Securing Sensitive Data in a Financial Application with AWS KMS

Technical Documentation of Secure Key Management with AWS KMS

Table of Contents

Team Name: Data Defenders

Team Leader: Takala

Project Manager: Awa

Technical Lead: Jaelin

Technical Lead Support: Mariana

Introduction

System Overview

Installation

Configuration

Usage

Integration with Financial Application

Best Practices

Troubleshooting

Security Considerations

API Reference

Glossary

AWS *(Amazon Web Services)* A cloud computing provider offered by Amazon, providing a vast collection of on-demand IT resources and services over the internet

Access Control Mechanisms to control who or what can access data and resources

Asymmetric Key Used for digital signing and verification, or key exchange. Choose this if you need to sign or verify data.

Cloud Providers Companies offering cloud computing services

Compliance Adhering to regulations and standards

Data Classification Categorizing data by sensitivity levels to implement appropriate security measures

DynamoDB Fully managed, serverless, NoSQL key-value database offered by AWS, designed to provide fast, predictable performance with seamless scalability

Encryption The process of scrambling data to make it unreadable without a decryption key

Encryption Key A string of code used to encrypt and decrypt data

HSM *(Hardware Security Model)* A specialized physical device that safeguards and manages encryption keys, often used for high-security applications

IAM *(Identity and Access Management)* A framework of policies, processes and technologies that help organizations manage digital identities and control what users can do within their computer systems or online applications

IAM Roles A way to grant permissions to access AWS services and resources specifying what can or cannot be performed within an AWS account, allowing for enhanced security, flexibility, and service integration between AWS and other services and resources

Key Administrators IAM users or roles who have permission to administer the key (e.g., manage key policies).

Key Alias A human readable name for a key

KMS *(Key Management Service)* A cloud-based service for generating, storing, and managing encryption keys securely

Key Policy Define a key policy to specify who can use the key and what operations they can perform.

Key Rotation The process of regularly changing encryption keys to enhance security

Key Usage Permissions Define which IAM users or roles can use the key for encryption and decryption.

Salted

Sensitive Data Information that, if compromised, could cause harm or damage

Tamper-Resistant Describes a device designed to resist physical attacks aimed at extracting sensitive information

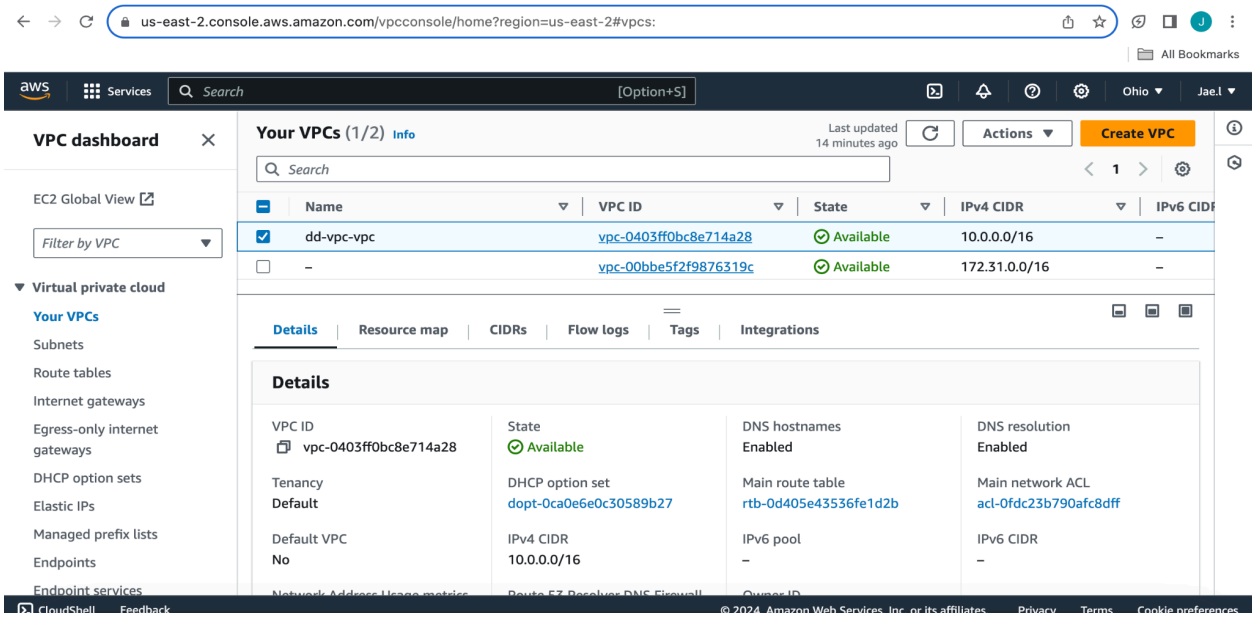
Threat Modeling Identifying potential threats and developing countermeasures

Vulnerability Assessment Process of identifying security weaknesses in a system

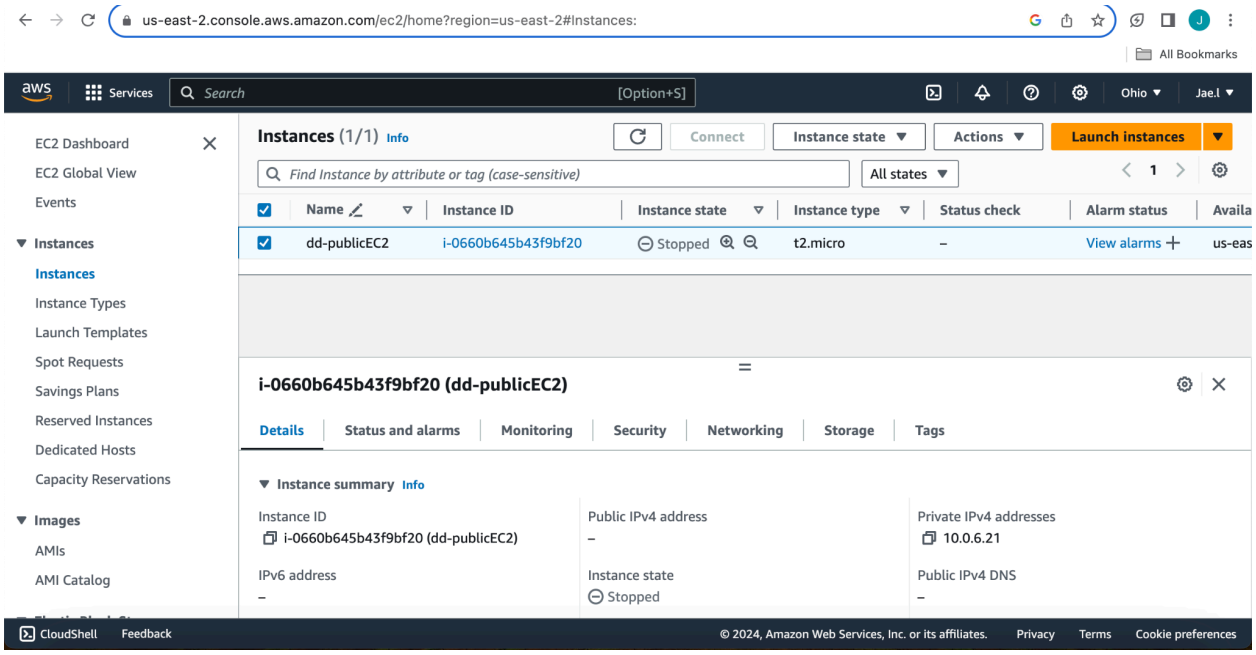
References

Configuring our VPC, EC2 Instance and Subnets Intro KMS Key Creation to & Lifecycle Management

1. We created our own VPC (Virtual Private Cloud)

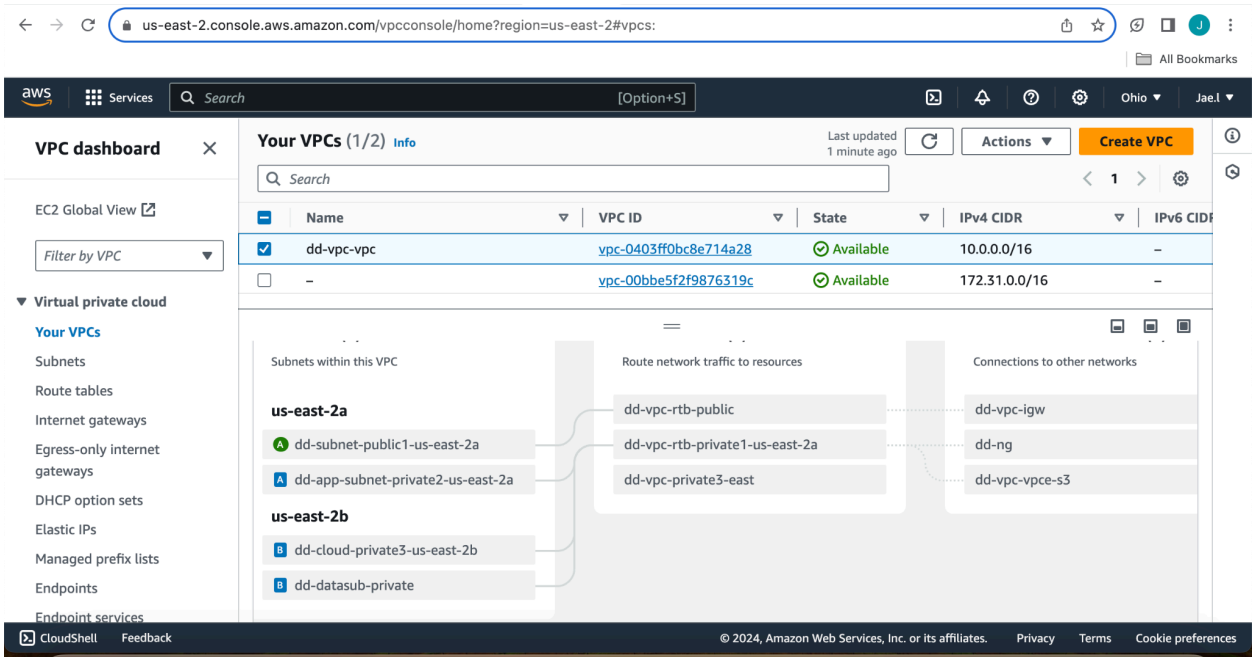


2. Within our VPC , we created an EC2 instance



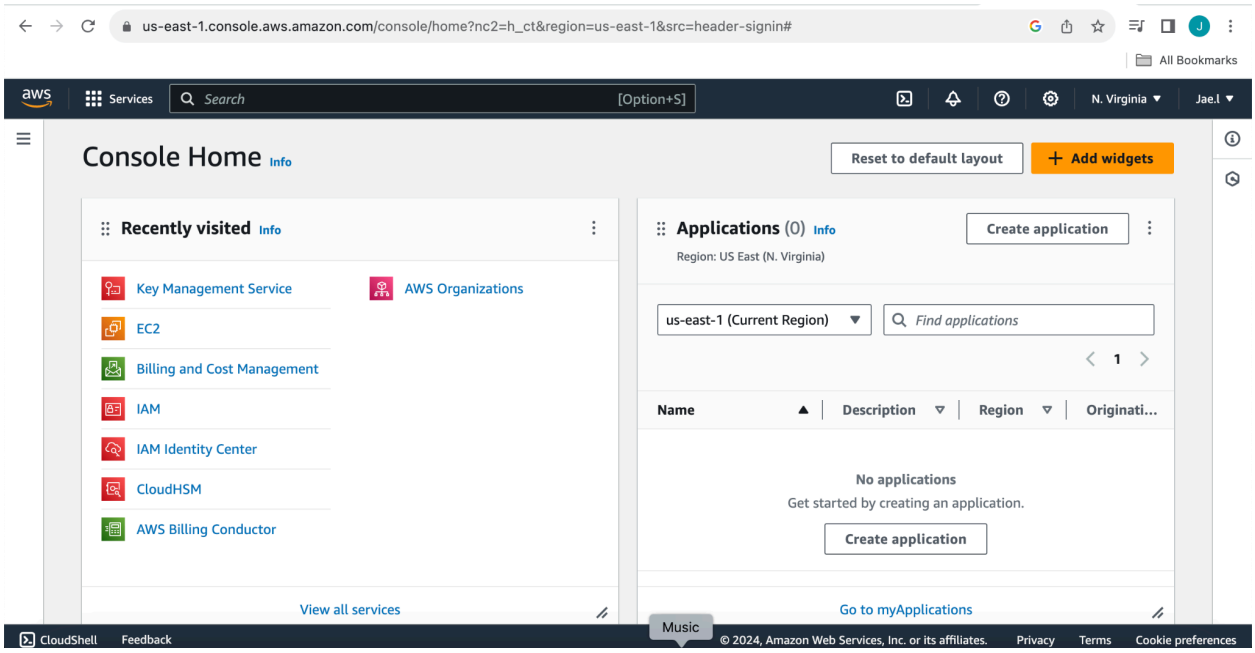
3.We created 4 subnets within our VPC

- 1 public
- 3 private: Our 3 private subnets were used for our applications, financial data, and cloudhsm
- Our public subnet is connected to a Internet Gateway
- Our private is connected to a NAT Gateway
- Security rules were added to each subnet to enhance security

