

Securing Sensitive Data in a Financial Application with AWS KMS

Technical Documentation of Secure Key Management with AWS KMS

Table of Contents

1. Introduction
2. System Overview
3. Installation
4. Configuration
5. Usage
6. Integration with Financial Application
7. Best Practices
8. Troubleshooting
9. Security Considerations
10. API Reference
11. Glossary
12. References

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)

The screenshot shows the AWS VPC Dashboard. In the main pane, there are two entries:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
dd-vpc-vpc	vpc-0403ff0bc8e714a28	Available	10.0.0.0/16	-
-	vpc-00bbe5f2f9876319c	Available	172.31.0.0/16	-

The "Details" tab is selected in the bottom navigation bar. The details for the first VPC are as follows:

Attribute	Value	Attribute	Value
VPC ID	vpc-0403ff0bc8e714a28	State	Available
Tenancy	Default	DHCP option set	dopt-0ca0e6e0c30589b27
Default VPC	No	IPv4 CIDR	10.0.0.0/16
Endpoints	-	IPv6 pool	-
Network Address Usage metrics	-	Route 53 Resolver DNS Firewall	-
Owner ID	-		

2. Within our VPC , we created an EC2 instance

The screenshot shows the AWS EC2 Instances Dashboard. There is one instance listed:

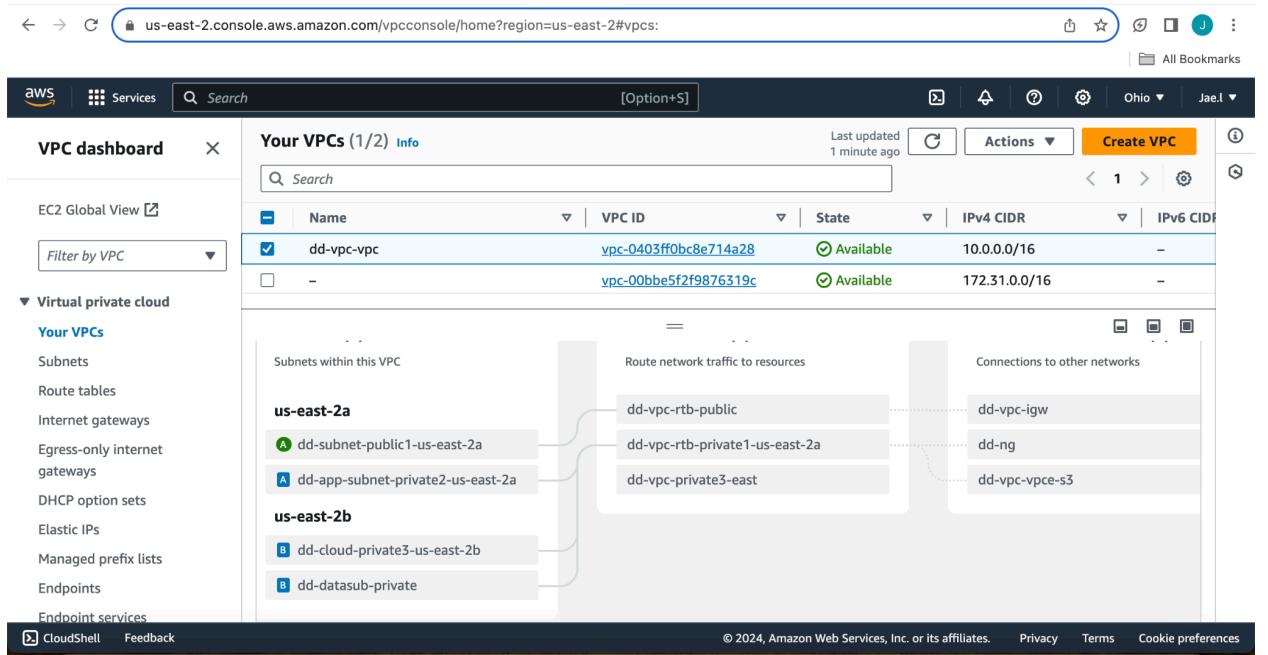
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability zone
dd-publicEC2	i-0660b645b43f9bf20	Stopped	t2.micro	-	-	us-east-2a

The "Details" tab is selected in the bottom navigation bar. The details for the instance are as follows:

Attribute	Value	Attribute	Value
Instance ID	i-0660b645b43f9bf20 (dd-publicEC2)	Public IPv4 address	-
IPv6 address	-	Instance state	Stopped

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/>

The screenshot shows the AWS Console Home page. On the left, under 'Recently visited', there is a list of services: Key Management Service, AWS Organizations, EC2, Billing and Cost Management, IAM, IAM Identity Center, CloudHSM, and AWS Billing Conductor. On the right, under 'Applications (0)', it says 'Region: US East (N. Virginia)'. There is a search bar for 'Find applications' and a button to 'Create application'. Below this, it says 'No applications' and 'Get started by creating an application.' with a 'Create application' button.

