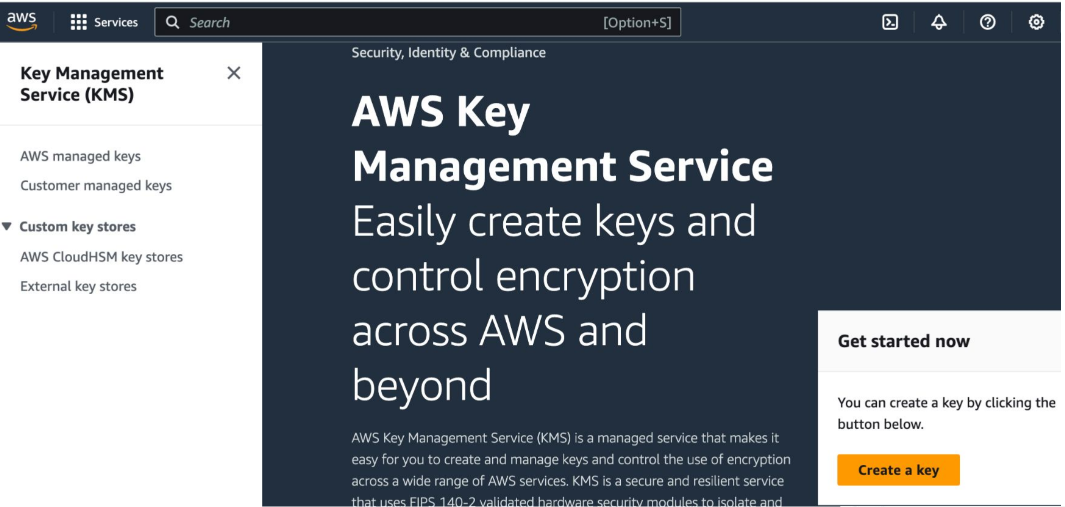
SECURING SENSITIVE DATA WITH AWS KMS AND CLOUDHSM

TEAM: DATA DEFENDERS

OBJECTIVE

- Our capstone project aims to secure sensitive data using keys generated and managed through AWS KMS.

- Our project aims to use AWS KMS for cryptographic operations to ensure data is encrypted and only accessible by those who should have access.



Security, Identity & Compliance

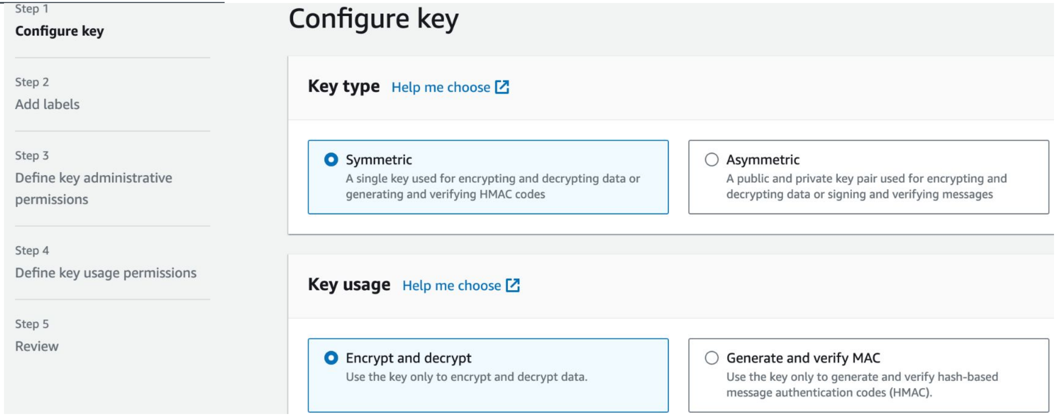
AWS Key Management Service

Easily create keys and control encryption across AWS and beyond

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and

Get started now

You can create a key by clicking the button below.



Configure key

Key type

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

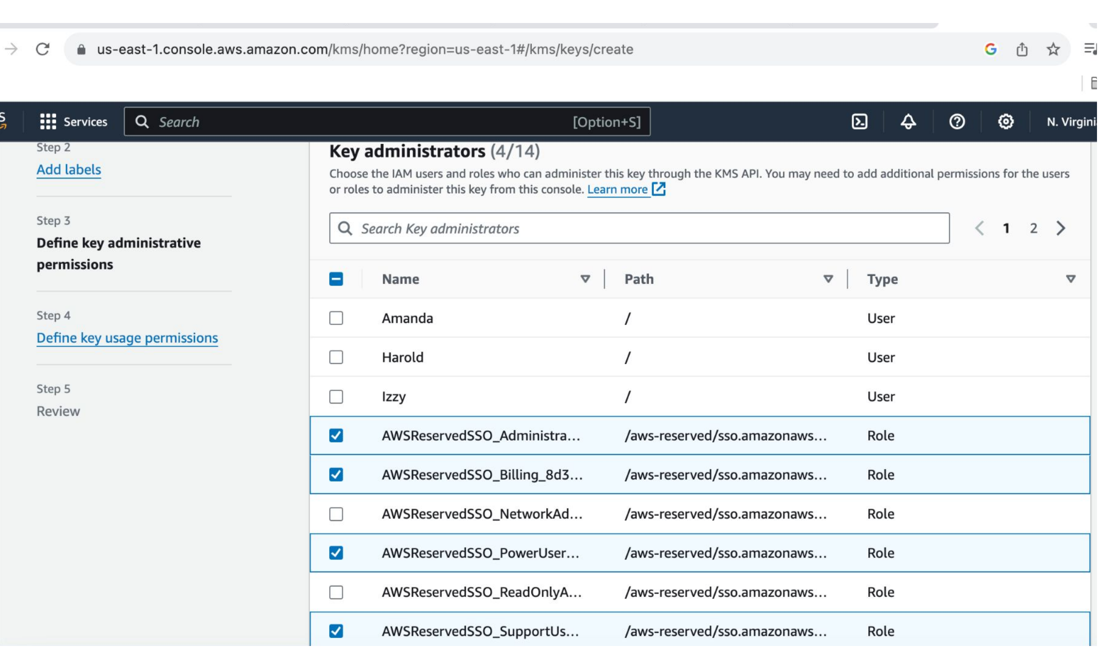
○ Asymmetric
A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage

● 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).

KEY CREATION VIA AWS KMS CONSOLE



us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys/create

Step 2
Add labels

Step 3
Define key administrative permissions

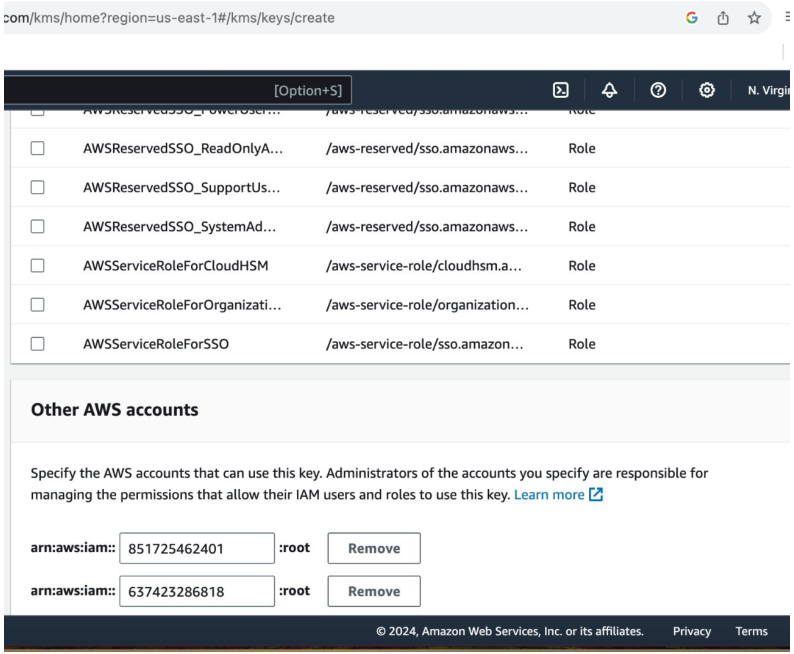
Step 4
Define key usage permissions

Step 5
Review

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
☑	AWSReservedSSO_Administra…	/aws-reserved/sso.amazonaws…	Role
☑	AWSReservedSSO_Billing_8d3…	/aws-reserved/sso.amazonaws…	Role
□	AWSReservedSSO_NetworkAd…	/aws-reserved/sso.amazonaws…	Role
☑	AWSReservedSSO_PowerUser…	/aws-reserved/sso.amazonaws…	Role
□	AWSReservedSSO_ReadOnlyA…	/aws-reserved/sso.amazonaws…	Role
☑	AWSReservedSSO_SupportUs…	/aws-reserved/sso.amazonaws…	Role



com/kms/home?region=us-east-1#/kms/keys/create

□	AWSReservedSSO_PowerUser…	/aws-reserved/sso.amazonaws…	Role
□	AWSReservedSSO_ReadOnlyA…	/aws-reserved/sso.amazonaws…	Role
□	AWSReservedSSO_SupportUs…	/aws-reserved/sso.amazonaws…	Role
□	AWSReservedSSO_SystemAd…	/aws-reserved/sso.amazonaws…	Role
□	AWSServiceRoleForCloudHSM	/aws-service-role/cloudhsm.a…	Role
□	AWSServiceRoleForOrganizati…	/aws-service-role/organization…	Role
□	AWSServiceRoleForSSO	/aws-service-role/sso.amazon…	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

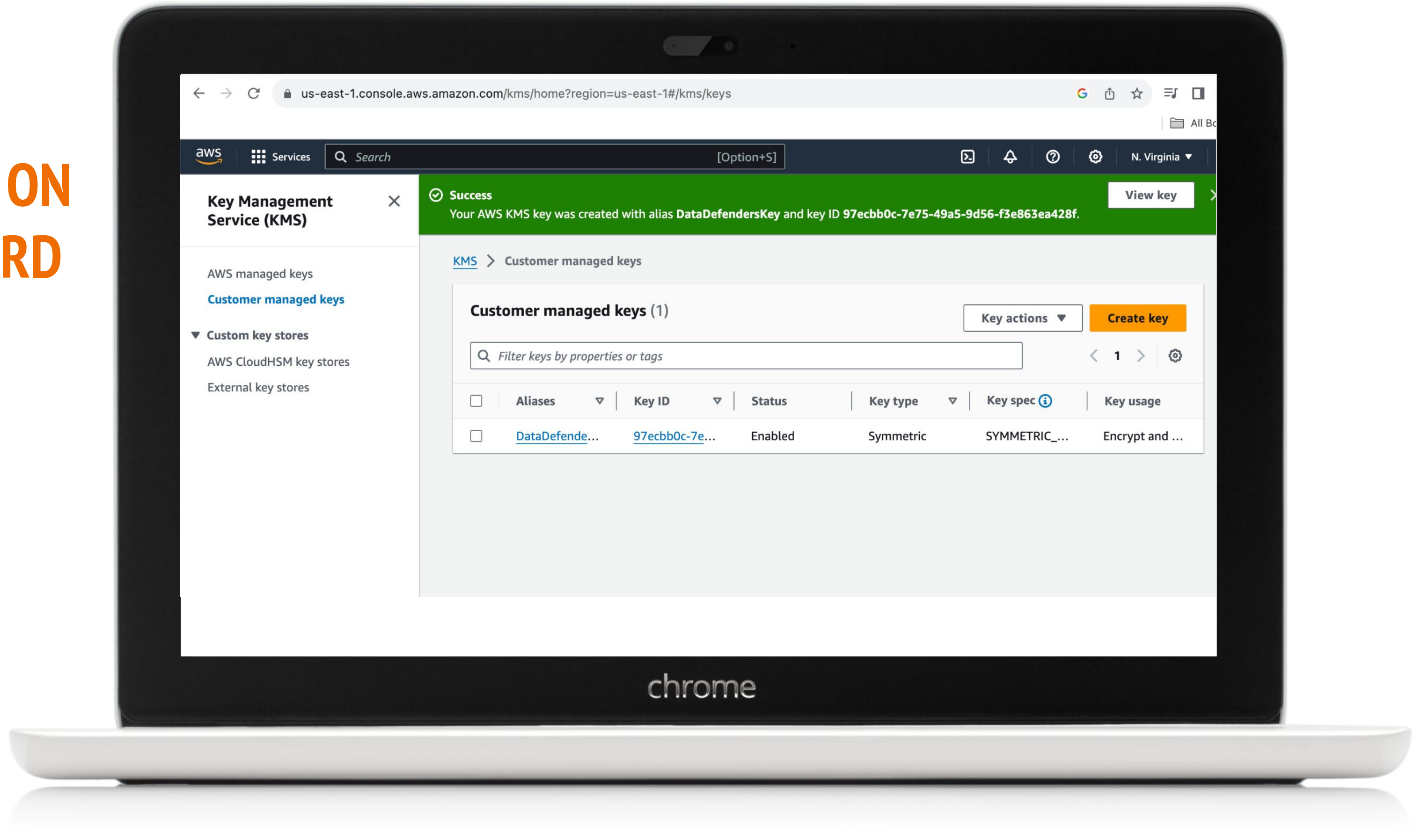
arn:aws:iam:: 637423286818 :root Remove

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms

CMK KEY ADMINISTRATORS

CMK KEY USAGE PERMISSIONS

FINALIZED KEY ON CMK DASHBOARD



us-east-1.console.aws.amazon.com/kms/home?region=us-east-1#/kms/keys

Key Management Service (KMS)

AWS managed keys

Customer managed keys

▼ Custom key stores

AWS CloudHSM key stores

External key stores

Success
Your AWS KMS key was created with alias **DataDefendersKey** and key ID **97ecbb0c-7e75-49a5-9d56-f3e863ea428f**.

View key

KMS > Customer managed keys

Customer managed keys (1)

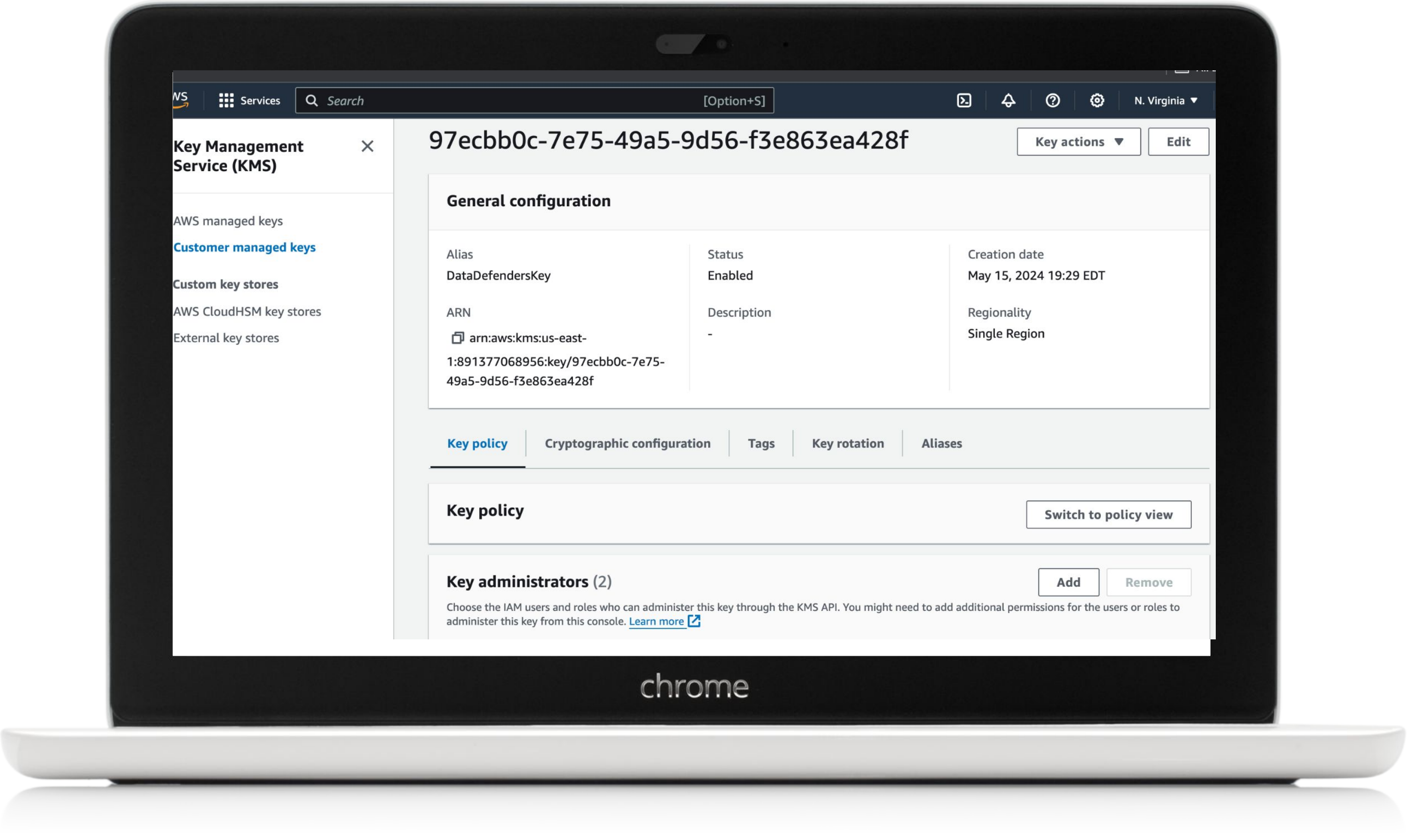
Key actions ▼ | Create key

Filter keys by properties or tags

< 1 >

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

REVIEW FINALIZED KEY CONFIGURATION



97ecbb0c-7e75-49a5-9d56-f3e863ea428f

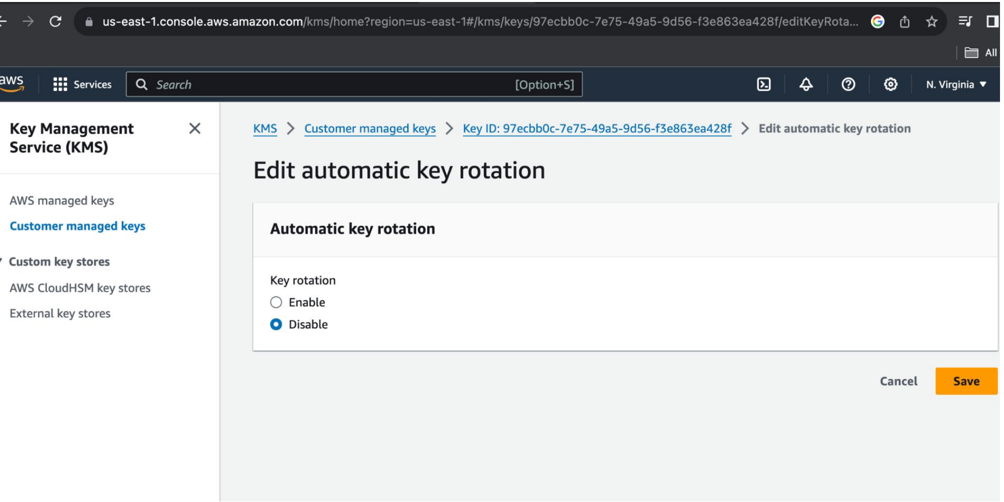
General configuration

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

Key policy

Key administrators (2)

Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key from this console. Learn more

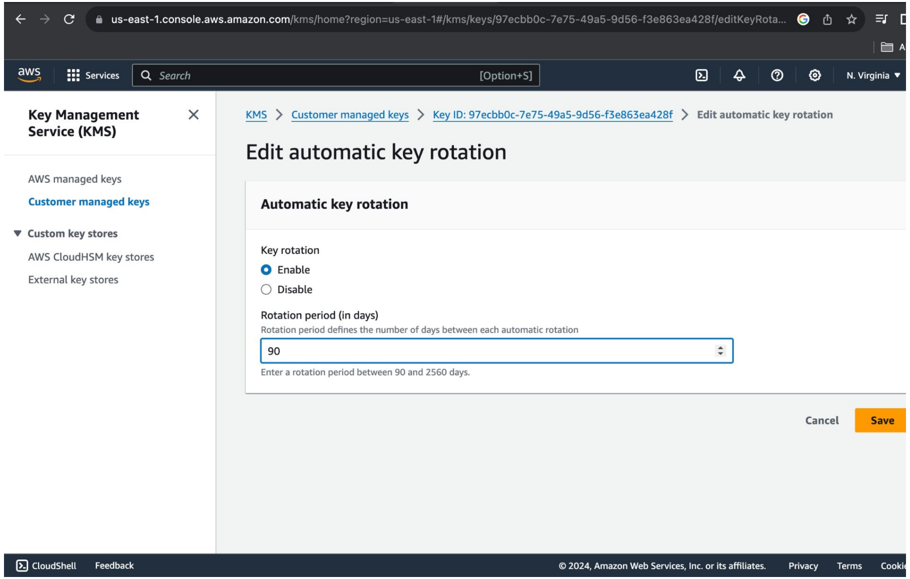


us-east-1.console.amazon.com/kms/home?region=us-east-1#/kms/keys/97ecbb0c-7e75-49a5-9d56-f3e863ea428f/editKeyRota...
All
aws
Services
Search
[Option+S]
N. Virginia
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
KMS > Customer managed keys > Key ID: 97ecbb0c-7e75-49a5-9d56-f3e863ea428f > Edit automatic key rotation
Cancel
Save

Edit automatic key rotation

Automatic key rotation

Key rotation
○ Enable
● Disable



us-east-1.console.amazon.com/kms/home?region=us-east-1#/kms/keys/97ecbb0c-7e75-49a5-9d56-f3e863ea428f/editKeyRota...
aws
Services
Search
[Option+S]
N. Virginia
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
KMS > Customer managed keys > Key ID: 97ecbb0c-7e75-49a5-9d56-f3e863ea428f > Edit automatic key rotation
Cancel
Save
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cooki

Edit automatic key rotation

Automatic key rotation

Key rotation
● Enable
○ Disable

Rotation period (in days)
Rotation period defines the number of days between each automatic rotation
90
Enter a rotation period between 90 and 2560 days.

KEY ROTATION

KEY ROTATION IS DISABLED BY DEFAULT ON AWS KMS FOR CUSTOMER MANAGED KEYS.

ENABLE AUTOMATIC KEY ROTATION

SET ROTATION PERIOD (DEFAULT IS 365 DAYS AKA YEARLY ROTATION).

WHY USE CLOUD HSM?

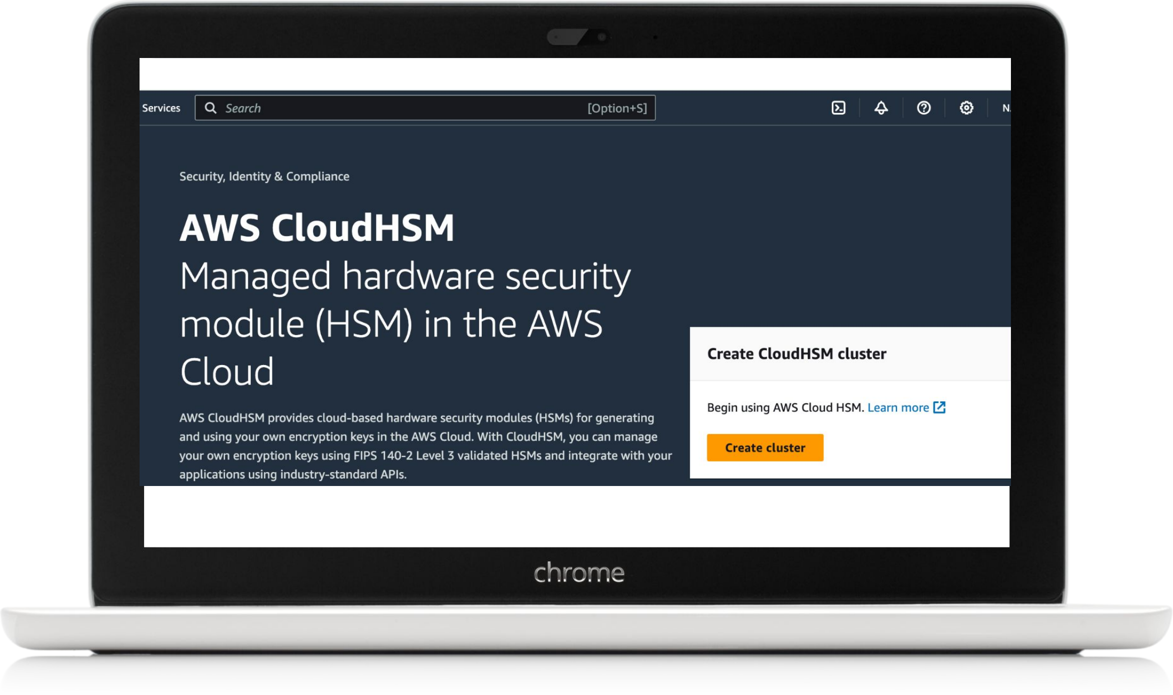
- AWS CloudHSM allows us to have dedicated hardware security modules (HSMs) for our cryptographic keys.

- An HSM is a computing device that processes cryptographic operations and securely stores our keys.

- If their operations involve sensitive data, organizations can use CloudHSM to meet compliance security standards for managing and storing private keys that protect highly confidential data. The HSMs provided by AWS CloudHSM are FIPS 140-2 level 3 certified and comply with PCI DSS requirements.

GENERATING A CLOUDHSM CLUSTER

NAVIGATE TO AWS CLOUDHSM USING CONSOLE SEARCH FUNCTION AND CLICK CREATE CLUSTER.



Security, Identity & Compliance

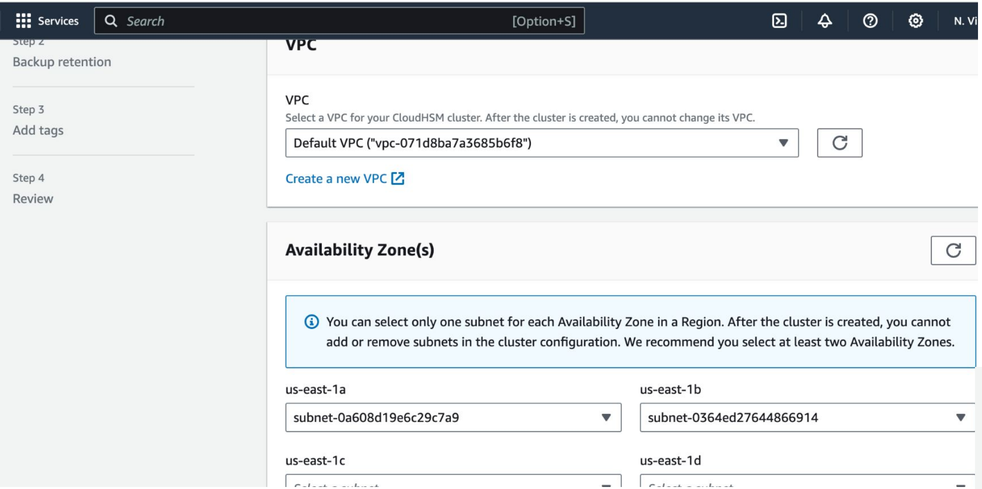
AWS CloudHSM

Managed hardware security module (HSM) in the AWS Cloud

AWS CloudHSM provides cloud-based hardware security modules (HSMs) for generating and using your own encryption keys in the AWS Cloud. With CloudHSM, you can manage your own encryption keys using FIPS 140-2 Level 3 validated HSMs and integrate with your applications using industry-standard APIs.

Create CloudHSM cluster

Begin using AWS Cloud HSM. Learn more



Step 2
Backup retention

Step 3
Add tags

Step 4
Review

VPC

VPC
Select a VPC for your CloudHSM cluster. After the cluster is created, you cannot change its VPC.
Default VPC ("vpc-071d8ba7a3685b6f8")

Create a new VPC

Availability Zone(s)

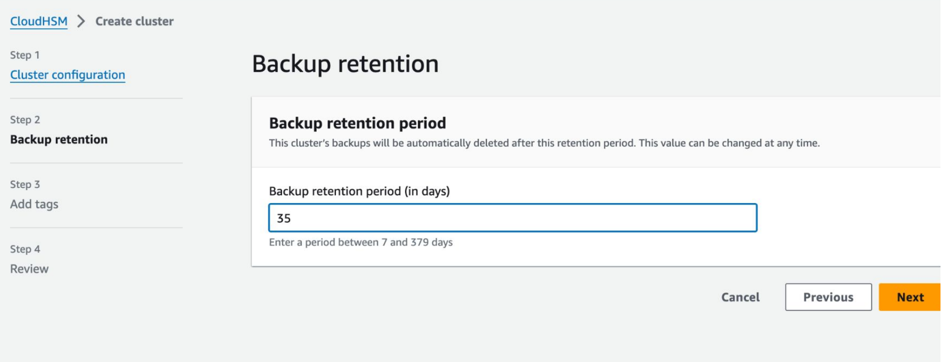
You can select only one subnet for each Availability Zone in a Region. After the cluster is created, you cannot add or remove subnets in the cluster configuration. We recommend you select at least two Availability Zones.

us-east-1a
subnet-0a608d19e6c29c7a9

us-east-1b
subnet-0364ed27644866914

us-east-1c
Select a subnet

us-east-1d
Select a subnet


CloudHSM > Create cluster

Step 1
Cluster configuration

Step 2
Backup retention

Step 3
Add tags

Step 4
Review

Backup retention

Backup retention period
This cluster's backups will be automatically deleted after this retention period. This value can be changed at any time.

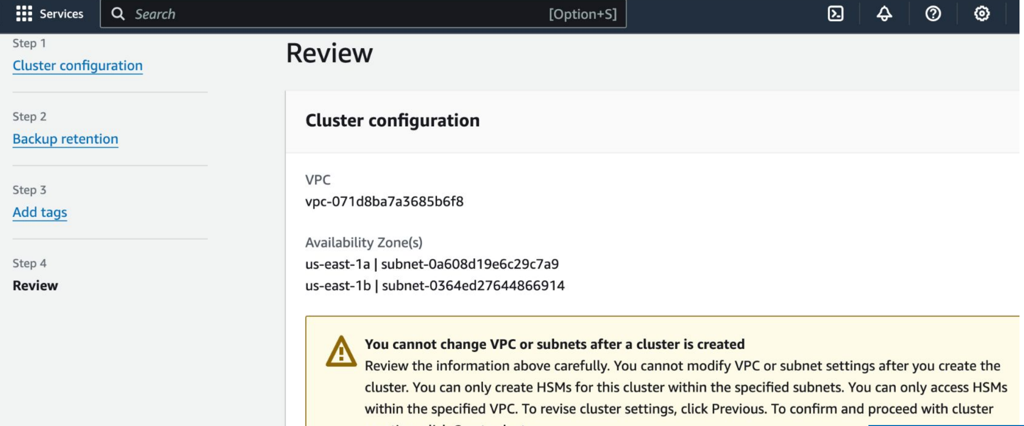
Backup retention period (in days)
35
Enter a period between 7 and 379 days

NETWORK CONFIGURATIONS FOR CLOUDHSM CLUSTER

SELECT VPC, AVAILABILITY ZONES, AND SUBNETS WHERE YOUR CLOUDHSM CLUSTER WILL BE LOCATED. SELECT MULTIPLE AZs FOR HIGHER CLUSTER AVAILABILITY AND FAULT TOLERANCE.

CONFIGURE RETENTION PERIOD OF AUTOMATIC CLUSTER BACKUPS

SET THE NUMBER OF DAYS THAT CLOUDHSM SHOULD KEEP CLUSTER BACKUPS FOR (BACKUPS WILL BE AUTOMATICALLY DELETED AFTER THE SPECIFIED PERIOD HAS PASSED).



Step 1
Cluster configuration

Step 2
Backup retention

Step 3
Add tags

Step 4
Review

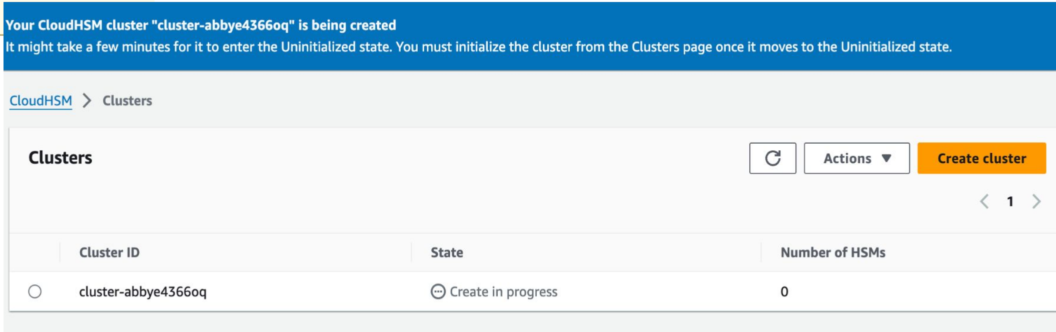
Review

Cluster configuration

VPC
vpc-071d8ba7a3685b6f8

Availability Zone(s)
us-east-1a | subnet-0a608d19e6c29c7a9
us-east-1b | subnet-0364ed27644866914

You cannot change VPC or subnets after a cluster is created
Review the information above carefully. You cannot modify VPC or subnet settings after you create the cluster. You can only create HSMs for this cluster within the specified subnets. You can only access HSMs within the specified VPC. To revise cluster settings, click Previous. To confirm and proceed with cluster creation, click Create cluster.

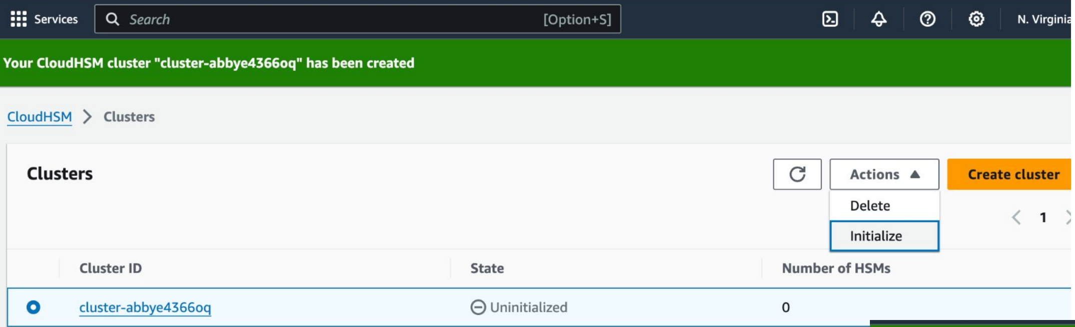


Your CloudHSM cluster "cluster-abbye4366oq" is being created
It might take a few minutes for it to enter the Uninitialized state. You must initialize the cluster from the Clusters page once it moves to the Uninitialized state.

	Cluster ID	State	Number of HSMs
○	cluster-abbye4366oq	Create in progress	0

REVIEW CLUSTER CONFIGURATIONS

WAIT FOR CLUSTER CREATION TO BE FINALIZED.



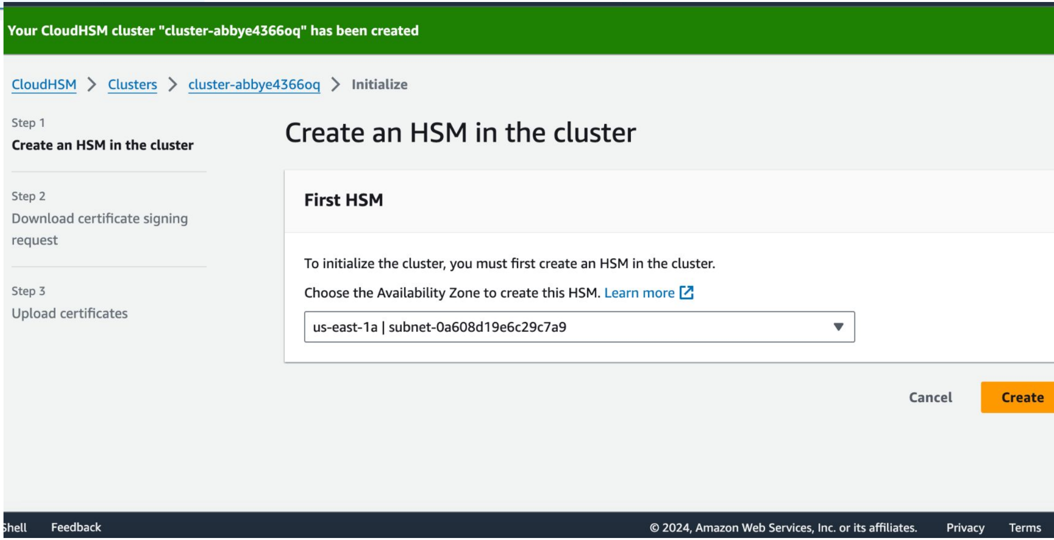
Your CloudHSM cluster "cluster-abbye4366oq" has been created

CloudHSM > Clusters

Clusters

	Cluster ID	State	Number of HSMs
●	cluster-abbye4366oq	⊖ Uninitialized	0

INITIALIZE CLUSTER



Your CloudHSM cluster "cluster-abbye4366oq" has been created

CloudHSM > Clusters > cluster-abbye4366oq > Initialize

Step 1
Create an HSM in the cluster

Step 2
Download certificate signing request

Step 3
Upload certificates

Create an HSM in the cluster

First HSM

To initialize the cluster, you must first create an HSM in the cluster.

Choose the Availability Zone to create this HSM. Learn more

us-east-1a | subnet-0a608d19e6c29c7a9

CREATE AN HSM INSIDE YOUR CLUSTER USING AWS CONSOLE

AWS CLI COMMANDS FOR INTEGRATING AWS KMS KEYS WITH CLOUD HSM

CREATE AN AWS CLOUDHSM KEY STORE:

```
aws kms create-custom-key-store \
        --custom-key-store-name ExampleCloudHSMKeyStore \
        --cloud-hsm-cluster-id cluster-1a23b4cdefg \
        --key-store-password kmsPswd \
        --trust-anchor-certificate file://customerCA.crt
```

CONNECT KMS CUSTOM KEY STORE TO CLOUDHSM CLUSTER:

```
aws kms connect-custom-key-store --custom-key-store-id
cks-1234567890abcdef0
```

CREATE KEY WITH CLOUDHSM STORE:

```
aws kms create-key \
    --origin AWS_CLOUDHSM \
    --custom-key-store-id cks-1234567890abcdef0
```

ENABLE KEY ROTATION:

```
aws kms enable-key-rotation \
    --key-id 1234abcd-12ab-34cd-56ef-1234567890ab \
    --rotation-period-in-days 180
```

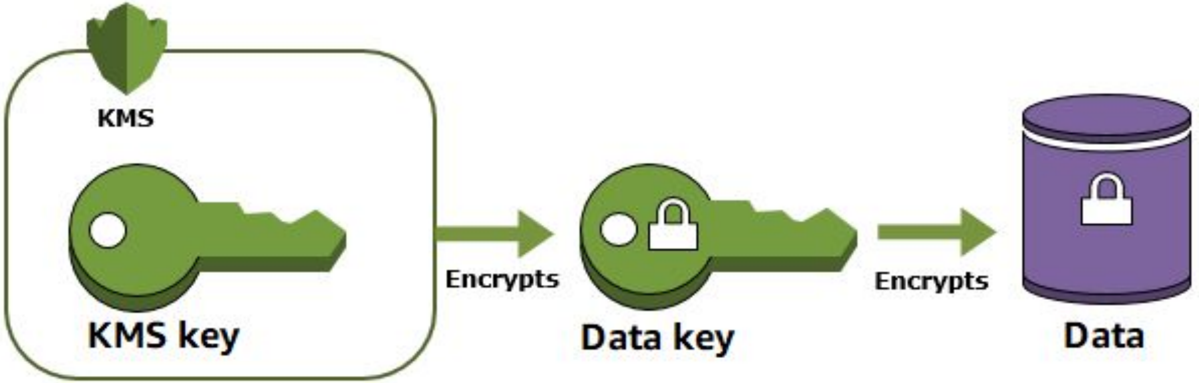
DATA DEFENDERS

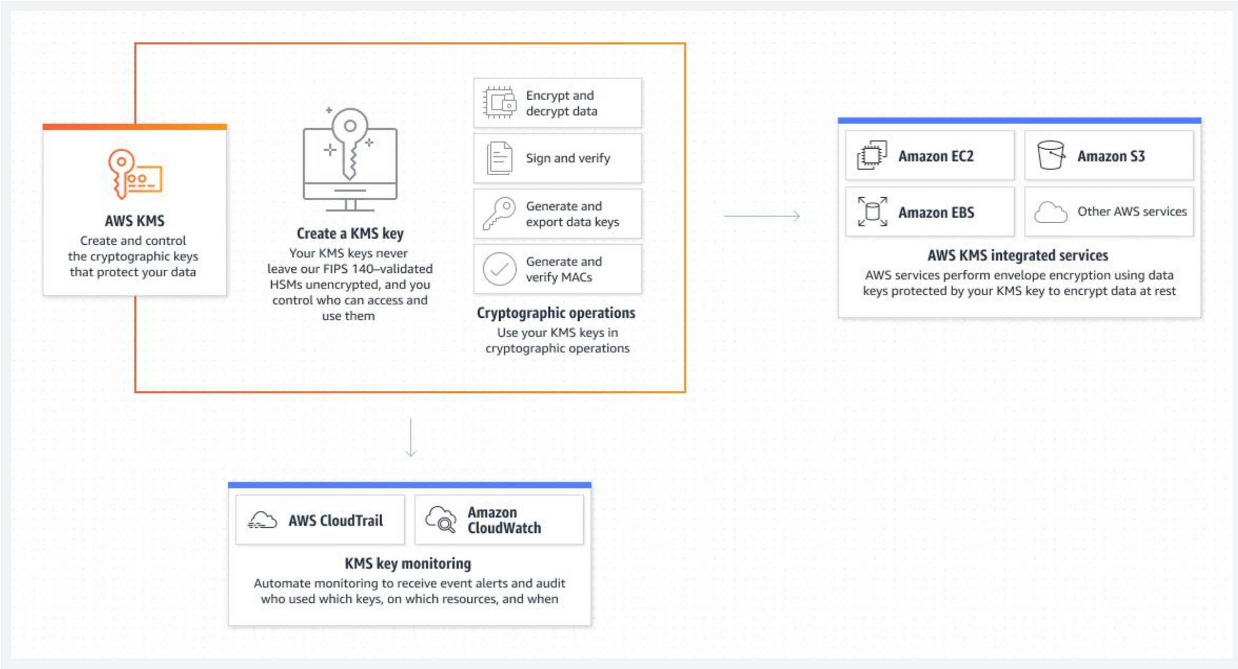
AWA AFO

TAKALA CROOK

MARIANA ESPINOZA

JAELIN LAZENBERRY





AWS KMS
Create and control the cryptographic keys that protect your data

Create a KMS key
Your KMS keys never leave our FIPS 140–validated HSMs unencrypted, and you control who can access and use them

Cryptographic operations
Use your KMS keys in cryptographic operations

AWS KMS integrated services
AWS services perform envelope encryption using data keys protected by your KMS key to encrypt data at rest

KMS key monitoring
Automate monitoring to receive event alerts and audit who used which keys, on which resources, and when