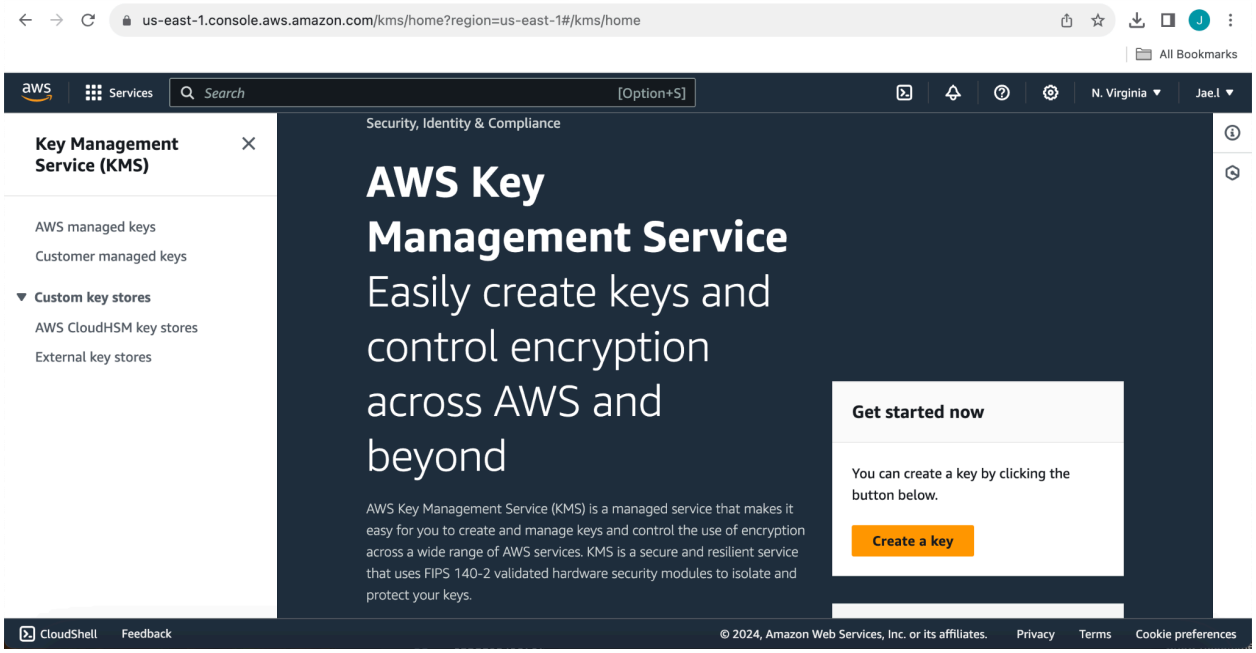


KMS Key Creation & Lifecycle Management: *Creating Customer Master Keys*

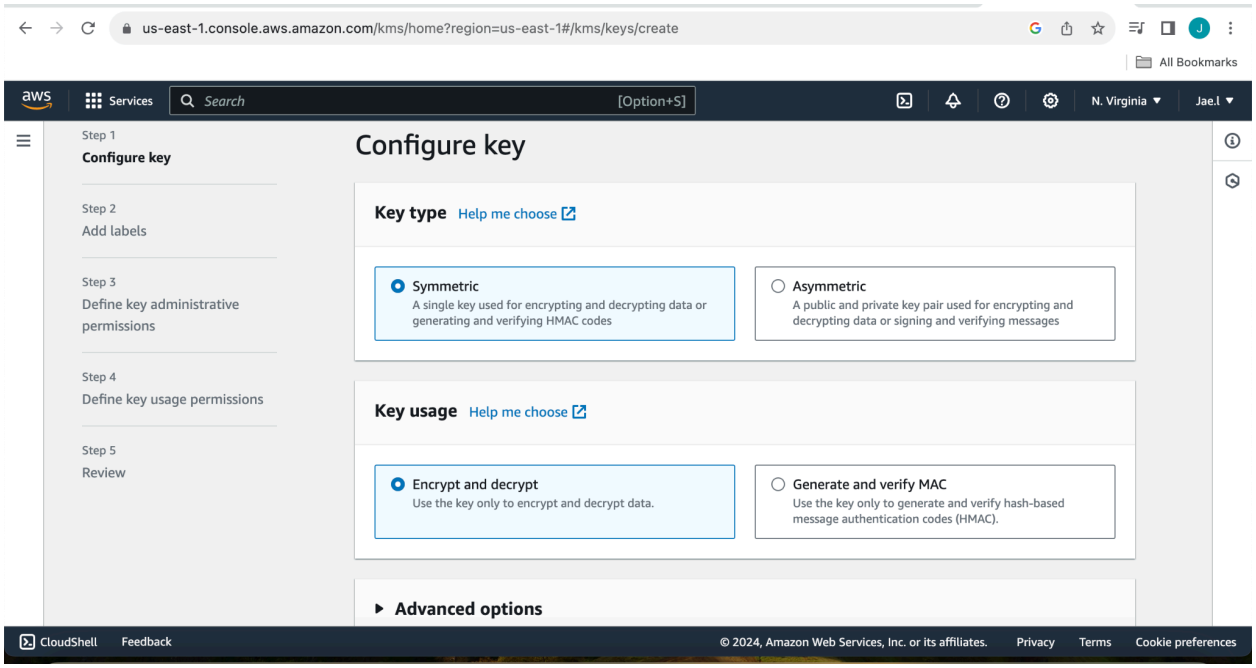
1. **Sign in to the AWS Management Console:** Go to the AWS Management Console and sign in to your AWS account. https://console.aws.amazon.com/



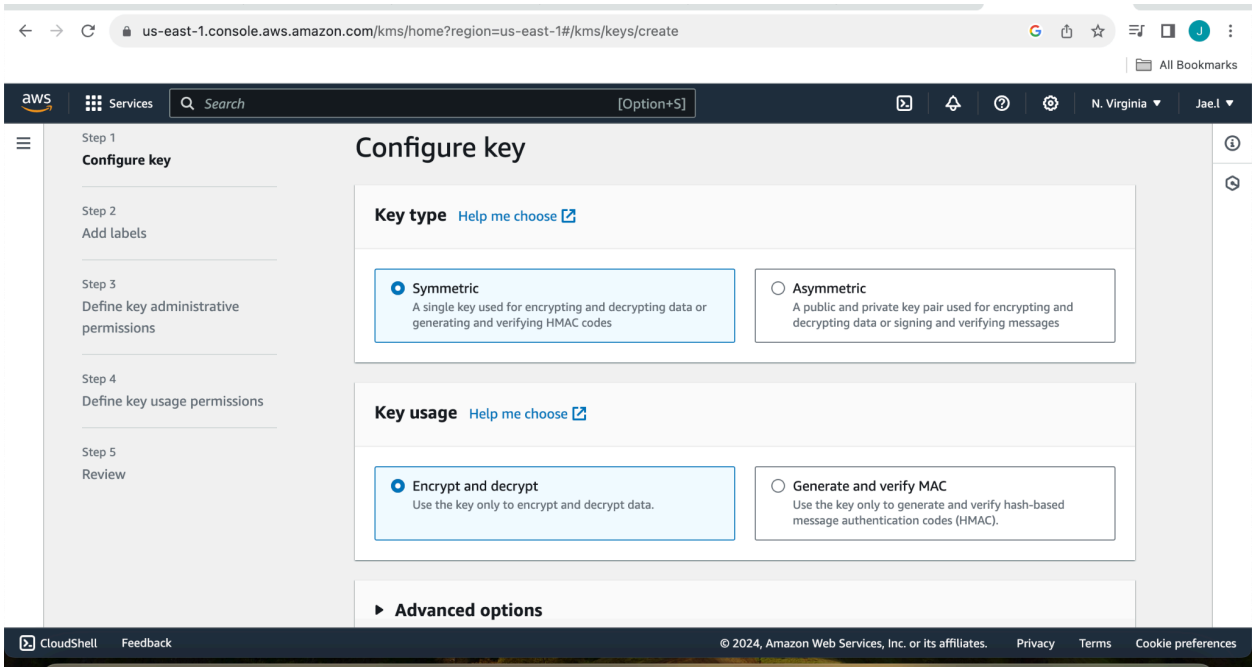
2. **Open the KMS Console:** Navigate to the KMS service from the list of available AWS services.



3. **Create a Key**: Click on "Create key" to start the process of creating a new KMS key.