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

The screenshot shows the AWS KMS Home page. On the left, there is a sidebar with 'Key Management Service (KMS)' selected. Under it, there are sections for 'AWS managed keys' and 'Customer managed keys', and a 'Custom key stores' section with 'AWS CloudHSM key stores' and 'External key stores'. The main content area has a heading 'AWS Key Management Service' with the subtext 'Easily create keys and control encryption across AWS and beyond'. It includes a paragraph about AWS KMS being a managed service for encryption keys. On the right, there is a 'Get started now' section with a 'Create a key' button.

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

The screenshot shows the AWS KMS 'Configure key' wizard at Step 1: 'Key type'. The left sidebar lists steps from 1 to 5. The main area shows two options: 'Symmetric' (selected) and 'Asymmetric'. Both options have detailed descriptions below them.

Key type [Help me choose](#)

Symmetric
A single key used for encrypting and decrypting data or generating and verifying HMAC codes

Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage [Help me choose](#)

Encrypt and decrypt
Use the key only to encrypt and decrypt data.

Generate and verify MAC
Use the key only to generate and verify hash-based message authentication codes (HMAC).

Advanced options

4. Choose Key Type: AWS KMS supports two types of keys:

- Symmetric Key
- Asymmetric Key

This screenshot is identical to the one above, showing the 'Configure key' wizard at Step 1: 'Key type'. The 'Symmetric' key type is selected, and the 'Encrypt and decrypt' usage option is also selected. The rest of the interface, including the sidebar steps and footer, is the same.

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

Key administrators (4/14)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Name	Path	Type
Amanda	/	User
Harold	/	User
Izzy	/	User
<input checked="" type="checkbox"/> AWSReservedSSO_Administr...	/aws-reserved/sso.amazonaws...	Role
<input checked="" type="checkbox"/> AWSReservedSSO_Billing_8d3...	/aws-reserved/sso.amazonaws...	Role
<input type="checkbox"/> AWSReservedSSO_NetworkAd...	/aws-reserved/sso.amazonaws...	Role
<input checked="" type="checkbox"/> AWSReservedSSO_PowerUser...	/aws-reserved/sso.amazonaws...	Role
<input type="checkbox"/> AWSReservedSSO_ReadOnlyA...	/aws-reserved/sso.amazonaws...	Role
<input checked="" type="checkbox"/> AWSReservedSSO_SupportUs...	/aws-reserved/sso.amazonaws...	Role

Other AWS accounts

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam:: 851725462401 :root	Remove
arn:aws:iam:: 637423286818 :root	Remove

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

The screenshot shows the AWS KMS console with a green success banner at the top stating: "Your AWS KMS key was created with alias DataDefendersKey and key ID 97ecbb0c-7e75-49a5-9d56-f3e863ea428f." Below the banner, the "Customer managed keys" section displays one key entry:

Aliases	Key ID	Status	Key type	Key spec	Key usage
DataDefende...	97ecbb0c-7e...	Enabled	Symmetric	SYMMETRIC_...	Encrypt and ...

