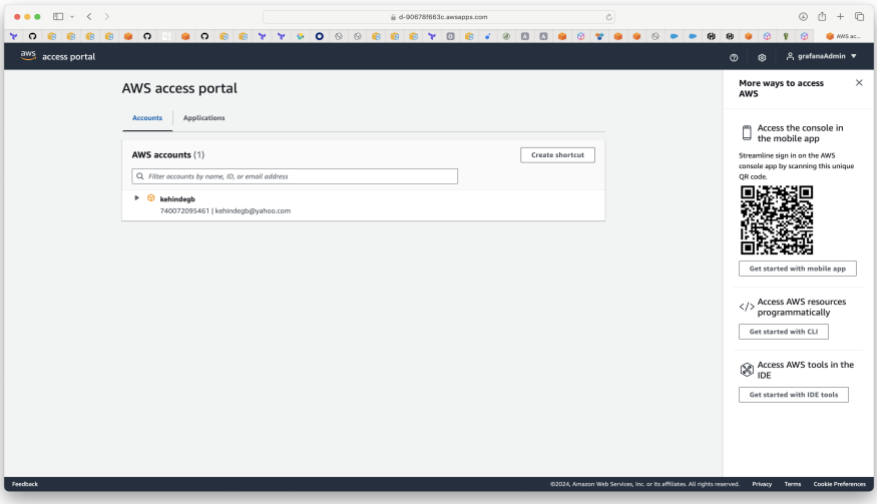


4.0.12 If you already have a virtual MFA device, then click option 2 to reveal the QR code. Scan the code using your virtual MFA device. The grafanaAdmin use will be configure.

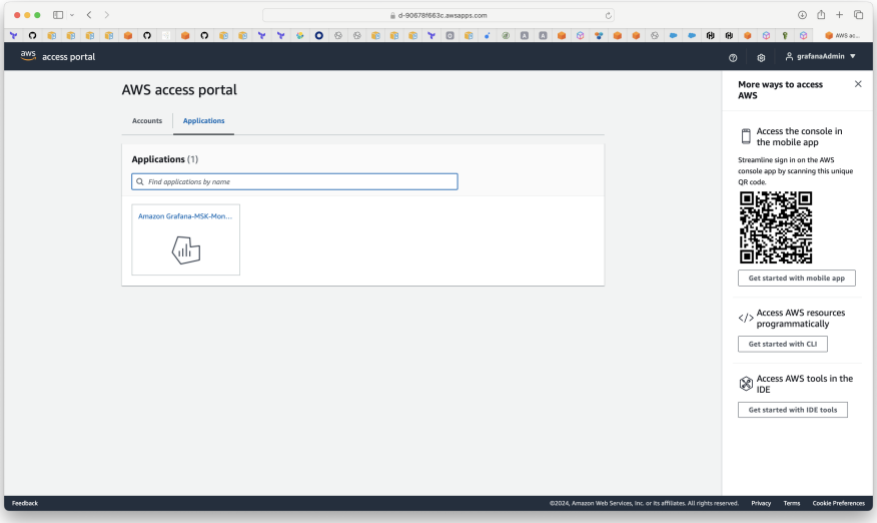
4.0.13 Next, enter the code provided by your virtual MFA device in the box, a new page is display indicating your Authenticator app is registered as shown below