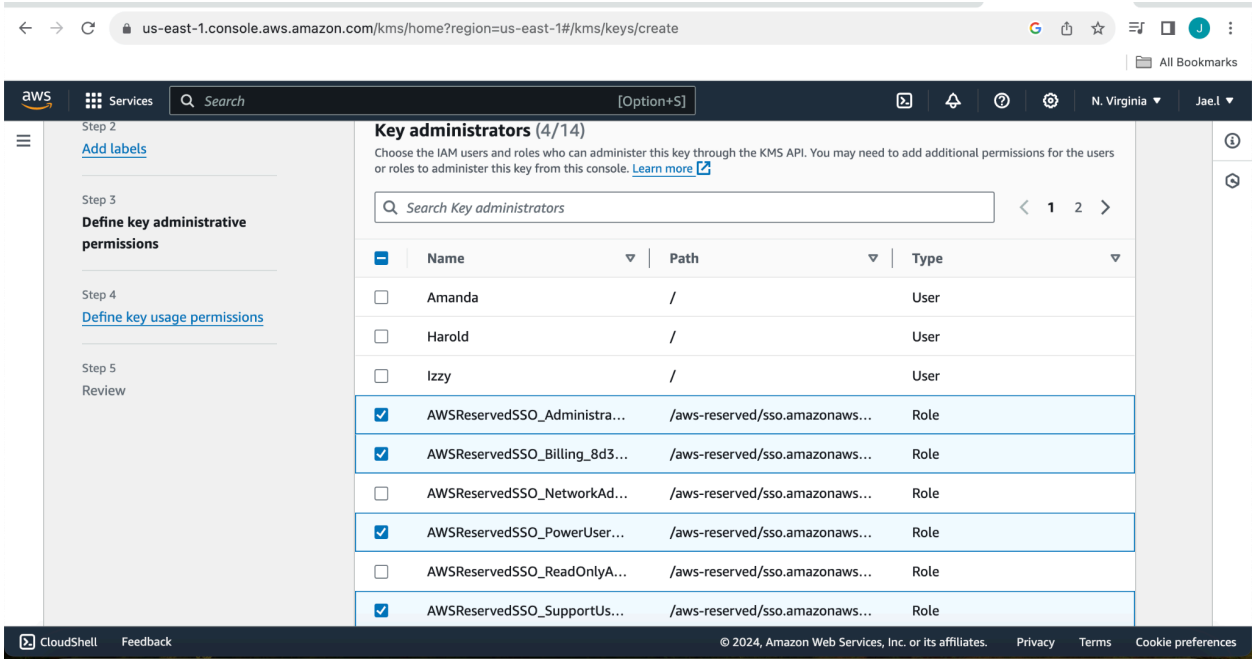


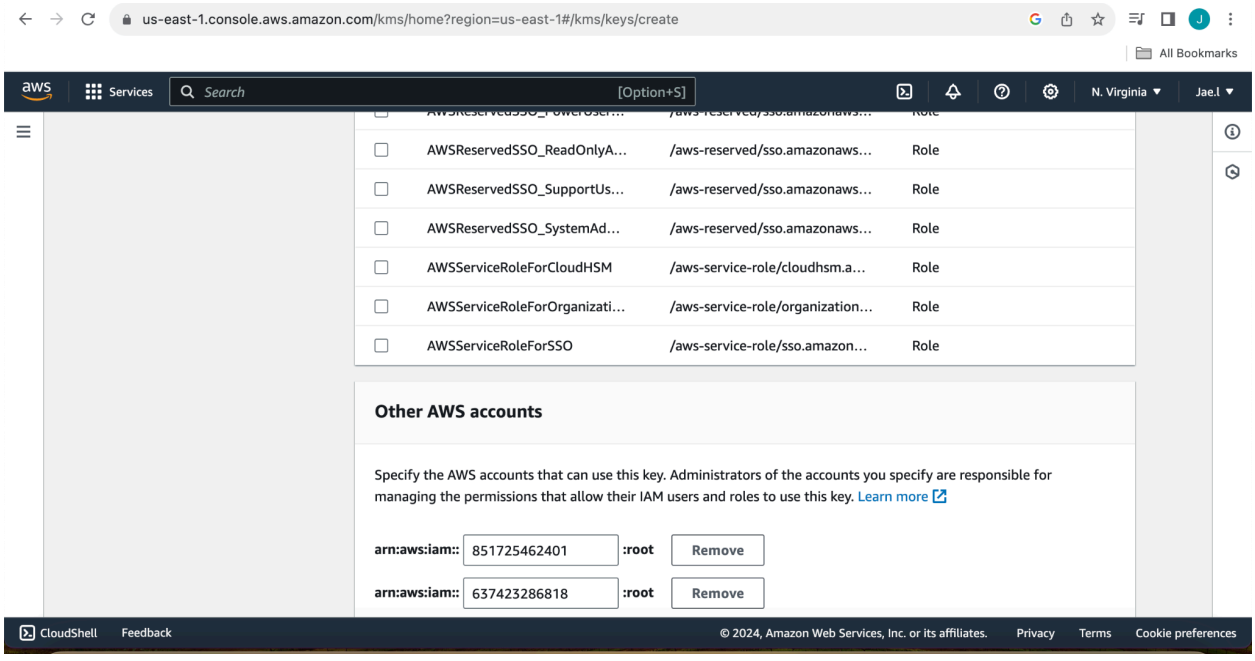
4. **Choose Key Type:** AWS KMS supports two types of keys:
   - Symmetric Key
   - Asymmetric Key



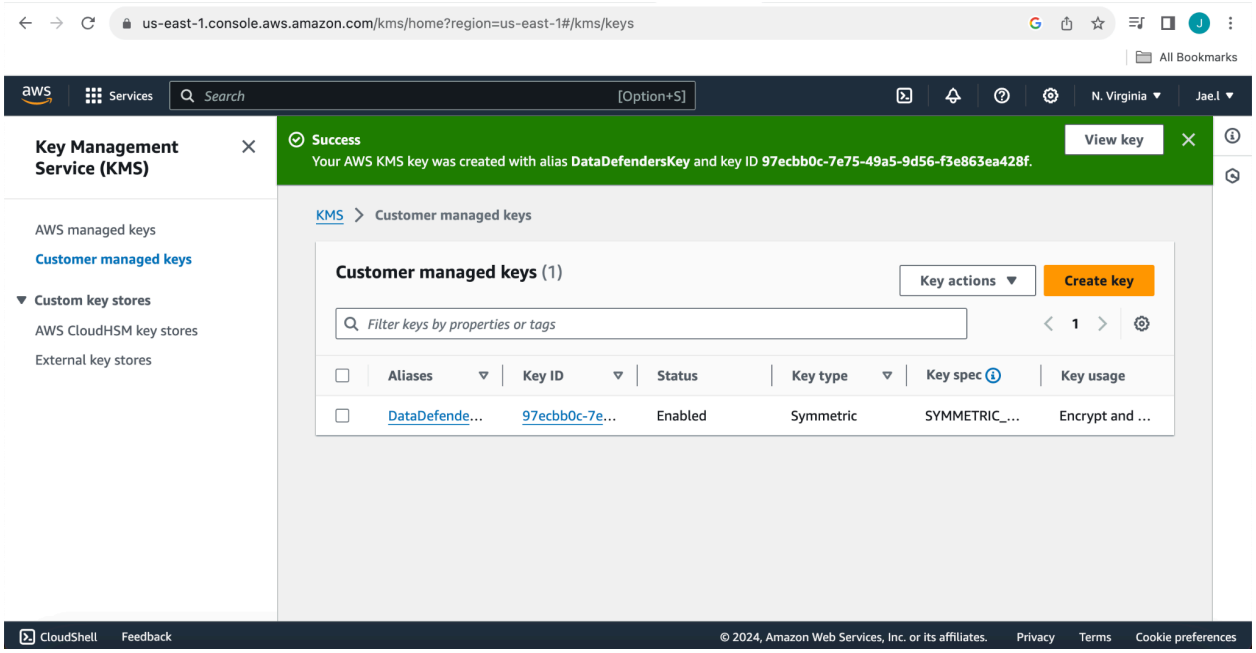
5. **Configure Key Settings:** Depending on the key type chosen, you'll have different configuration options. Here are some common settings:

- Key Alias
- Key Administrators
- Key Usage Permissions
- Key Policy

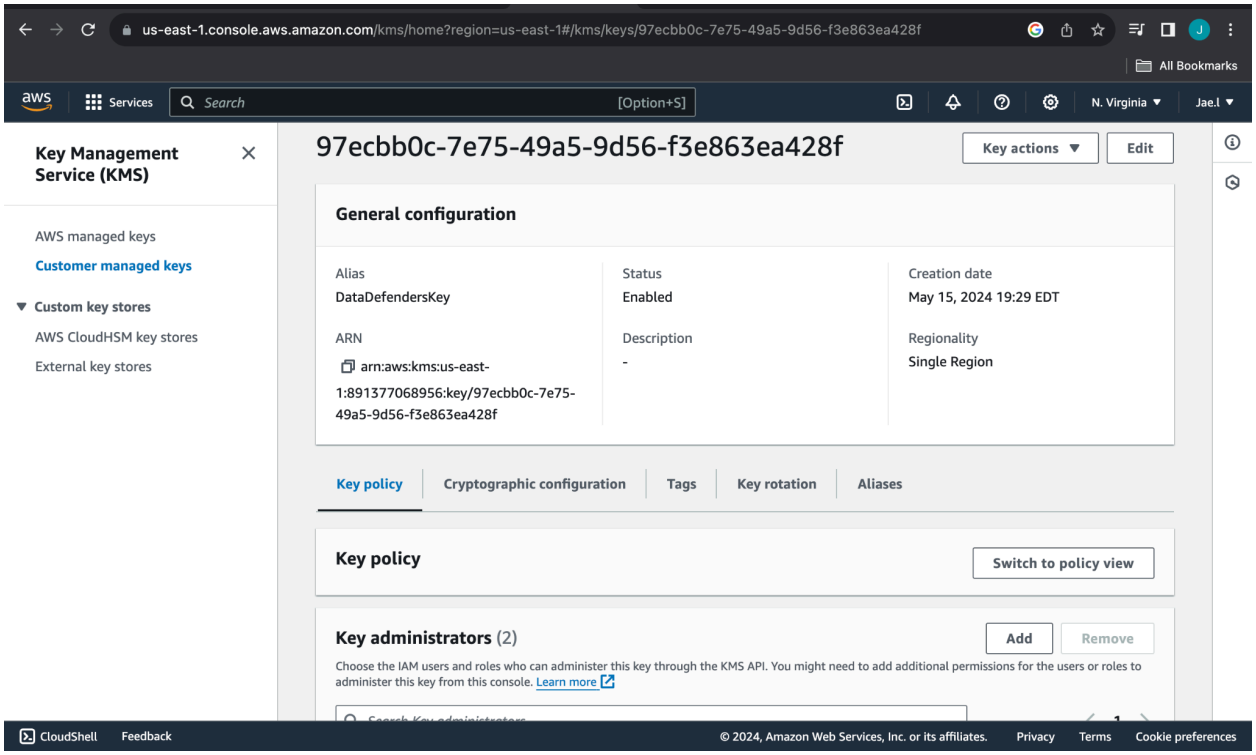




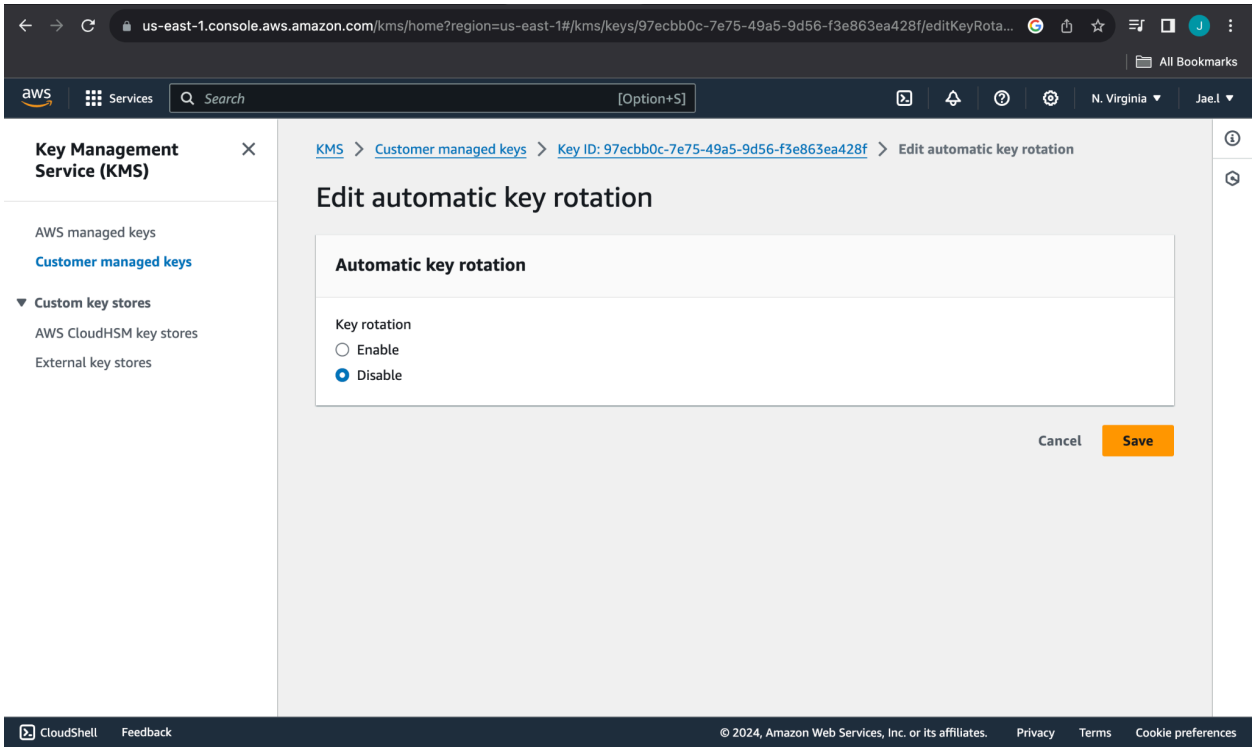
6. **Review and Finish:**Review the configuration details to ensure everything is correct. If everything looks good, click on the "Finish" button