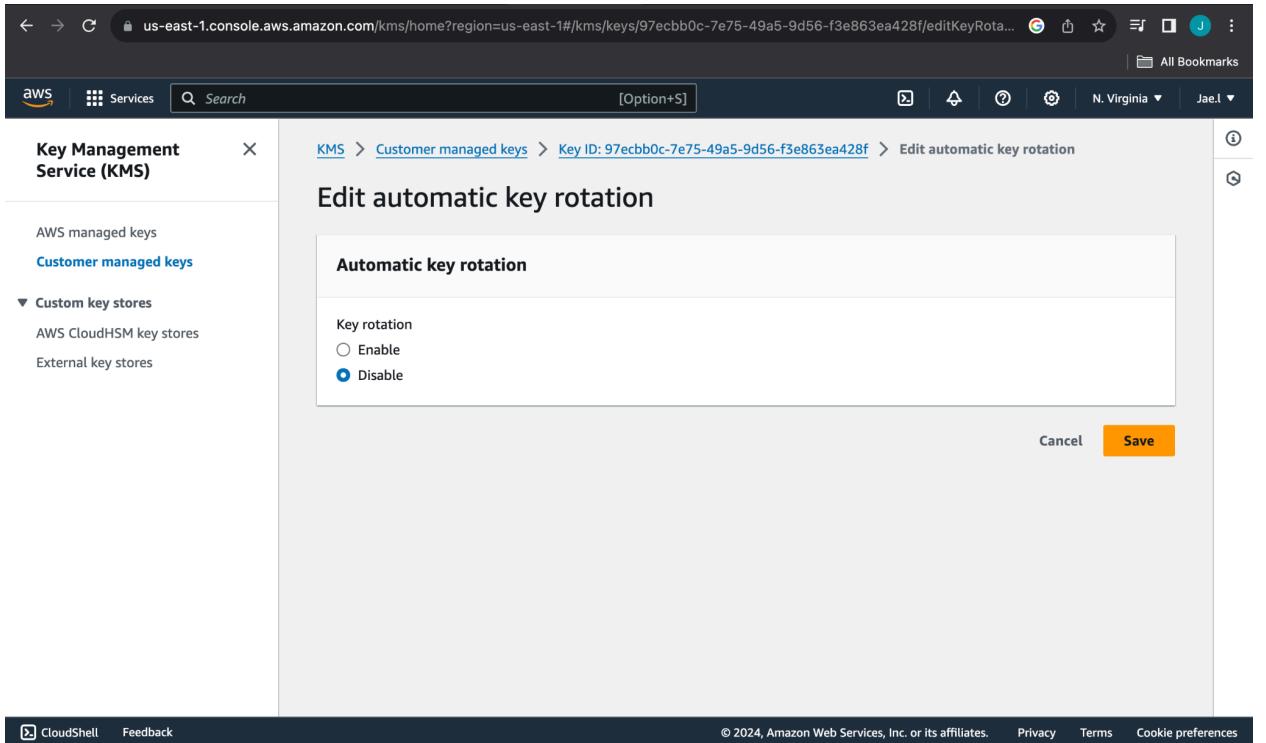
7. Edit automatic key rotation: After the key is created, select the key and click on “key rotation”

The screenshot shows the AWS KMS console on the key configuration page for the key ID 97ecbb0c-7e75-49a5-9d56-f3e863ea428f. The "General configuration" section includes the following details:

Alias	Status	Creation date
DataDefendersKey	Enabled	May 15, 2024 19:29 EDT
ARN	Description	Regionality
arn:aws:kms:us-east-1:891377068956:key/97ecbb0c-7e75-49a5-9d56-f3e863ea428f	-	Single Region

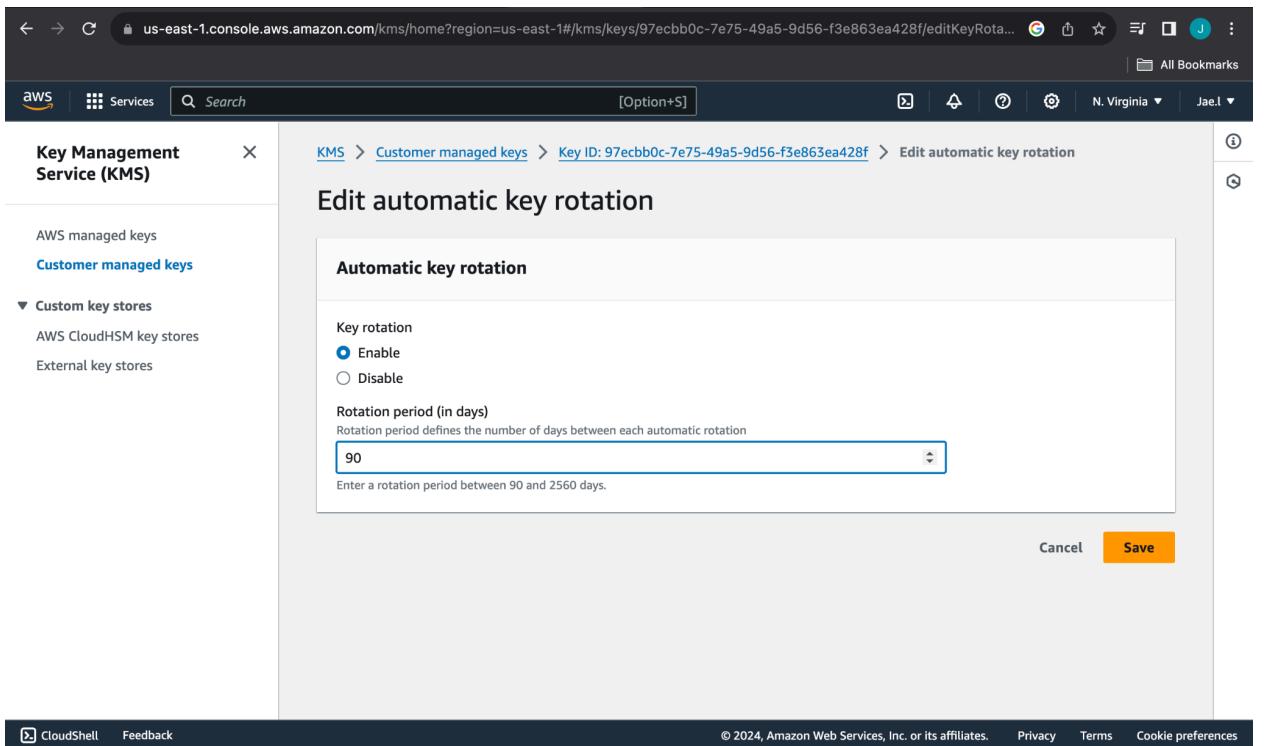
The "Key policy" tab is selected, showing the "Key policy" section with a "Switch to policy view" button. The "Key administrators" section shows two entries with "Add" and "Remove" buttons. At the bottom, there is a "Samples" link.