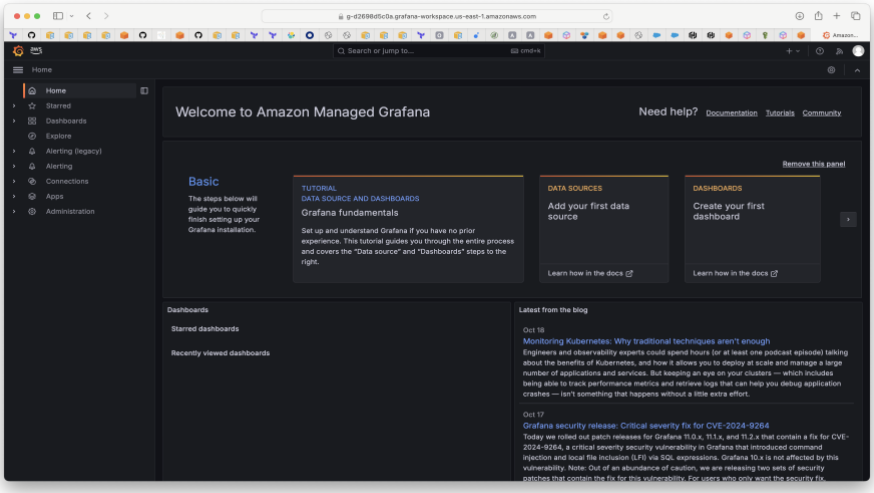
4.0.14 Next, click done and you will be redirected to the sign-in. Sign-in as "grafanaAdmin" user, after entering your password, you will be prompted to authenticate with MFA code. Once you supply the code, you will be redirected to "AWS Access Portal" page as shown below:



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

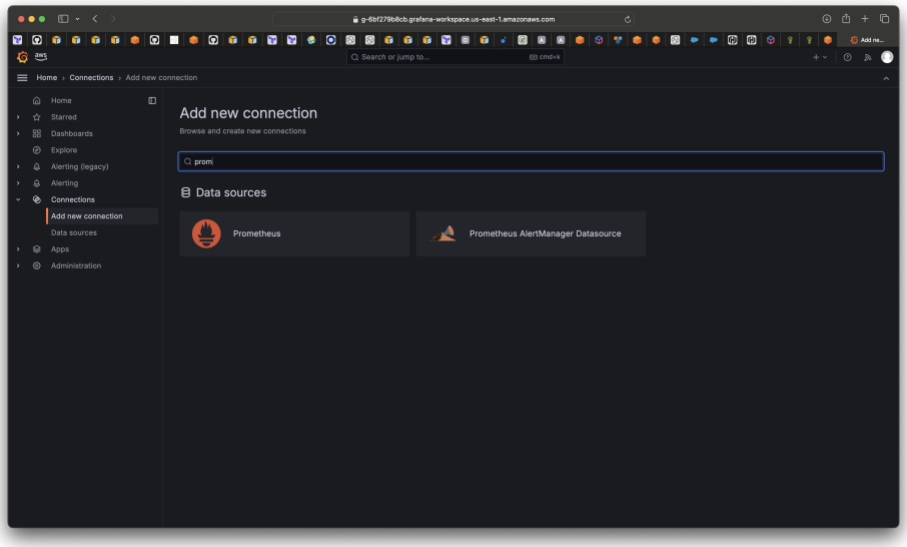


4.0.16 Next, click on your configured application and you will be redirected to the Amazon Managed Grafana Console as shown below:

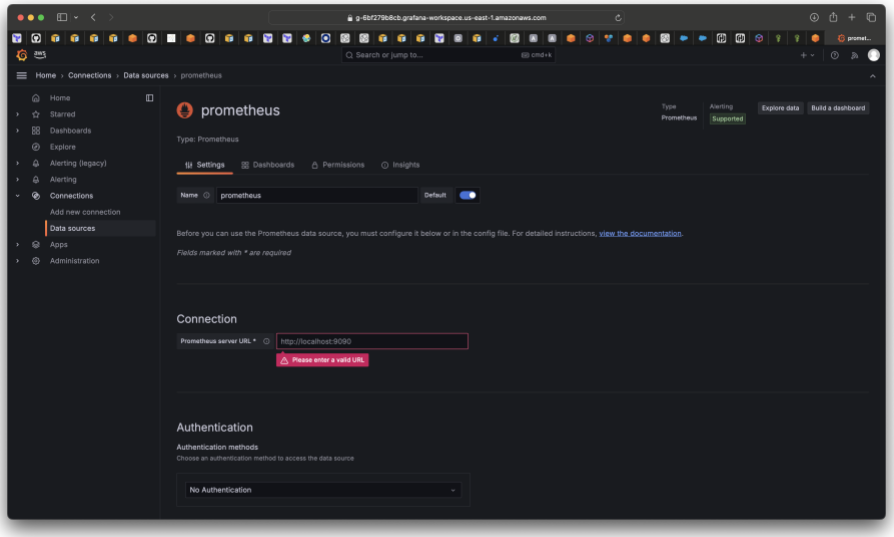


4.0.17 Configure Prometheus Data Source Connection

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:



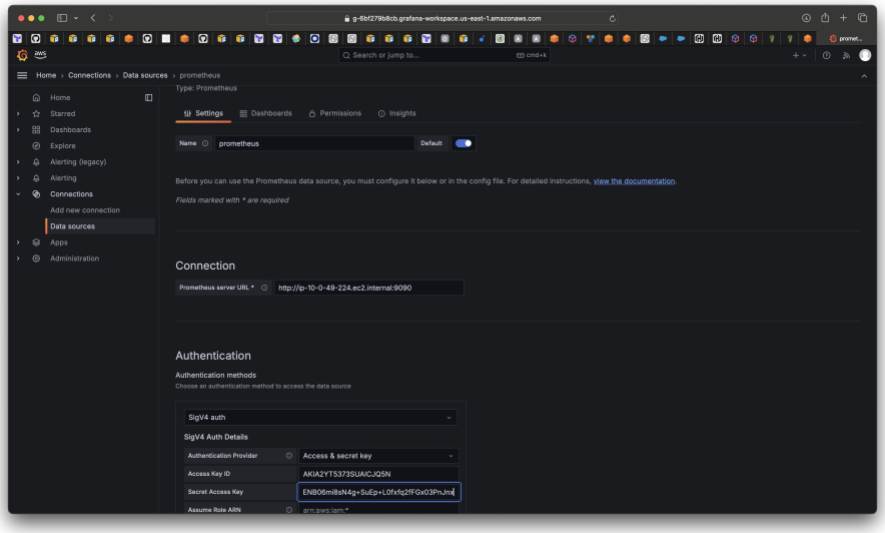
Click on Prometheus, and on the displayed window, click on “Add new data source button”, the window below is displayed



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

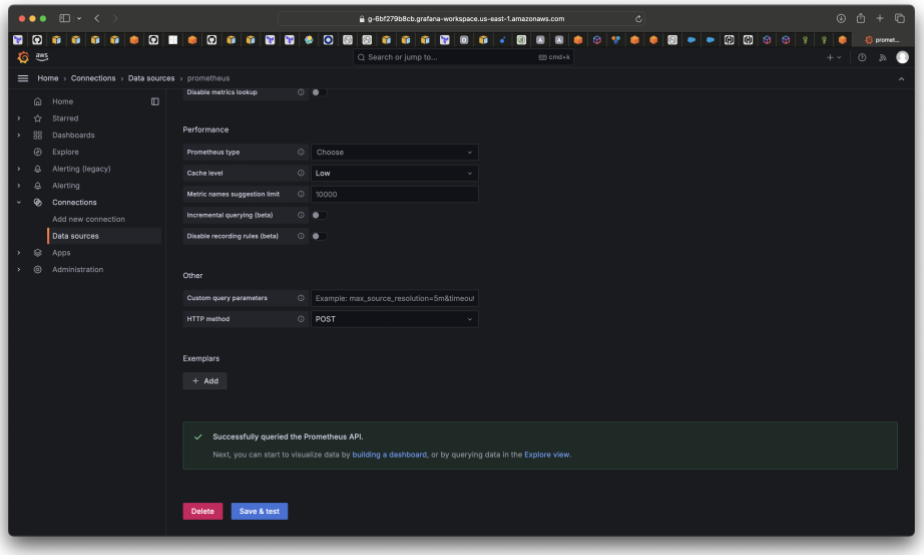
Still, in the same window above, under Authentication section, click on the drop-down list and select SigV4Auth, in the Authentication Provider drop down list, select Access & Secret Key. Next enter the value for Access Key ID and Secret Access Key (to get these values, logon to your Kafka Client Instance.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