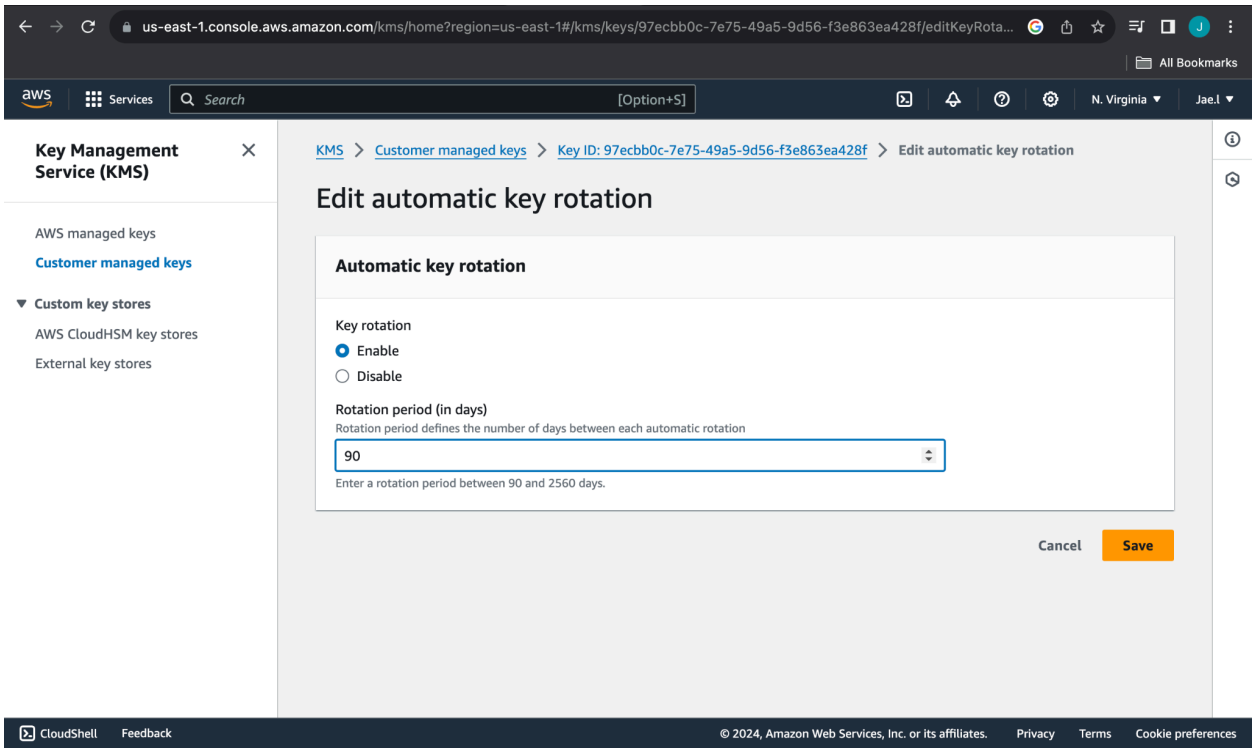
7. **Edit automatic key rotation:** After the key is created, select the key and click on “key rotation”



- **Edit automatic key rotation:** Click enable

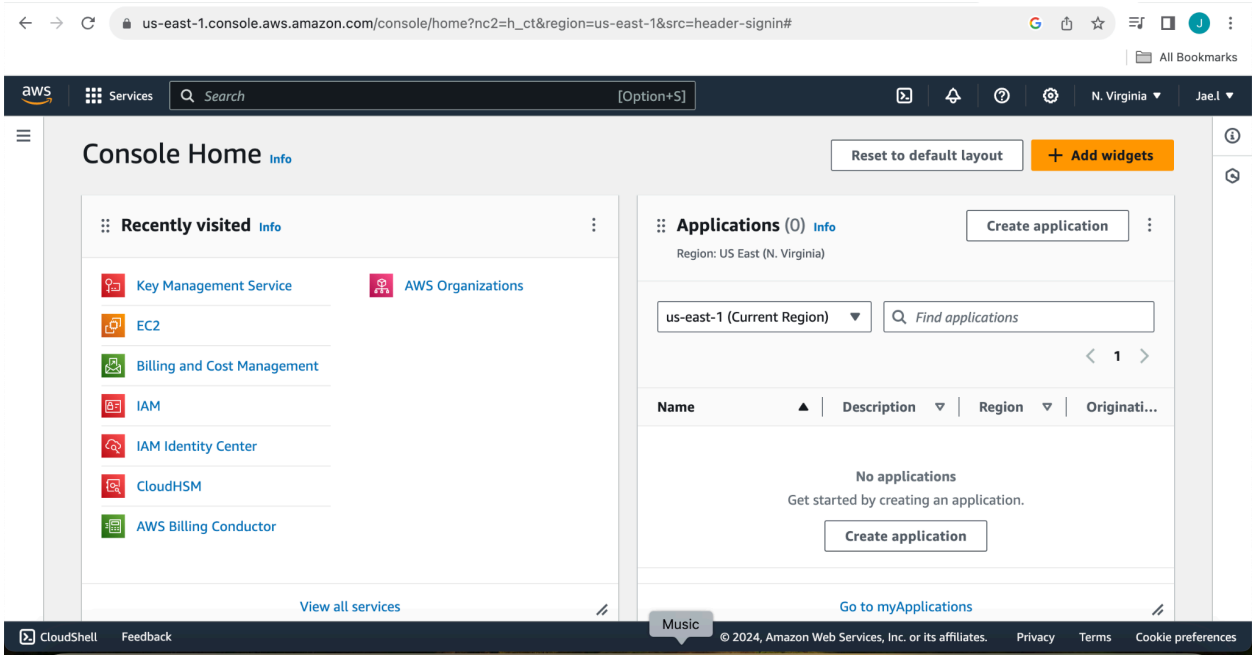


- **Insert rotation period days and save**

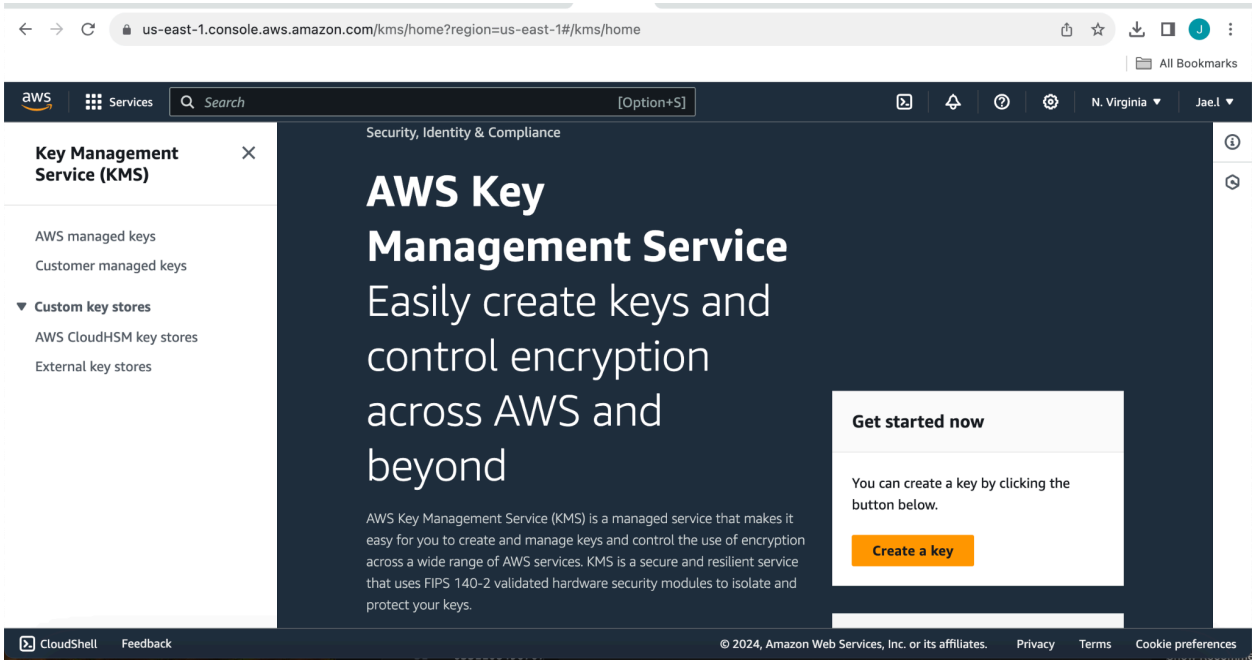


Creating Data Encryption Keys (DEKs) for Envelope Encryption

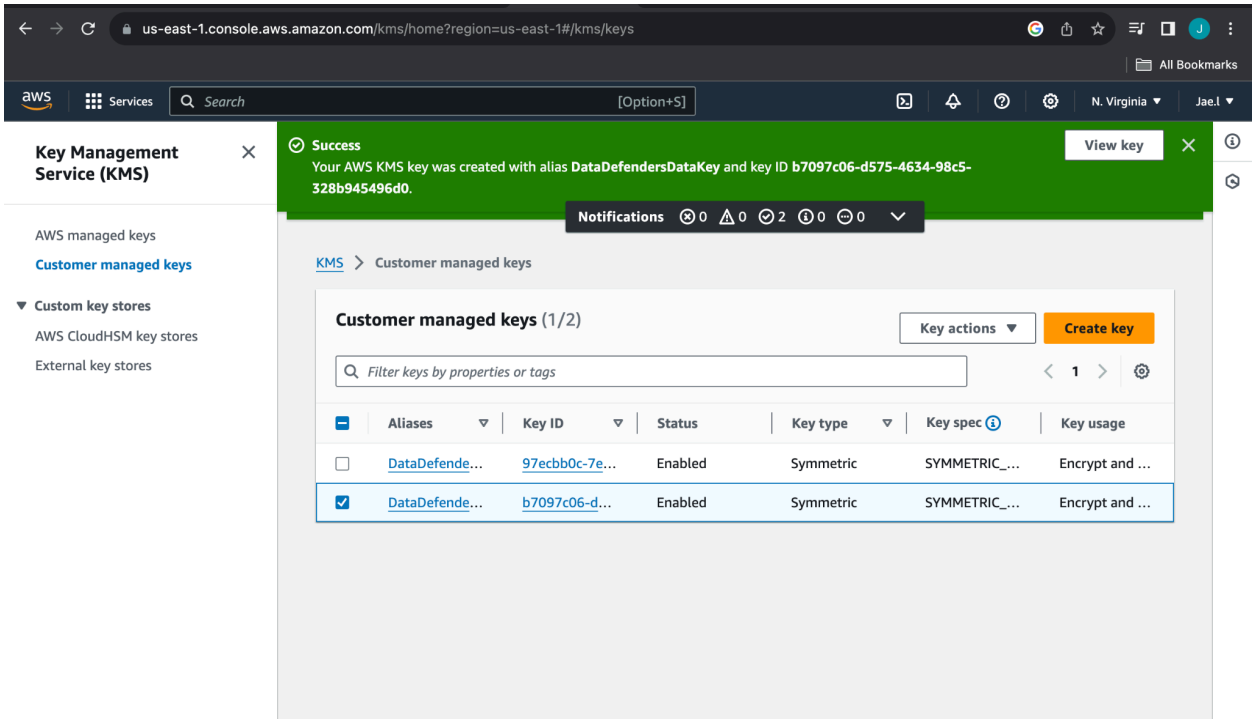
1. **Sign in to the AWS Management Console**: Log in to the AWS Management Console using your credentials.



2. **Navigate to AWS KMS**: Go to the AWS Key Management Service (KMS) console. You can find it under the "Security, Identity, & Compliance" section.