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



The screenshot shows the AWS KMS console. The left sidebar has 'Customer managed keys' selected under 'Custom key stores'. The main content area is titled 'Edit automatic key rotation' and contains a 'Automatic key rotation' section. In this section, there is a 'Key rotation' field with two options: 'Enable' (unchecked) and 'Disable' (checked). At the bottom right of the form are 'Cancel' and 'Save' buttons.

- **Insert rotation period days and save**



This screenshot is identical to the previous one, but the 'Rotation period (in days)' field at the bottom of the 'Automatic key rotation' section is now highlighted with a blue border, indicating it is the active input field. The value '90' is typed into the field. The rest of the interface, including the 'Key rotation' settings and the 'Save' button, remains the same.

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.

The screenshot shows the AWS Management Console Home page. At the top, there's a navigation bar with links for 'Services' and a search bar. Below the navigation bar, the 'Console Home' section is visible. On the left, a sidebar titled 'Recently visited' lists services like Key Management Service, EC2, Billing and Cost Management, IAM, IAM Identity Center, CloudHSM, and AWS Billing Conductor. To the right, there's a section titled 'Applications (0)' which says 'No applications'. It includes a 'Create application' button and a 'Find applications' search bar. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information from 2024.

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

The screenshot shows the AWS Key Management Service (KMS) home page. The left sidebar is titled 'Key Management Service (KMS)' and contains sections for 'AWS managed keys', 'Customer managed keys', and 'Custom key stores' (which is expanded to show 'AWS CloudHSM key stores' and 'External key stores'). The main content area features a large title 'AWS Key Management Service' with the subtitle 'Easily create keys and control encryption across AWS and beyond'. Below the title, a paragraph explains what KMS is and how it works. To the right, there's a 'Get started now' section with a 'Create a key' button. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information from 2024.

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.

The screenshot shows the AWS KMS console in a web browser. The URL is `us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys`. A success message at the top right states: "Your AWS KMS key was created with alias DataDefendersDataKey and key ID b7097c06-d575-4634-98c5-328b945496d0." Below this, the "Customer managed keys" section is displayed. The table lists two keys:

Aliases	Key ID	Status	Key type	Key spec	Key usage
DataDefende...	97ecbb0c-7e...	Enabled	Symmetric	SYMMETRIC_...	Encrypt and ...
<input checked="" type="checkbox"/> DataDefende...	b7097c06-d...	Enabled	Symmetric	SYMMETRIC_...	Encrypt and ...

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.

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.

The screenshot shows the AWS KMS console for a key named "jlazeberry.fellow". The terminal window displays the following command history:

```
update-alias          | update-custom-key-store
update-key-description | update-primary-region
verify                | verify-mac
help
jlazeberry.fellow@tkhadminatl-Air ~ % generate-data-key
zsh: command not found: generate-data-key
jlazeberry.fellow@tkhadminatl-Air ~ % aws kms generate-data-key --key-id b7097c06-d575-4634-98c5-328b945496d0 --key-spec AES_256
06-d575-4634-98c5-328b945496d0 --key-spec AES_256
{
    "CiphertextBlob": "AQIDAHHmYoEraQAGSr56H1DjFLx7vZtZicvu4Nt6dG0iyRwEZhXkk
DntIjv3gbblsA/kdAAAfjBBgqkhkIGwBbwgbzbtaGeAMgGCSqSGlz3DQEHTAbglhgkZOMEA
S4wEQM0E9MwAhuo5AgEqDv/W3IEjl3Wznej87B/aEZo06EB6r0qMBFw90nybkYla0kC0Oj
bClRy06n9dkgqGCF1SA+nM6J8tws=",
    "Plaintext": "2KSvw#TF85tbnhZlqxHOfHVGAE234ieF8zM4wBnhHu0",
    "KeyId": "arn:aws:kms:us-east-1:891377068956:key/b7097c06-d575-4634-98c5-328b945496d0"
}
jlazeberry.fellow@tkhadminatl-Air ~ %
```