Once these values have been populated, as show below:

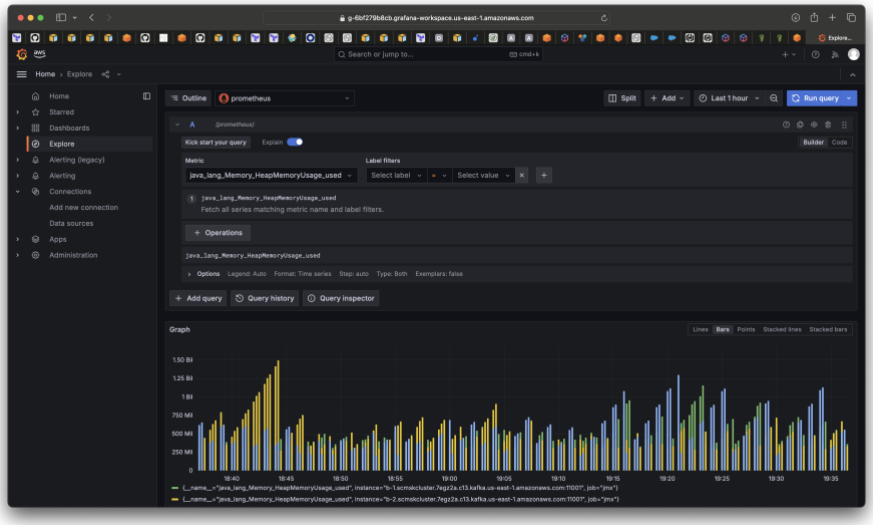


Next, scroll down to the bottom of the page and click on the button “Save & Test”

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



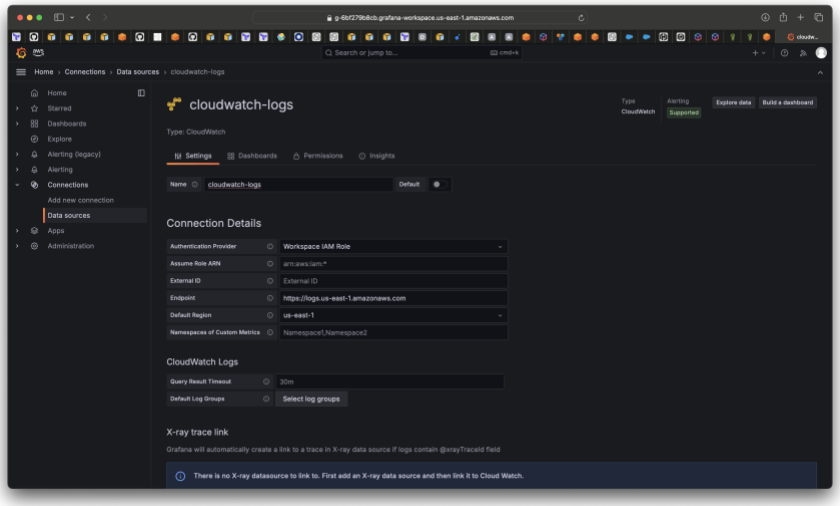
Next, on the left pane, click on Explore, on the displayed window, on the right pane, Prometheus is selected in the Outline section, under Metric, select are metric of your choosing and click on run query to display the visuals for that metric as shown below:



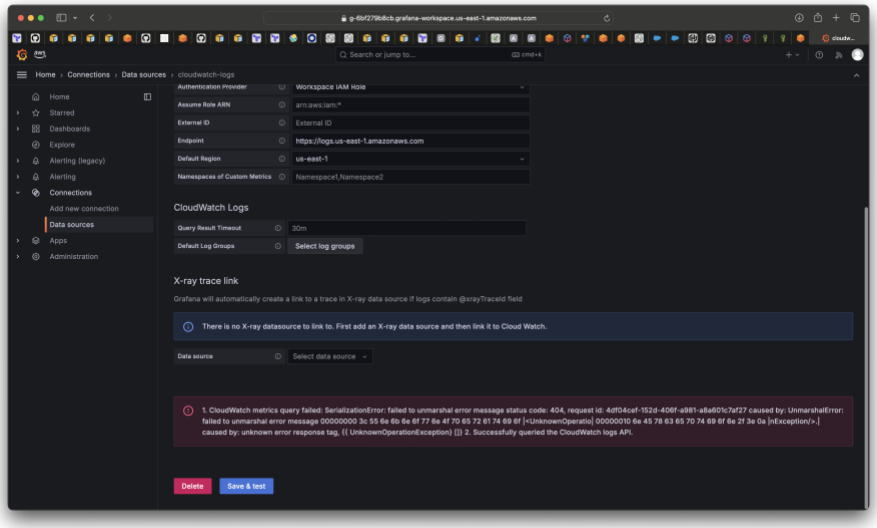
Configure CloudWatch Data Source Connection

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

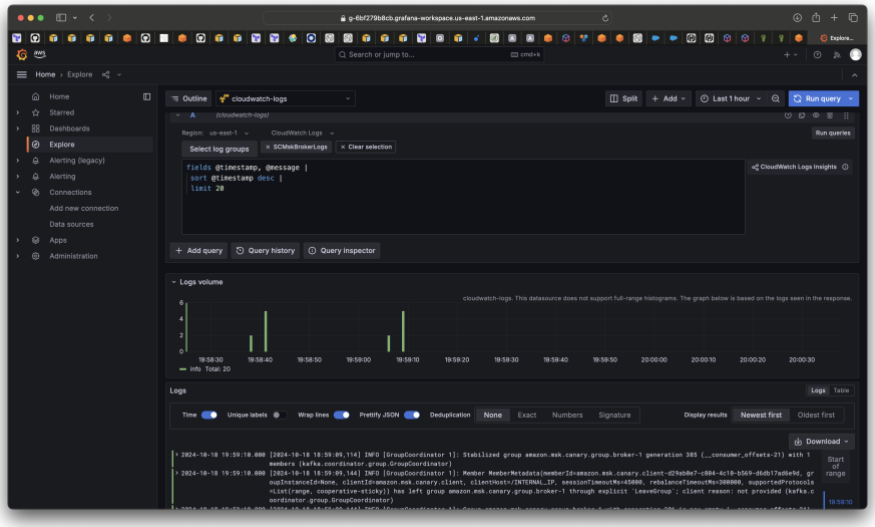
Setup CloudWatch logs Data Source as shown below:



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

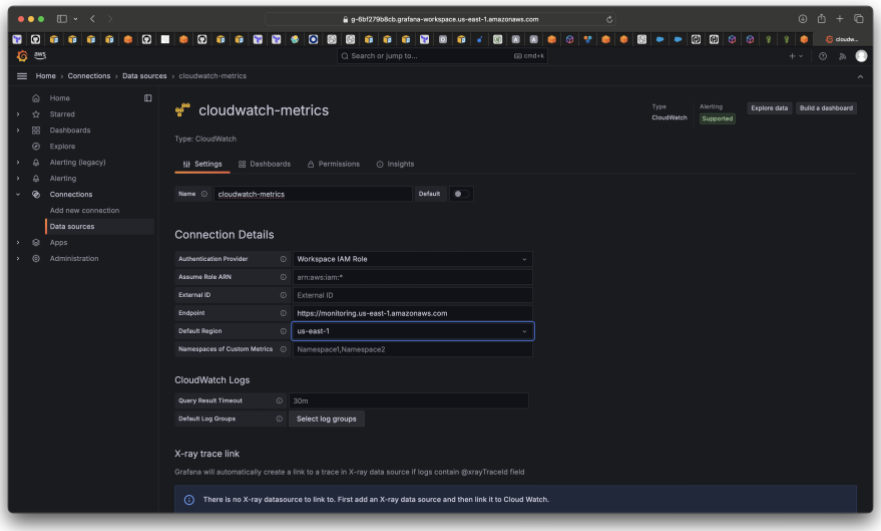


Next, Explore Logs, using the same process as before. Sample Log visualization is displayed as show below:

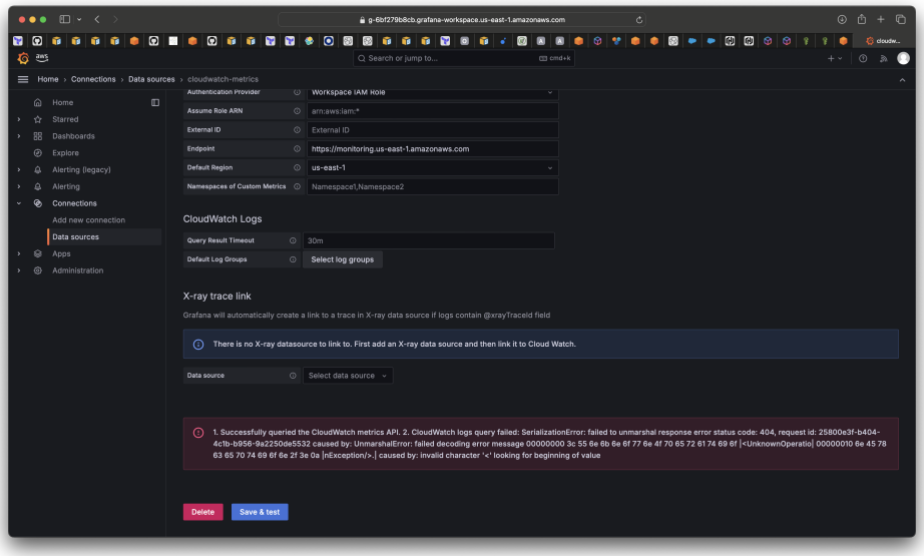


Next, repeat this same process for the monitoring end point to capture CloudWatch Metrics.

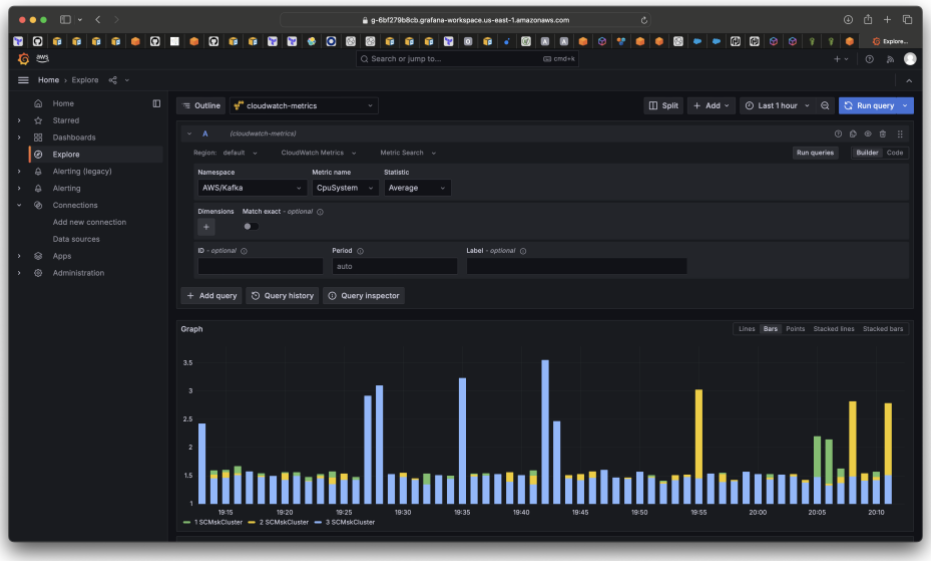
Setup CloudWatch Metrics Data Source as shown below:



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