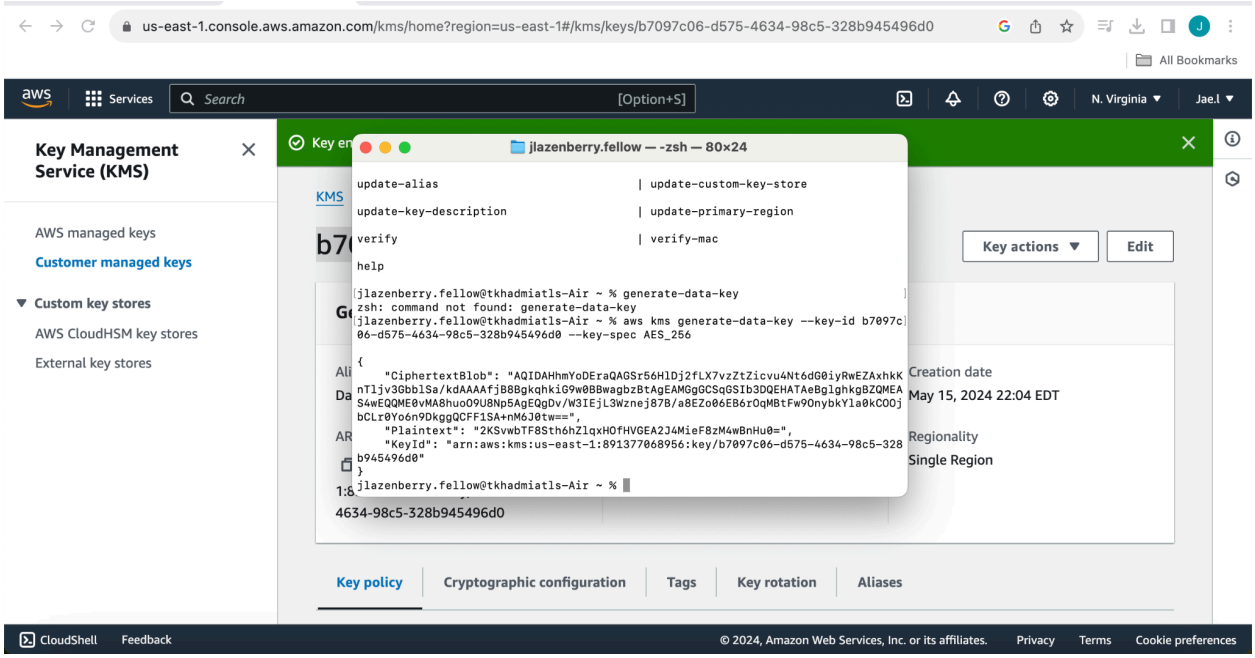
3. **Choose or Create a Customer Master Key (CMK)**: Before you can generate data encryption keys (DEKs), you need to have a Customer Master Key (CMK) created. You can either choose an existing CMK or create a new one.



4. **Generate a Data Encryption Key (DEK)**: Once you have a CMK selected, you can generate a DEK using that CMK through the AWS CLI.
5. We will now open the AWS CLI and use the command *cat* to see what our "financial.csv" file contains. This is the file we are going to use for envelope encryption.

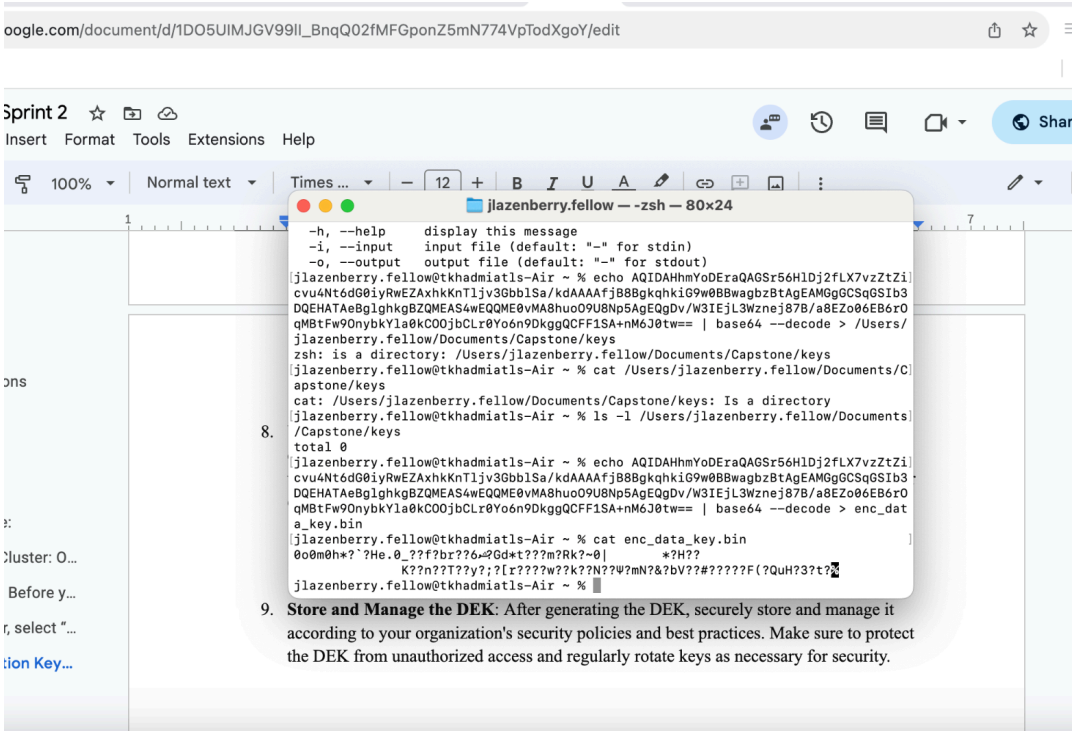
```
jlazenberry.fellow@tkhadmiatls-Air Downloads % cat mock_data.csv
card_number,card_holder_name,expiration_date,cvv,billing_address,billing_city,billing_state,billing_zip_code,card_type,card_issuer
5610784066498510,Myrtia Scimoni,10/1/2024,360,61513 South Street,Tsévié,,,bankcard,Jamia
5610462524671255,Lavena Uccello,7/4/2023,906,3568 Stoughton Avenue,Tondabayashichō,,589-0013,bankcard,Yadel
4936399450451315920,Howie Dachs,10/8/2022,262,888 Morningstar Drive,Strání,,687 65,switch,Skalith
5355118209792969,Etti Rayment,5/2/2025,267,83 Nova Street,Bom Despacho,,35600-000,mastercard,Avamba
5602253107628931,Blithe Hubbold,6/5/2025,506,34612 Marcy Hill,Stockholm,AB,111 20,bankcard,Tazzy
3556893471817528,Sioux Hearnes,6/19/2025,345,8 Novick Court,Lityn,,,jcb,Skalith
3547262808264071,Suzie Rickasse,4/20/2023,542,54 Derek Plaza,Koski Tl,,31501,jcb,Jaxnation
4041598573240609,Patsy Joynes,1/5/2024,872,180 Montana Circle,Nangtang,,,visa,Zooxo
347761140269274,Asher Bohje,10/6/2025,133,5345 Steensland Junction,Niederanven,,L-6948,americanexpress,Voolia
3548770929852607,Clementine Berardt,10/2/2024,853,726 Golf View Lane,Nantes,B5,44307 CEDEX 3,jcb,Brainverse
201757193624659,Guilbert Levis,1/22/2022,688,2 Cascade Pass,Rimpakgede,,,diners-club-enroute,Trupe
374479930641091,Siouxie Wilsey,8/20/2022,826,62643 Bunker Hill Parkway,Cunday,,734048,americanexpress,Skaboo
4175007668157536,Hetty Pech,5/8/2024,774,54754 Gina Center,Barberton,,1309,visa-electron,Kimia
30343494333907,Abby Besnardeau,7/31/2025,942,98 Scofield Plaza,New Orleans,LA,70183,diners-club-carte-blanche,Realcube
3582858737958687,Lucilia Gosnold,9/21/2022,537,4 Northview Circle,Setanggor,,,jcb,Devpoint
30466903887435,Warren Ollis,8/13/2024,756,9 Di Loreto Park,Kuty,,,diners-club-carte-blanche,Feednation
4911069844870144 32,Gorden Dirkin,8/7/2022,912,26 Stoughton Pass,Bagansiapiapi,,,switch,Skimia
6304512282812215635,Alister Dummigan,10/27/2023,758,07694 Fremont Way,Yongfeng,,,maestro,Feedfire
5048379152194164,Skipp Shovelin,5/20/2025,845,56921 Dennis Road,Xiacaoqiao,,,mastercard,Skiba
3582431824879677,Ethe Skahill,1/17/2024,525,6971 Hollow Ridge Avenue,Simunul,,7505,jcb,Kwideo
3587181317963349,Becka Scullard,6/26/2025,518,5 Stoughton Center,Shamkhor,,,jcb,Miboo
3565270551094170,Ethan Nehl,1/29/2025,284,9 Russell Alley,Chemin Grenier,,,jcb,Linklinks
3577461608133279,Merv Korneichuk,7/16/2025,800,53 American Street,Sovetakan,,,jcb,Jayo
6706995596502380546,Sidnee Philliphs,6/8/2025,383,02 Union Plaza,Zhovti Vody,,,laser,Twitterwire
5562423567488062,Mal Attard,8/18/2025,486,4 Ludington Terrace,Panyuran,,,mastercard,Snaptags
30013116486397,Madelene Etock,6/7/2023,229,9167 Ridgeway Park,Molsheim,C1,67124 CEDEX,diners-club-carte-blanche,Thoughtstorm
5108755220102320,Yuri Kearton,1/6/2022,312,9246 Bashford Place,Pohonsirih,,,mastercard,Rhyzio
5020277087480549,Garvy Goldberg,7/18/2022,481,34041 Ruskin Trail,Uppsala,C,753 14,maestro,Photobean
3855448916326 1,Adelina McLafferty,3/22/2022,769,43 Farwell Point,Changliu,,,diners-club-carte-blanche,Babblestorm
5893895760194110,Tedi Lynam,8/28/2025,160,9121 Talmadge Plaza,La Paz,OAX,71161,maestro,Zooveo
6304801872701104 53,Ruben Mathouse,2/24/2022,691,7859 Hoepker Terrace,Žabieniec,,05-509,laser,Wordify
3577619336112846,Laurena Berka,12/23/2024,447,2 Vera Trail,Santa Marta de Penaguião,17,5030-473,jcb,Brainverse
3568359551330465,Virgilio Longlands,12/20/2023,136,719 Thompson Terrace,Budapest,BU,1062,jcb,Meezzy
5010126154083612,Edyth Brunsden,1/1/2025,599,35 Coleman Plaza,Huiwan,,,mastercard,Gigaclub
4844455837414547,Zaria Boyle,5/30/2023,514,926 Green Ridge Trail,Ambatondrazaka,,,visa-electron,Browsecat
3540328705799241,Wiley Rickarsey,3/18/2024,735,4506 Dorton Junction,Zaječí,,691 05,jcb,Jaxbean
3541735369252052,Camille Kegg,6/20/2025,330,7 Donald Plaza,Victoria,,6406,jcb,Innotype
5602246302994280,Adora Madeley,10/21/2023,102,022 Transport Parkway,Quba,,,bankcard,Feedfire
3554614361722830,Kristofor Castano,2/25/2022,917,604 Petterle Park,Tengqiao,,,jcb,Meedoo
3557516418838211,Cassandry Butland,11/20/2022,265,58150 Vernon Street,Paatan,,9406,jcb,Tagchat
5610503417267617669,Gianina O'Scannill,4/15/2023,753,23 Huxley Court,Douentza,,,china-unionpay,Gigashots
3548235395982387,Austine Haughin,4/20/2022,565,173 Briar Crest Court,Malartic,QC,X0G,jcb,Tazz
3587568029037109,Alix Gardner,3/29/2024,249,2 Pankratz Plaza,Mingshuihe,,,jcb,Edgeify
3558035478435007,Maxwell Guthrie,11/1/2022,838,44 Superior Center,Tanggung,,,jcb,Rhycero
3546970775596371,Dorine Dudin,11/28/2023,202,286 Grayhawk Junction,Banjar Bias,,,jcb,Ooba
4905008818949283801,Dian Huddy,7/3/2024,532,20018 Delaware Place,Foros do Trapo,15,2985-129,switch,Tekfly
5602236188570061,Zane Argente,5/14/2025,182,8 Sloan Park,Shuidong,,,china-unionpay,Youtags
5018558669026482476,Clarisse De La Hay,4/27/2023,918,084 Springs Alley,Best,06,5684,maestro,Midel
5602236008026123,Ayn Scawton,4/9/2025,718,32 Pleasure Terrace,Shcherbinka,,142720,china-unionpay,Twinte
30508103798548,Ondrea Cudiff,8/7/2022,824,97 Rockefeller Center,Torez,,,diners-club-carte-blanche,Innojam
4041596669295008,Ava Gentil,10/22/2025,131,3 Fremont Point,Can-Avid,,6806,visa,Skipfire
3589624865815948,Rab Eady,6/14/2023,936,16 Grasskamp Plaza,Chengnan,,,jcb,Izio
5010129602179743,Leona Cumine,8/29/2025,818,8 Buell Place,la Massana,,AD400,mastercard,Kanoodle
```

6. **Specify Key Metadata (Optional):** You can specify optional metadata when generating the DEK, such as an alias or description, to help identify and manage the key.
7. **Generate the DEK**: Once you're satisfied with the configuration, proceed to generate the DEK.