The right side of the screen shows the key details:

- Key actions ▾
- Edit
- Creation date: May 15, 2024 22:04 EDT
- Regionality: Single Region

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.

```

google.com/document/d/1DO5UIMJGV99lI_BnqQ02fMFGponZ5mN774VpTodXgoY/edit

Sprint 2 Insert Format Tools Extensions Help
Normal text Times ... 12 B I U A
jlazenberry.fellow --zsh - 80x24
1
-h, --help      display this message
-i, --input     input file (default: "-" for stdin)
-o, --output    output file (default: "-" for stdout)
jlazenberry.fellow@tkhadmiatis-Air ~ % echo AQIDAHHmYoDEraQAGSr56HlDj2fLX7vzTzIi
cvu4Ntdd0iyRwEZAxhkKnTijv3Gbb1Sa/kdAAAAfjBBBqkqhkjG9wB8wagbzBtAgEAMGgCSqGS1b3
DQEHTAeBg1ghkbZOMEAS4WEQQME0vMA8huo9U8Nb5AgEqQDv/W3IEjl3Wznej87B/a8EZo06EB6r0
qMBtfw9OnybkYla0kC00jbClr8Yoón9DkggQCFF1SA+nM6J0tw== | base64 --decode > /Users/
jlazenberry.fellow/Documents/Capstone/keys
zsh: is a directory: /Users/jlazenberry.fellow/Documents/Capstone/keys
jlazenberry.fellow@tkhadmiatis-Air ~ % cat /Users/jlazenberry.fellow/Documents/C
apstone/keys
cat: /Users/jlazenberry.fellow/Documents/Capstone/keys: Is a directory
jlazenberry.fellow@tkhadmiatis-Air ~ % ls -l /Users/jlazenberry.fellow/Documents/
/Capstone/keys
total 0
jlazenberry.fellow@tkhadmiatis-Air ~ % echo AQIDAHHmYoDEraQAGSr56HlDj2fLX7vzTzIi
cvu4Ntdd0iyRwEZAxhkKnTijv3Gbb1Sa/kdAAAAfjBBBqkqhkjG9wB8wagbzBtAgEAMGgCSqGS1b3
DQEHTAeBg1ghkbZOMEAS4WEQQME0vMA8huo9U8Nb5AgEqQDv/W3IEjl3Wznej87B/a8EZo06EB6r0
qMBtfw9OnybkYla0kC00jbClr8Yoón9DkggQCFF1SA+nM6J0tw== | base64 --decode > enc_dat
a_key.bin
jlazenberry.fellow@tkhadmiatis-Air ~ % cat enc_data_key.bin
00000000? ?He.0.??f?b??6+Gdt??m?Rk?=? *?R?
K?n????T?y?:?l????w?Rk?=?n?W?mN?&?bV??#?????F(?QuH?3?t??
jlazenberry.fellow@tkhadmiatis-Air ~ %

```

8. **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.

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

docs.google.com/document/d/1DO5UIMJGV99II_BnqQ02fMFGponZ5mN774VpTodXgoY/edit

DataDefender-Sprint 2

File Edit View Insert Format Tools Extension

Downloads -- zsh - 80x24

```
opiclab
3565590446282478,Nikola Colt,4/27/2024,752,15945 Continental Park,Faaa,,jcb,Jax
works
3545676021963387,Oneida Farnborough,7/6/2023,153,645 Vermont Parkway,Kariet Ark
ane,,jcb,Yozio
63846745570466133,Chaunce Dand,7/6/2024,740,22318 Dayton Trail,Meijiang,,,maestr
o,Divape
3561919193965163,Dani Davisson,7/11/2025,491,724 Roxbury Crossing,Kalianda,,jcb
,Blognation
201581575787870,Jacklyn Blowfield,9/24/2022,104,33598 Debs Lane,Balugo,,1001,din
ers-club-enroute,Jabbersphere
675954288408533871,Alick Gantz,2/3/2024,171,4 Mallory Pass,Oakland,CA,94622,maes
tro,Blogtags
3537659908193294,Renaldo Goulston,11/6/2025,212,9571 Corben Avenue,Liu Xia,.,jcb,F
liptune
374283708420021,Reece Blanckley,8/13/2024,265,7 Annamark Drive,Margamukti,,,amer
icanexpress,Latz
3578966812886131,Sibbie Antoons,6/3/2024,804,394 Maryland Park,Itajai,,88300-000
,jcb,Thoughtbeat
jlazeberry.fellow@tkhadminatl-Air downloads % openssl enc -aes-256-cbc -pbkdf2
-in financial.csv -out encrypted_financial.csv -pass pass:2KSvwbtF8St6hZlqxH0ff
VGEA2J4MieF8zkwBnHu0=
jlazeberry.fellow@tkhadminatl-Air downloads %
```

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.

Here our encrypted file says “salted” .

docs.google.com/document/d/1DO5UIMJGV99II_BnqQ02fMFGponZ5mN774VpTodXgoY/edit

DataDefender-Sprint 2

File Edit View Insert Format Tools Extension

Downloads -- zsh - 80x24

```
works
3545676021963387,Oneida Farnborough,7/6/2023,153,645 Vermont Parkway,Kariet Ark
ane,,jcb,Yozio
63846745570466133,Chaunce Dand,7/6/2024,740,22318 Dayton Trail,Meijiang,,,maestr
o,Divape
3561919193965163,Dani Davisson,7/11/2025,491,724 Roxbury Crossing,Kalianda,,jcb
,Blognation
201581575787870,Jacklyn Blowfield,9/24/2022,104,33598 Debs Lane,Balugo,,1001,din
ers-club-enroute,Jabbersphere
675954288408533871,Alick Gantz,2/3/2024,171,4 Mallory Pass,Oakland,CA,94622,maes
tro,Blogtags
3537659908193294,Renaldo Goulston,11/6/2025,212,9571 Corben Avenue,Liu Xia,.,jcb,F
liptune
374283708420021,Reece Blanckley,8/13/2024,265,7 Annamark Drive,Margamukti,,,amer
icanexpress,Latz
3578966812886131,Sibbie Antoons,6/3/2024,804,394 Maryland Park,Itajai,,88300-000
,jcb,Thoughtbeat
jlazeberry.fellow@tkhadminatl-Air downloads % openssl enc -aes-256-cbc -pbkdf2
-in financial.csv -out encrypted_financial.csv -pass pass:2KSvwbtF8St6hZlqxH0ff
VGEA2J4MieF8zkwBnHu0=
jlazeberry.fellow@tkhadminatl-Air downloads %
Salted_
jlazeberry.fellow@tkhadminatl-Air downloads %
```

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.

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.

The screenshot shows the AWS Management Console Home page. The left sidebar lists recently visited services: Key Management Service, EC2, Billing and Cost Management, IAM, IAM Identity Center, CloudHSM, and AWS Billing Conductor. The main content area is titled "Console Home" and shows the "Applications" section. It displays a message: "No applications. Get started by creating an application." A "Create application" button is visible. The top navigation bar includes tabs for "Services", "Search", and "CloudShell". The bottom footer contains links for "Feedback", "CloudShell", "Feedback", and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

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

The screenshot shows the AWS Key Management Service (KMS) console home page. The left sidebar has sections for "Key Management Service (KMS)", "AWS managed keys", "Customer managed keys", and "Custom key stores" (with options for "AWS CloudHSM key stores" and "External key stores"). The main content area features the title "AWS Key Management Service" and the subtext "Easily create keys and control encryption across AWS and beyond". Below this is a paragraph about AWS KMS and a "Get started now" section with a "Create a key" button. The top navigation bar includes tabs for "Services", "Search", and "CloudShell". The bottom footer contains links for "Feedback", "CloudShell", "Feedback", and copyright information: "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

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

The screenshot shows the AWS KMS console with the URL us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys. The left sidebar has sections for 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys' (which is selected), and 'Custom key stores'. The main area is titled 'Customer managed keys (2)' and contains a table with two rows. The first row has an alias 'DataDefende...', a key ID '97ecbb0c-7e...', and is disabled. The second row has an alias 'DataDefende...', a key ID 'b7097c06-d...', and is also disabled. The table includes columns for Aliases, Key ID, Status, Key type, Key spec, and Key usage.

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.

The screenshot shows the AWS KMS console with the URL us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys/97ecbb0c-7e75-49a5-9d56-f3e863ea428f. The left sidebar is identical to the previous screenshot. The main area shows the details for the key with the ARN 'arn:aws:kms:us-east-1:891377068956:key/97ecbb0c-7e75-49a5-9d56-f3e863ea428f'. A tooltip 'ARN copied' appears over the ARN value. Below the ARN, there are sections for General configuration, Key policy, Cryptographic configuration, Tags, Key rotation, and Aliases. The 'Key policy' tab is currently selected. At the bottom right of the main area, there is an 'Edit' button.

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

The screenshot shows the AWS search interface with the query 's3' entered in the search bar. The results are categorized under 'Services' and 'Features'. The 'Services' section contains cards for S3 (Scalable Storage in the Cloud), S3 Glacier (Archive Storage in the Cloud), AWS Snow Family (Large Scale Data Transport), and Storage Gateway (Hybrid Storage Integration). The 'Features' section contains a card for 'See all 39 results' for Features. The left sidebar shows navigation links for Buckets, Access Grants, Access Points, Object Lambda Access, Multi-Region Access, Batch Operations, IAM Access Analyzer, and Storage Lens.

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".

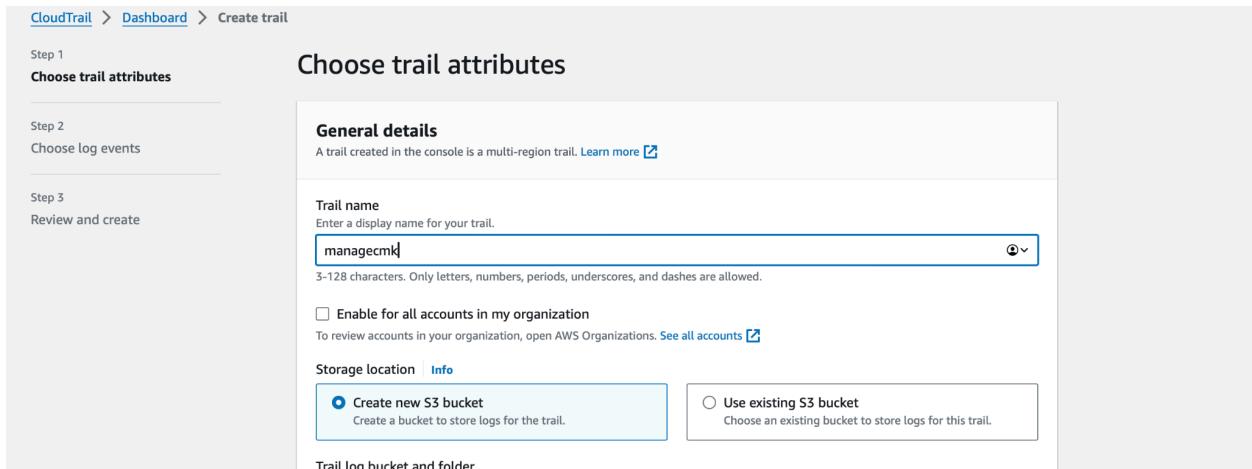
8. **Encrypt Individual Objects (Optional):** You can also encrypt individual objects uploaded to S3 using KMS-managed keys by specifying encryption options during upload. If you want to encrypt individual objects, make sure to specify the encryption settings accordingly during upload.

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.

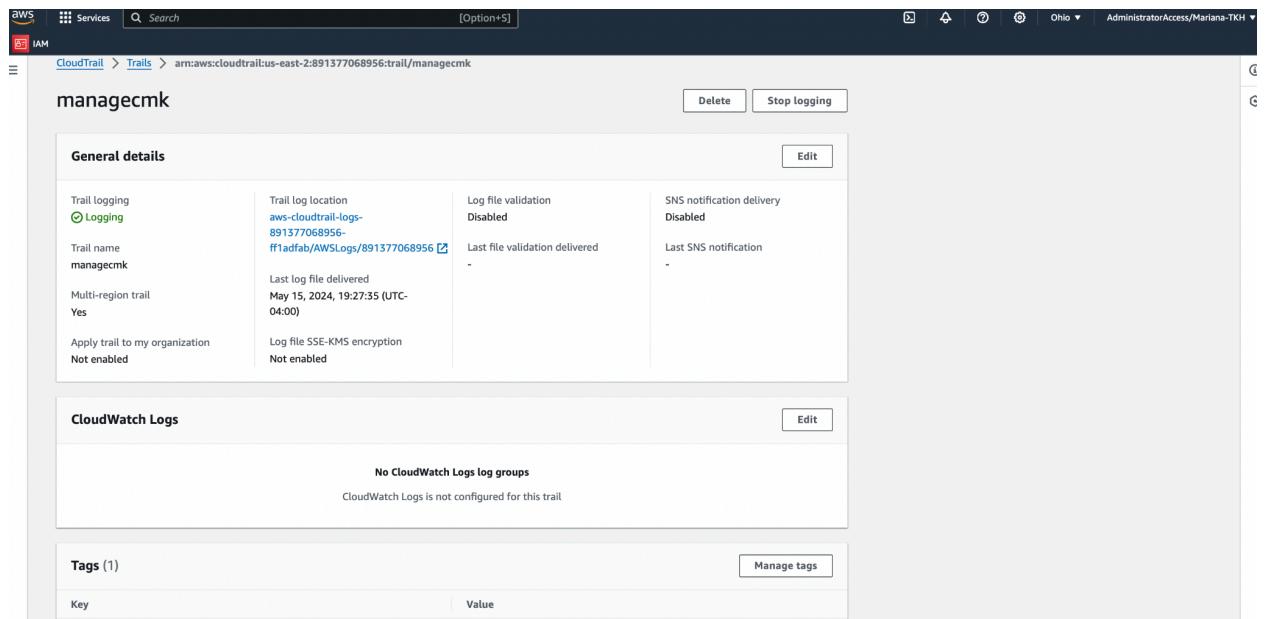
10. **Access and Permissions:** Ensure that IAM policies are properly configured to grant necessary permissions for users and roles to access the S3 bucket and the KMS CMK.

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).



Multi-region trail
Yes

Last log file delivered
May 15, 2024, 19:27:35 (UTC-04:00)

Apply trail to my organization
Not enabled

Log file SSE-KMS encryption
Not enabled

CloudWatch Logs

No CloudWatch Logs log groups

CloudWatch Logs is not configured for this trail

Tags (1)

Key	Value
datadefenders	cmk

Management events

API activity	Exclude AWS KMS events
All	No
	Exclude Amazon RDS Data API events
	No

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

Event history (10) Info					
Event history shows you the last 90 days of management events. May 15, 2024, 19:09:18 (UTC-04:00)					
Lookup attributes					
Resource type	▼	<input type="text"/> AWS::KMS::Key	X	<input type="button"/> Filter by date and time	
<input type="checkbox"/>	Event name	Event time	User name	Event source	Resource type
<input type="checkbox"/>	GetKeyPolicy	May 15, 2024, 19:09:25 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	ListAliases	May 15, 2024, 19:09:18 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	EnableKeyRotation	May 15, 2024, 19:09:18 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key, AWS::K...
<input type="checkbox"/>	GetKeyRotationStatus	May 15, 2024, 19:09:18 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	GetKeyRotationStatus	May 15, 2024, 19:08:56 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	ListKeyRotations	May 15, 2024, 19:08:56 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	ListResourceTags	May 15, 2024, 19:08:54 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	GetKeyPolicy	May 15, 2024, 19:08:50 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key
<input type="checkbox"/>	CreateKey	May 15, 2024, 19:06:02 (UTC-04...	Mariana-TKH	kms.amazonaws.com	AWS::KMS::Key, AWS::K...

The screenshot shows the AWS CloudTrail Event history page. The left sidebar includes links for Dashboard, Event history (selected), Insights, Lake (Dashboard, Query, Event data stores, Integrations), Trails, Settings, Pricing, and Documentation. The main content area displays a table of event history with columns for Event name, Event time, User name, Event source, and Resource. The table lists several events, all of which are GenerateDataKey operations. The most recent event is at the top of the list.

	Event name	Event time	User name	Event source	Resource
<input type="checkbox"/>	GenerateDataKey	June 26, 2024, 18:25:32 (UTC-0...)	-	kms.amazonaws.com	-
<input type="checkbox"/>	GenerateDataKey	June 26, 2024, 18:25:32 (UTC-0...)	-	kms.amazonaws.com	-
<input type="checkbox"/>	GetBucketAcl	June 26, 2024, 18:25:32 (UTC-0...)	-	s3.amazonaws.com	-
<input type="checkbox"/>	GetBucketAcl	June 26, 2024, 18:25:32 (UTC-0...)	-	s3.amazonaws.com	-
<input type="checkbox"/>	GenerateDataKey	June 26, 2024, 18:25:27 (UTC-0...)	-	kms.amazonaws.com	-
<input type="checkbox"/>	GetBucketAcl	June 26, 2024, 18:25:27 (UTC-0...)	-	s3.amazonaws.com	-