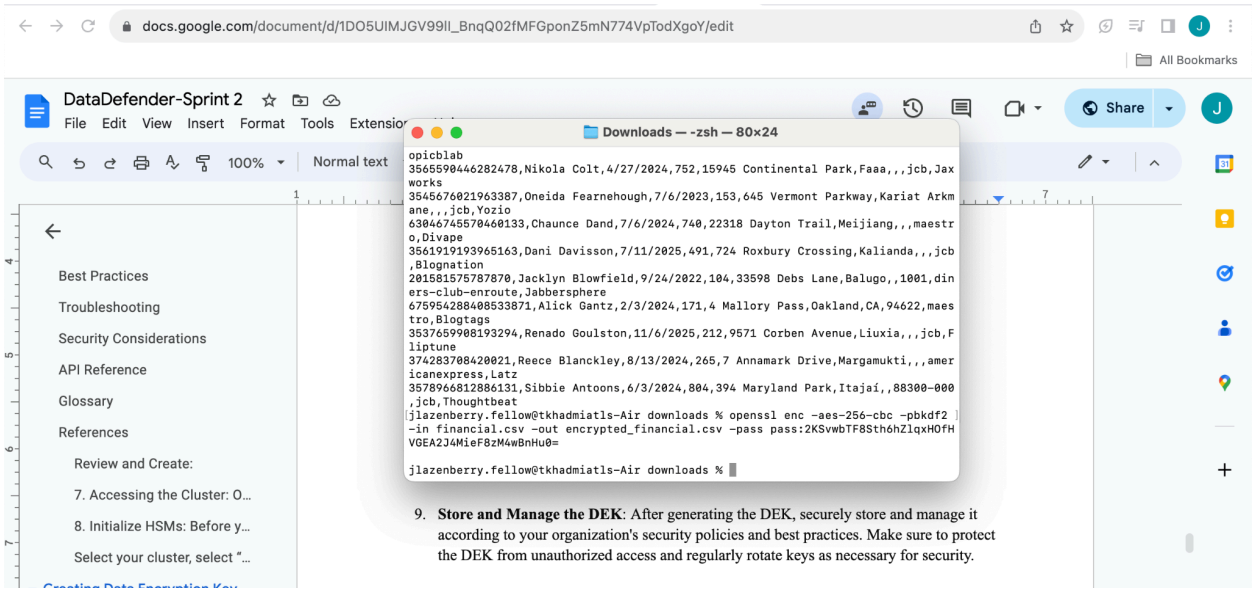
8. **Use the DEK for Encryption**: Once the DEK is generated, you can use it to encrypt data.

This is our key being decoded from base64 to binary. This is for more compatibility and security. This key was stored in a file.

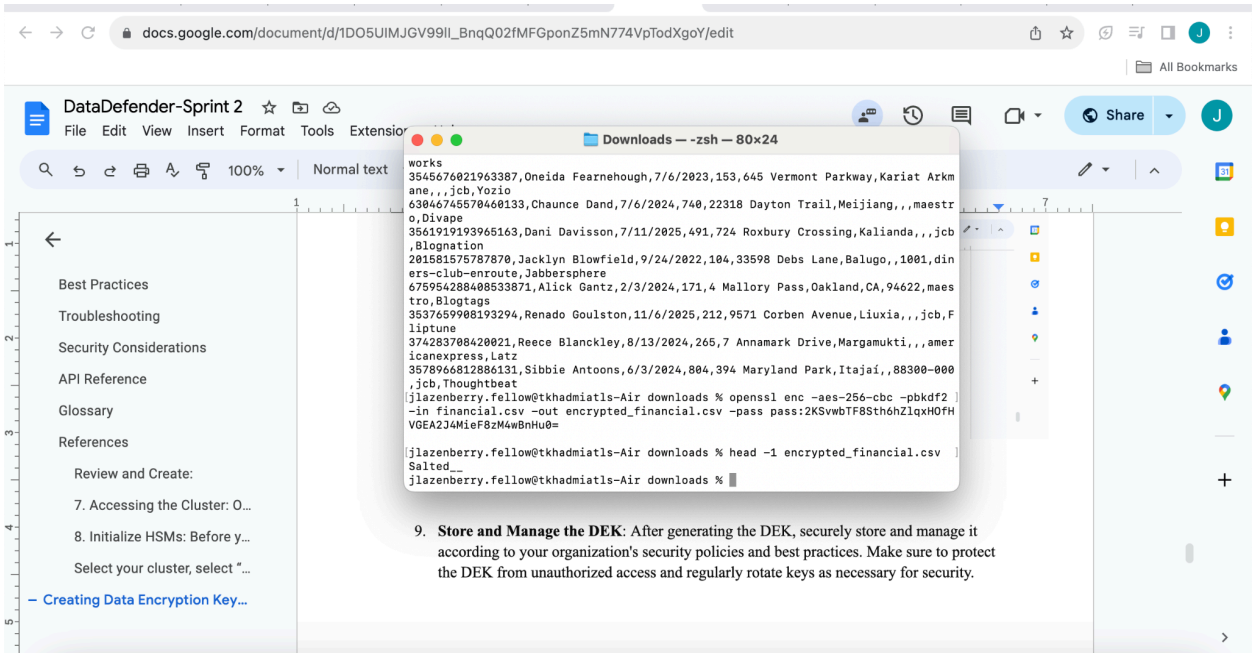


Our files have been encrypted.

- Financial.csv - This is our original secret file
- Encrypted_financial.csv - This file is our secret file encrypted
- Enc_data_key.bin - This file is our encrypted data key



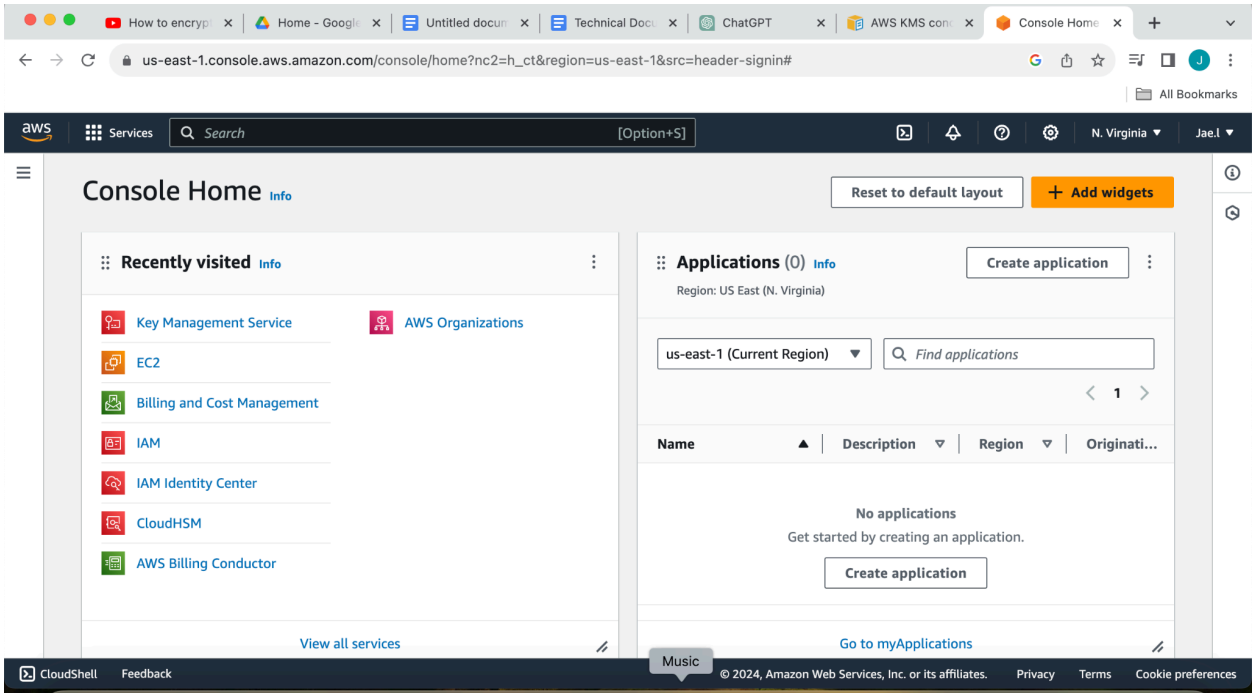
Here our encrypted file says “salted” .



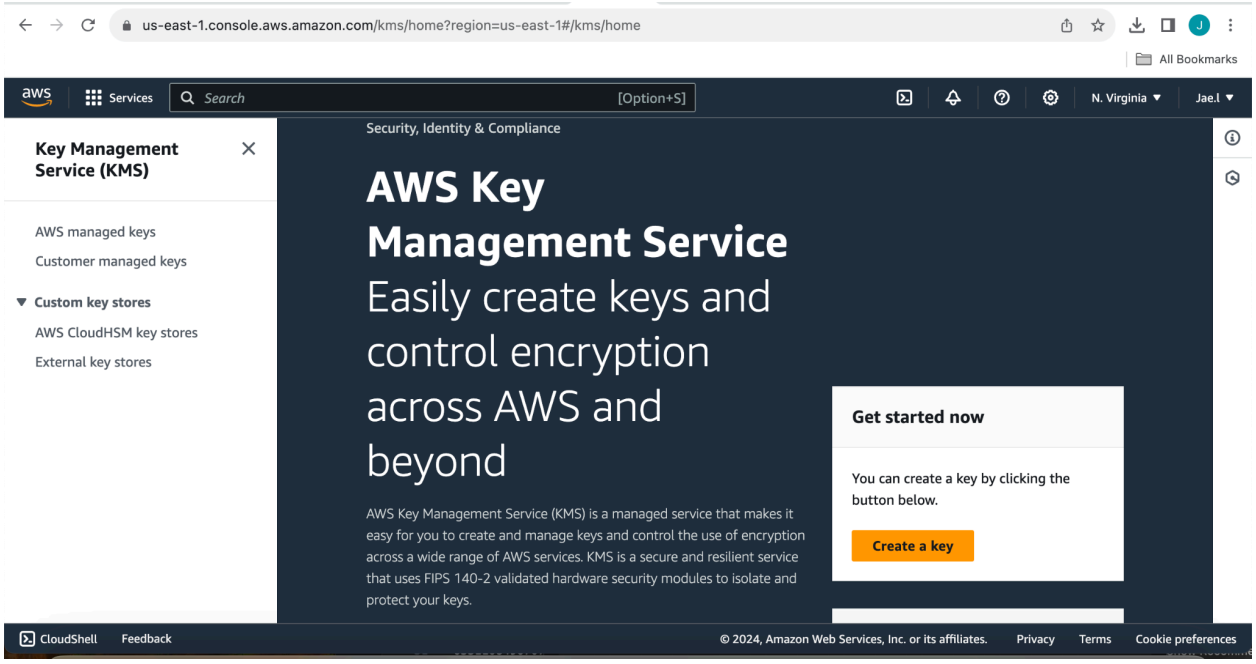
9. **Store and Manage the DEK**: After generating the DEK, securely store and manage it according to your organization's security policies and best practices. Make sure to protect the DEK from unauthorized access and regularly rotate keys as necessary for security.

KMS Integration Documentation with Encryption Services

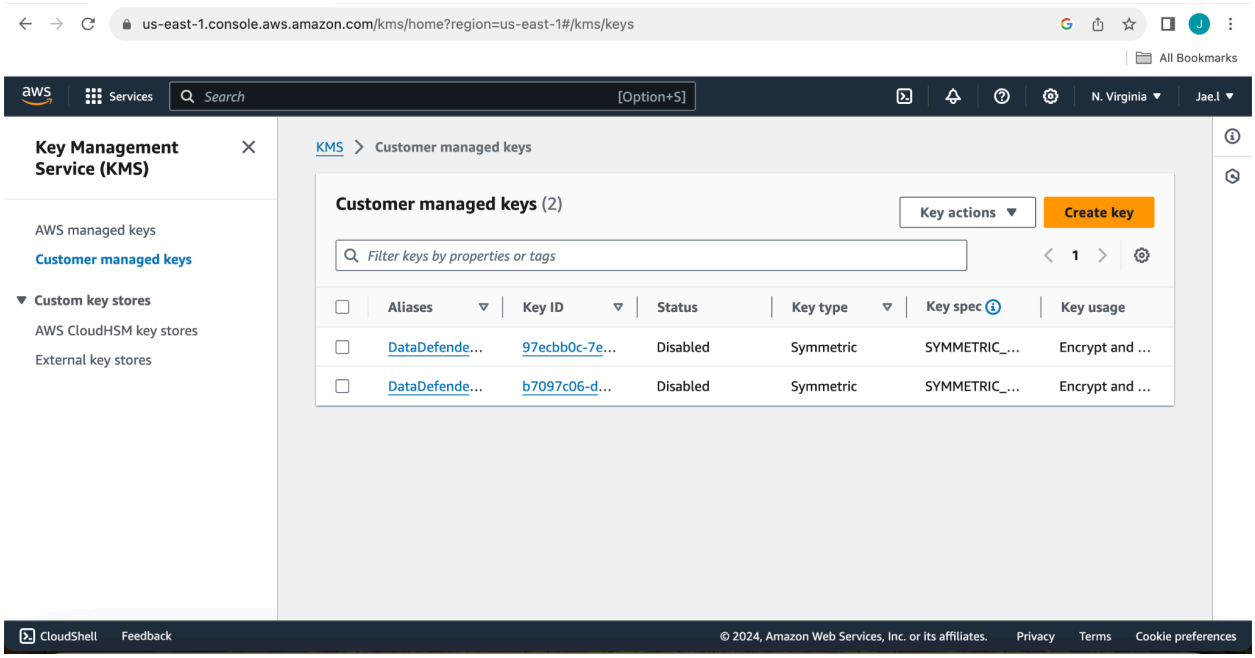
1. **Sign in to the AWS Management Console**: Log in to the AWS Management Console using your credentials.



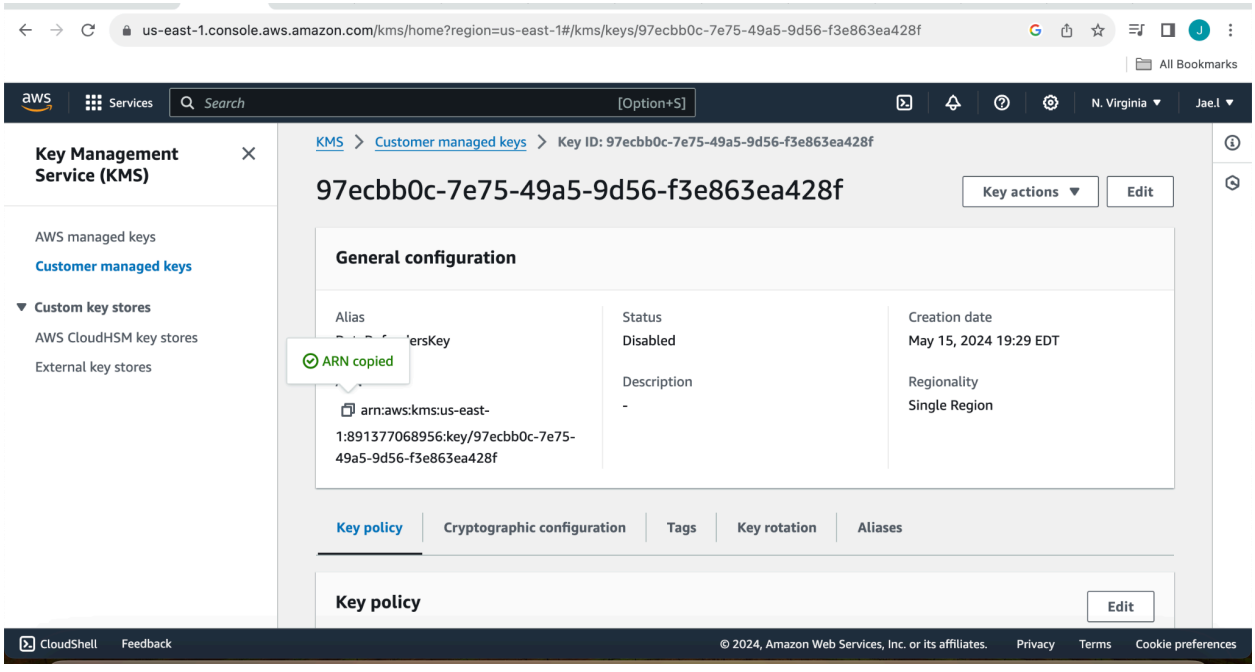
2. **Navigate to AWS KMS**: Go to the AWS Key Management Service (KMS) console.



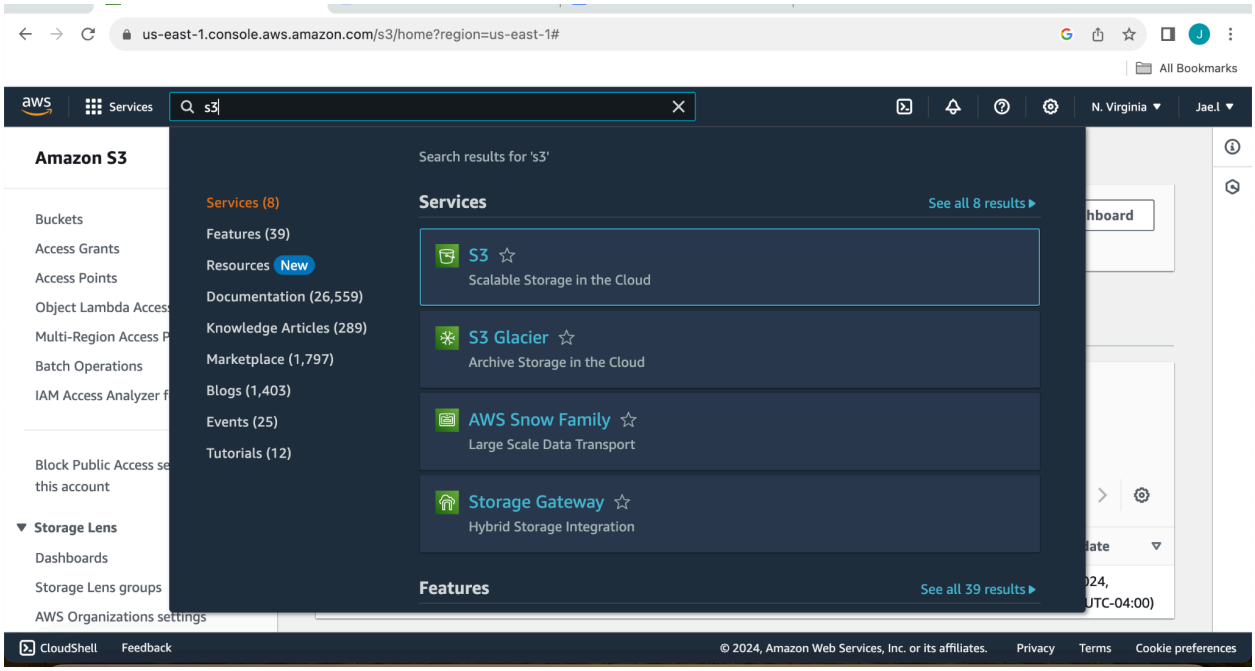
3. **Create a Customer Managed Key (CMK)**: If you don't already have a CMK, create one



4. **Note the ARN of the CMK**: After the CMK is created, note down its Amazon Resource Name (ARN). You'll need this to configure encryption for Amazon S3.



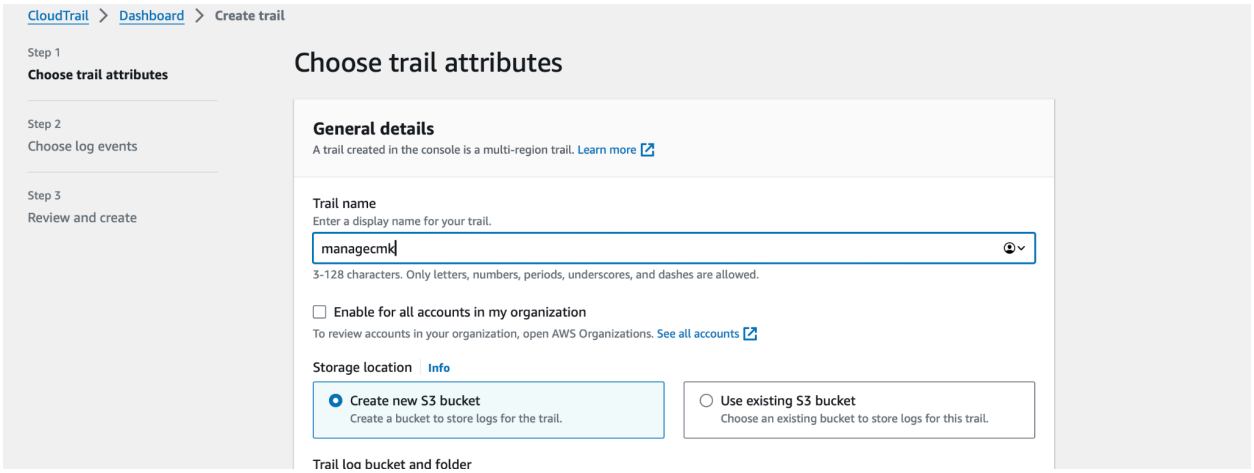
5. **Navigate to Amazon S3**: Go to the Amazon S3 console.



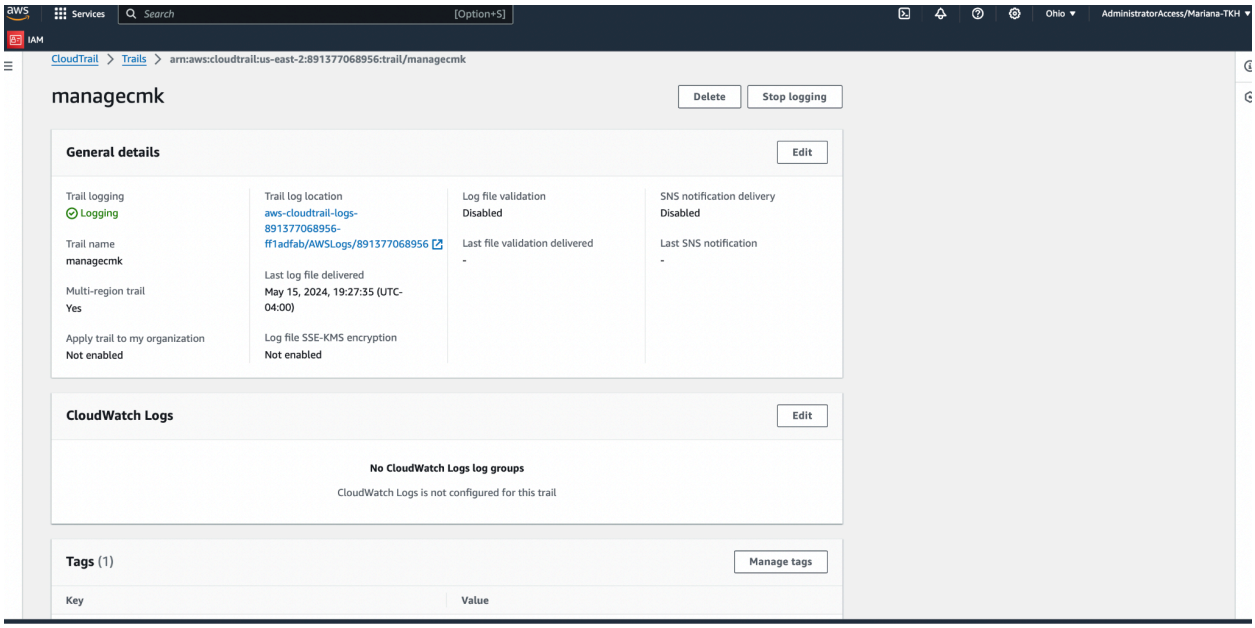
6. **Select a Bucket**: Choose the S3 bucket for which you want to enable encryption at rest.
7. **Enable Default Encryption**:
    - Click on the "Properties" tab for the selected bucket.
    - Scroll down to the "Default encryption" section.
    - Click "Edit".
    - Select "Enable" to enable default encryption.
    - Choose "AWS-KMS" as the default encryption key source.
    - Select the CMK you created earlier from the list.
    - Click "Save".
8. **Encrypt Individual Objects** (Optional): You can also encrypt individual objects uploaded to S3 using KMS-managed keys by specifying encryption options during upload. If you want to encrypt individual objects, make sure to specify the encryption settings accordingly during upload.
9. **Verify Encryption**: After enabling default encryption, any new objects uploaded to the S3 bucket will be automatically encrypted using the specified KMS-managed key. You can verify encryption by checking the encryption status of objects in the S3 console.
10. **Access and Permissions**: Ensure that IAM policies are properly configured to grant necessary permissions for users and roles to access the S3 bucket and the KMS CMK.

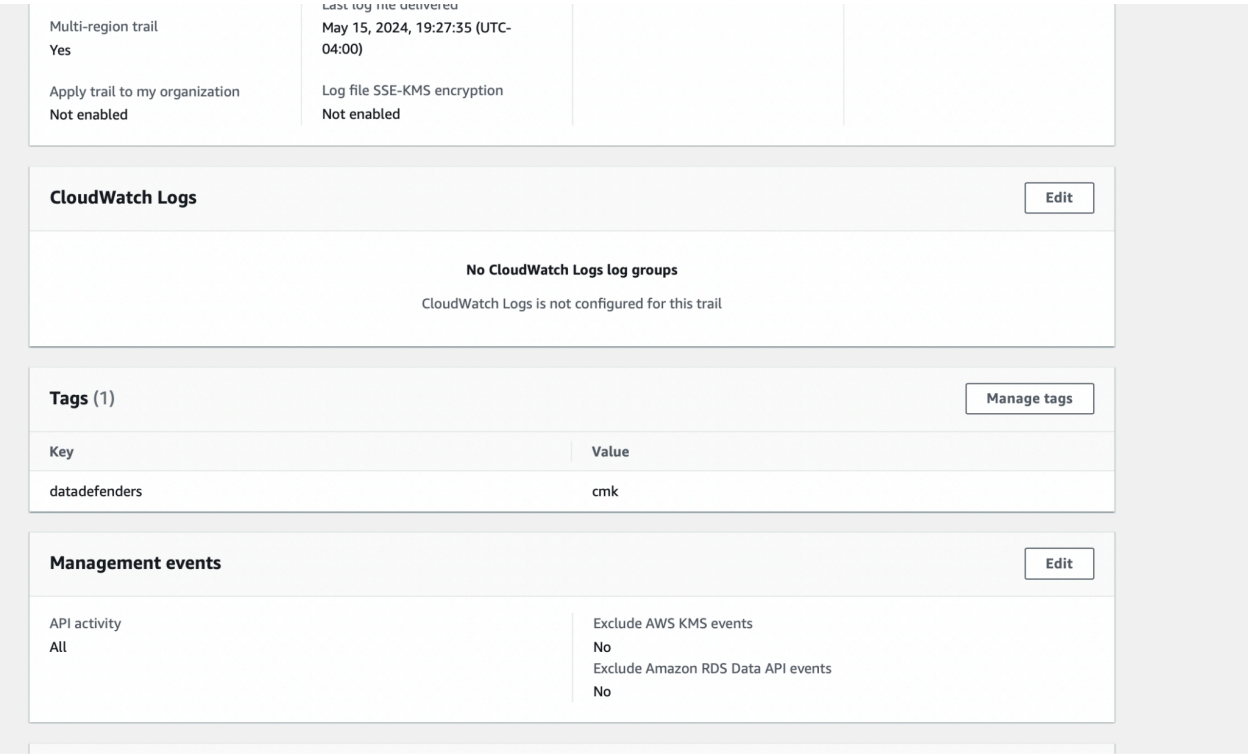
AWS CloudTrail Logging for Management Events (and KMS key events):

1. Navigate to AWS CloudTrail and click on create trail (top right).
2. Choose your trail configurations (if there is an existing s3 bucket for the logs you are capturing, choose an existing bucket otherwise create a new one to store the logs).

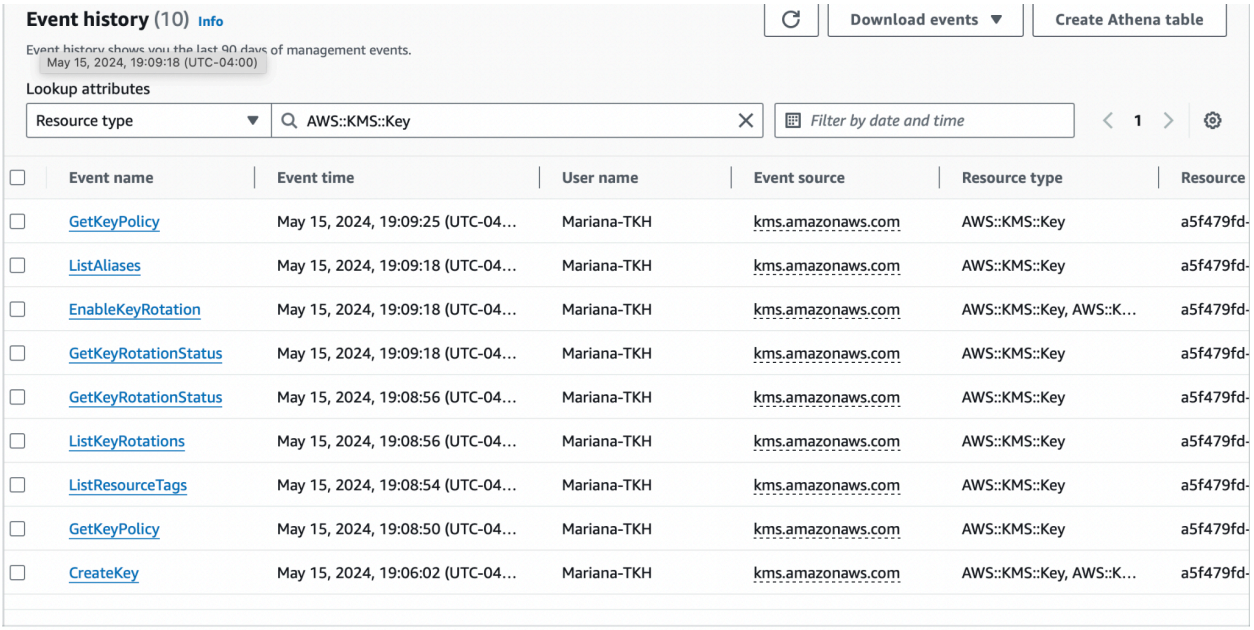


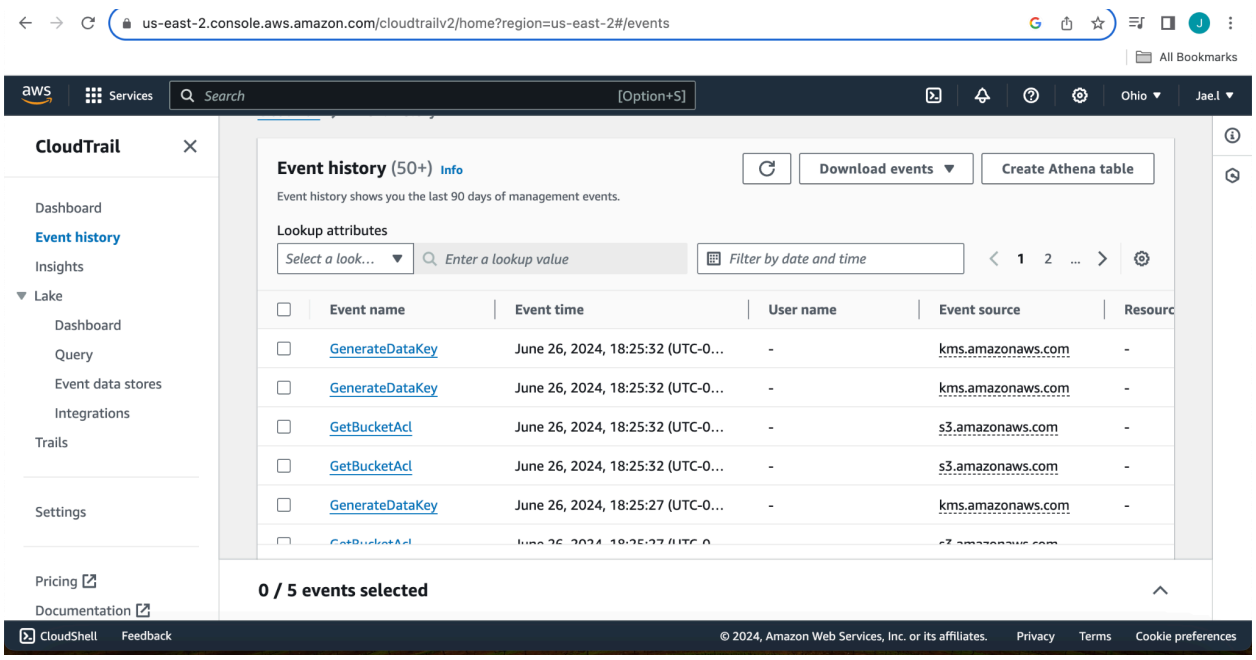
3. Verify trail was created properly (doesn't exclude KMS activity).





4. Check captured logs on the dashboard to see if KMS logs are being recorded.




us-east-2.console.aws.amazon.com/cloudtrailv2/home?region=us-east-2#/events
All Bookmarks
aws
Services
Search
[Option+S]
Ohio
Jae.l
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Create Athena table
Lookup attributes
Select a look...
Enter a lookup value
Filter by date and time
1
2
...
Event name
Event time
User name
Event source
Resourc
GenerateDataKey
June 26, 2024, 18:25:32 (UTC-0...
-
kms.amazonaws.com
GenerateDataKey
June 26, 2024, 18:25:32 (UTC-0...
-
kms.amazonaws.com
GetBucketAcl
June 26, 2024, 18:25:32 (UTC-0...
-
s3.amazonaws.com
GetBucketAcl
June 26, 2024, 18:25:32 (UTC-0...
-
s3.amazonaws.com
GenerateDataKey
June 26, 2024, 18:25:27 (UTC-0...
-
kms.amazonaws.com
0 / 5 events selected
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences