278-[SF]-Lab - Data Protection | Workbench - Vocareum

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=2253536&stepid=22535378hideNavBar=1

AWS

Used $0 of $1 | 00:45 | Start Lab | End Lab | AWS Details

EN-US

Data Protection Using Encryption

Lab overview

Cryptography is the conversion of communicated information into secret code that keeps the information confidential and private. Functions include authentication, data integrity, and nonrepudiation. The central function of cryptography is *encryption*, which transforms data into an unreadable form.

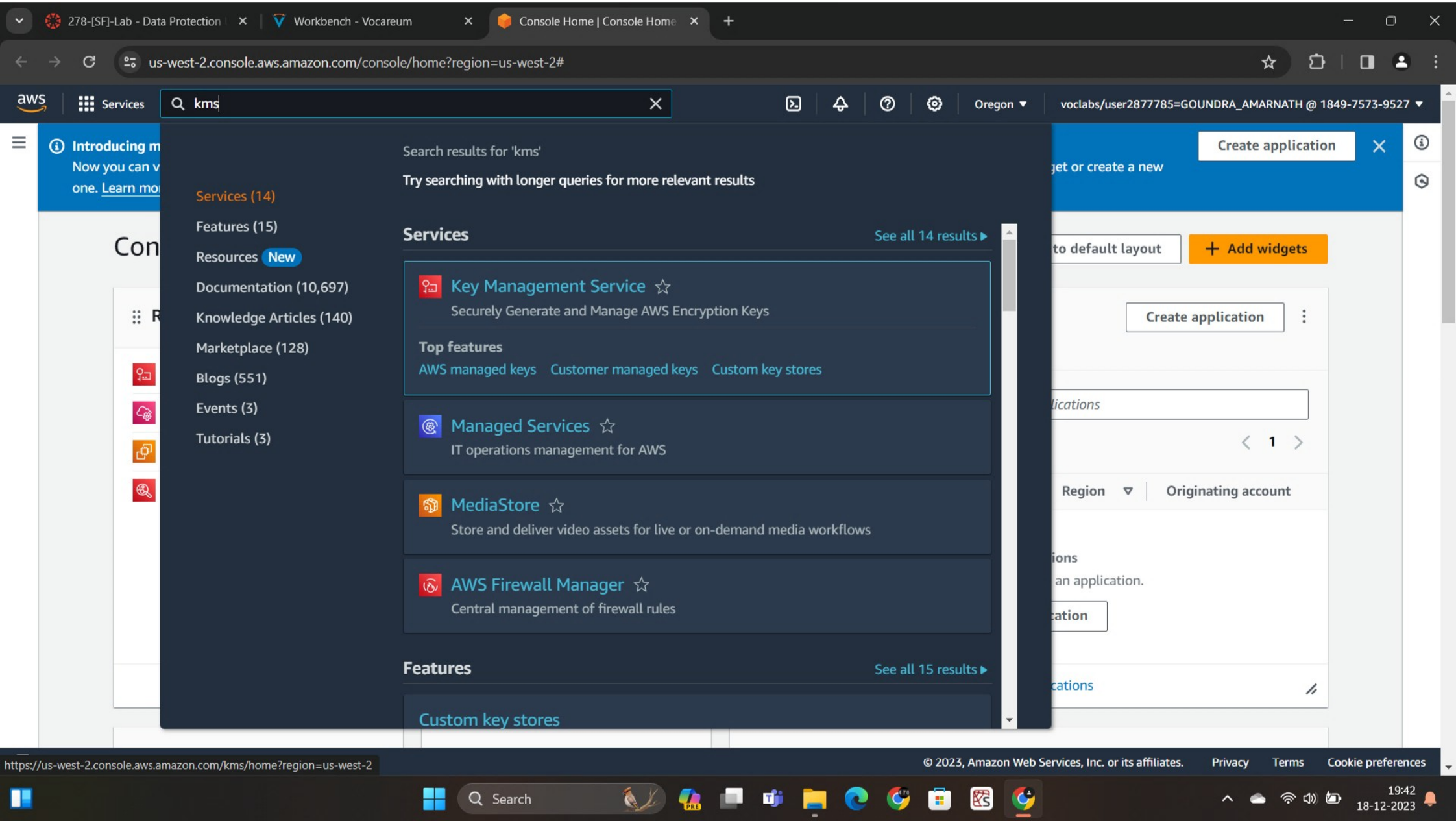
Encryption ensures privacy by keeping the information hidden from people who the information is not intended for. *Decryption*, the opposite of encryption, transforms encrypted data back into data; it won't make any sense until it has been properly decrypted.

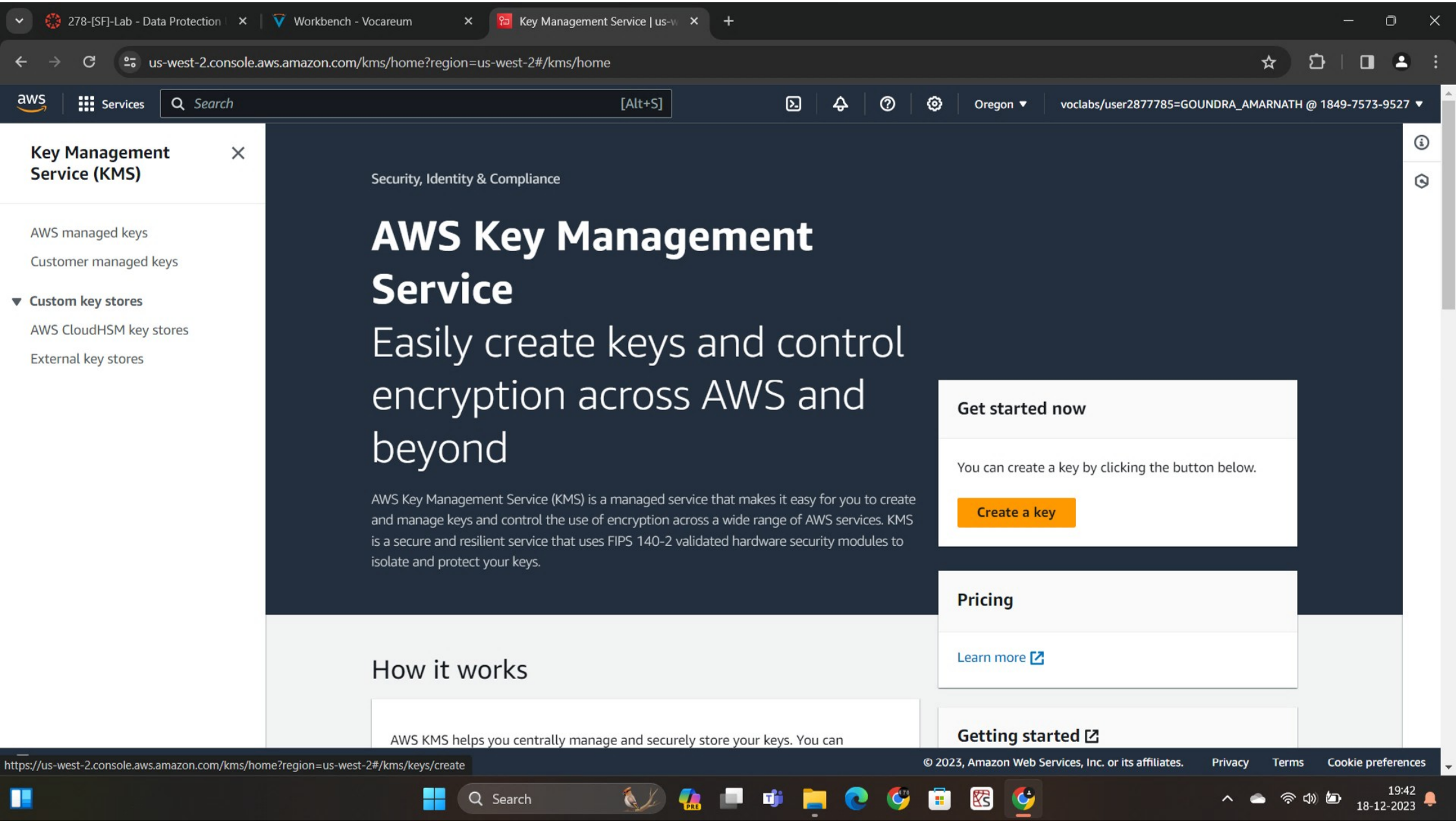
In this lab, you will connect to a file server that is hosted on an Amazon Elastic Compute Cloud (Amazon EC2) instance. You will configure the AWS Encryption command line interface (CLI) on the instance. You will create an encryption key by using the AWS Key Management Service (AWS KMS). The key will be used to encrypt and decrypt data. Next, you will create multiple text files that are unencrypted by default. You will then use the AWS KMS key to encrypt the files and view them while they are encrypted. You will finish the lab by decrypting the same files and viewing the contents.

Objectives

Search

19:40
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Console Home | Console Home
us-west-2.console.aws.amazon.com/console/home?region=us-west-2#
aws
Services
kms
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
Introducing m
Now you can v
one. Learn mo
Create application
get or create a new
Con
to default layout
Add widgets
Create application
lications
1
Region
Originating account
ions
an application.
cation
cations
Search results for 'kms'
Try searching with longer queries for more relevant results
Services (14)
Features (15)
Resources New
Documentation (10,697)
Knowledge Articles (140)
Marketplace (128)
Blogs (551)
Events (3)
Tutorials (3)
Services
See all 14 results
Key Management Service
Securely Generate and Manage AWS Encryption Keys
Top features
AWS managed keys
Customer managed keys
Custom key stores
Managed Services
IT operations management for AWS
MediaStore
Store and deliver video assets for live or on-demand media workflows
AWS Firewall Manager
Central management of firewall rules
Features
See all 15 results
Custom key stores
https://us-west-2.console.aws.amazon.com/kms/home?region=us-west-2
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:42
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Key Management Service | us-w
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/home
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
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 protect your keys.
Get started now
You can create a key by clicking the button below.
Create a key
Pricing
Learn more
How it works
AWS KMS helps you centrally manage and securely store your keys. You can
Getting started
https://us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/create
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:42
18-12-2023

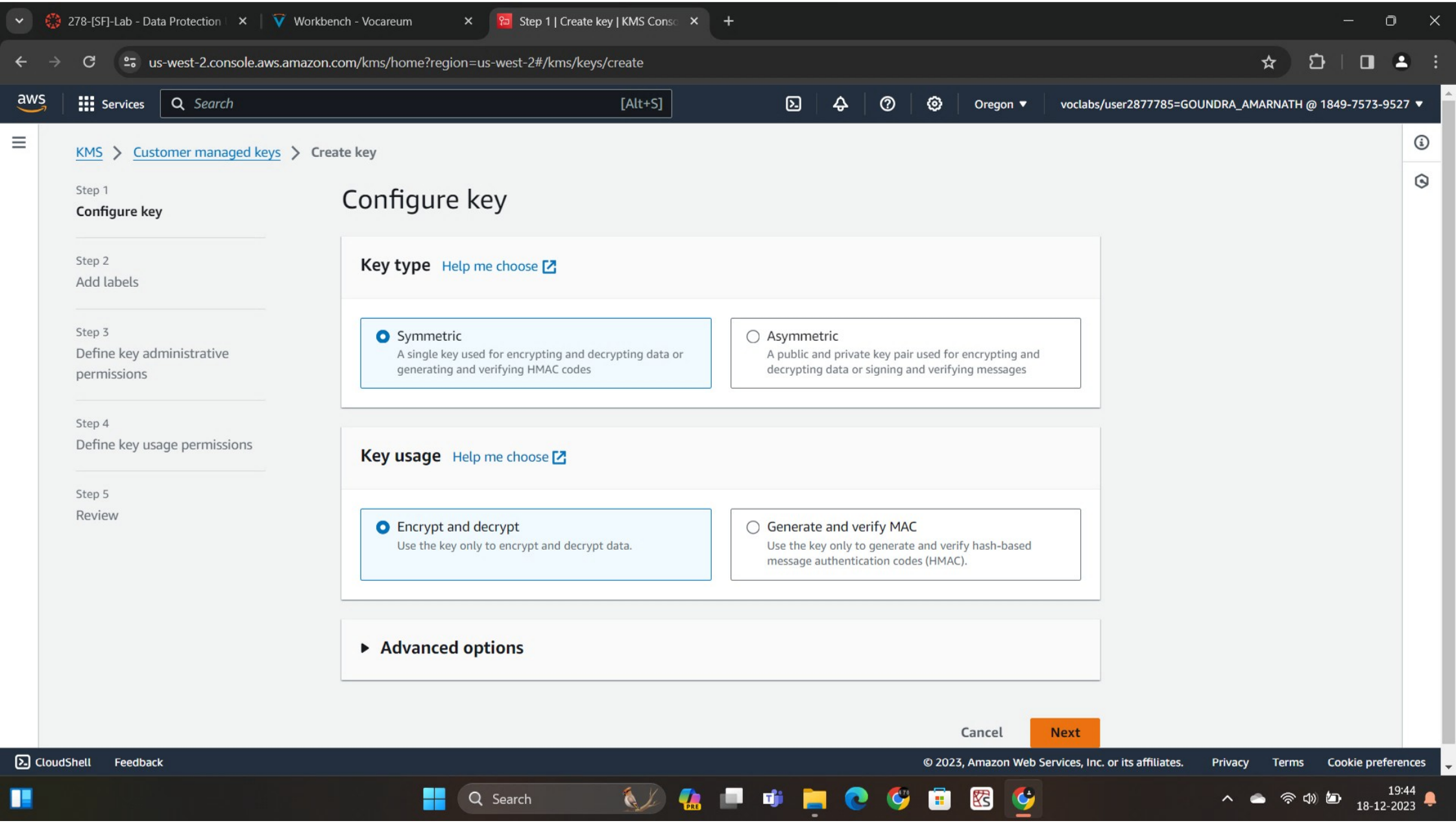
protect your keys.

6. In the console, enter **KMS** in the search 🔍 bar, and then choose **Key Management Service**.
7. Choose **Create a key**.
8. For **Key type**, choose **Symmetric**, and then choose **Next**.
   ℹ *Symmetric* encryption uses the same key to encrypt and decrypt data, which makes it fast and efficient to use. *Asymmetric* encryption uses a public key to encrypt data and a private key to decrypt information.
9. On the **Add labels** page, configure the following:
   - **Alias:** `MyKMSKey`
   - **Description:** `Key used to encrypt and decrypt data files.`
10. Choose **Next**.
11. On the **Define key administrative permissions** page, in the **Key administrators** section, search for and select the check box for `voclabs` and then choose **Next**.
12. On the **Define key usage permissions** page, in the **This account** section, search for and select the check box for `voclabs` and then choose **Next**.
13. Review the settings, and then choose **Finish**.
14. Choose the link for **MyKMSKey**, which you just created, and copy the **ARN** (Amazon Resource Name) value to a text editor.

You will use this copied ARN later in the lab.

Summary of task 1

In this task, you created a symmetric AWS KMS key and gave ownership of that key to the **voclabs** IAM role that was pre-created for this lab.


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Step 1 | Create key | KMS Cons
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/create
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review
Configure key
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
Cancel
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:44
18-12-2023

278-[SF]-Lab - Data Protection | Workbench - Vocareum | Step 2 | Create key | KMS Cons

us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/create

aws | Services | Search [Alt+S] | Oregon | voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Alias

MyKMSKey

Description - *optional*

You can change the description at any time.

Description

key

Tags - *optional*

You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. Learn more

This key has no tags.

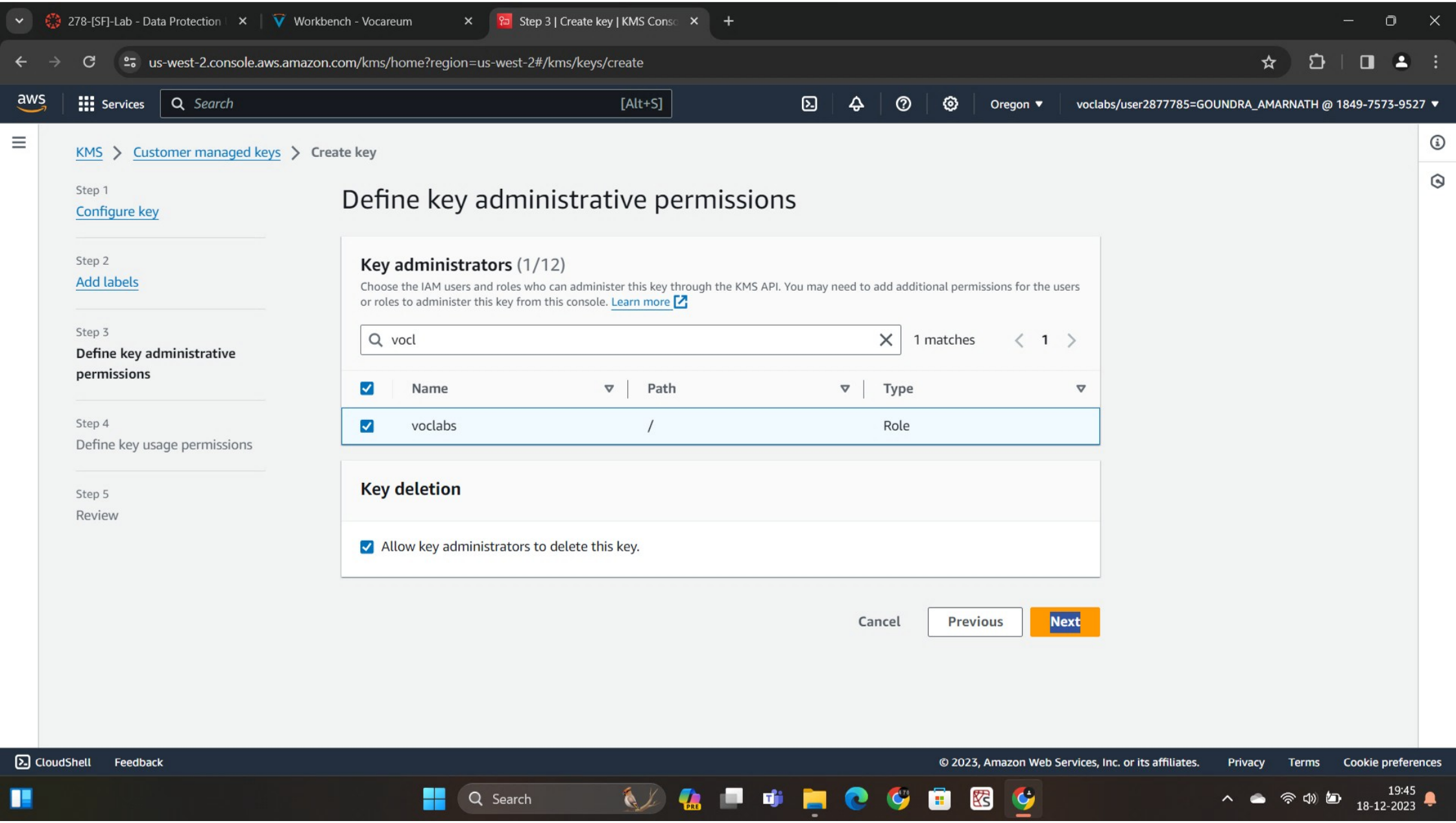
Add tag

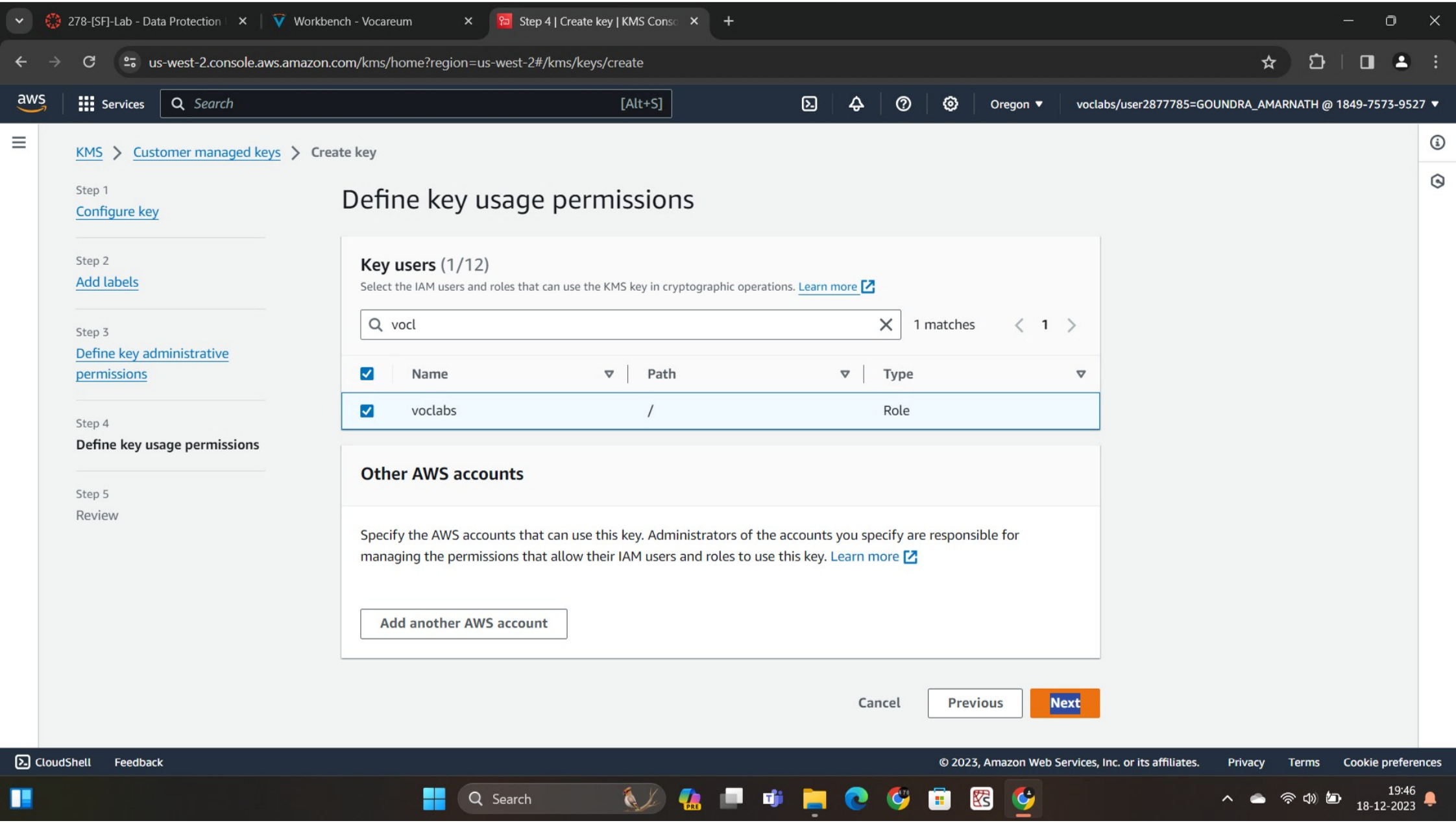
You can add up to 50 more tags.

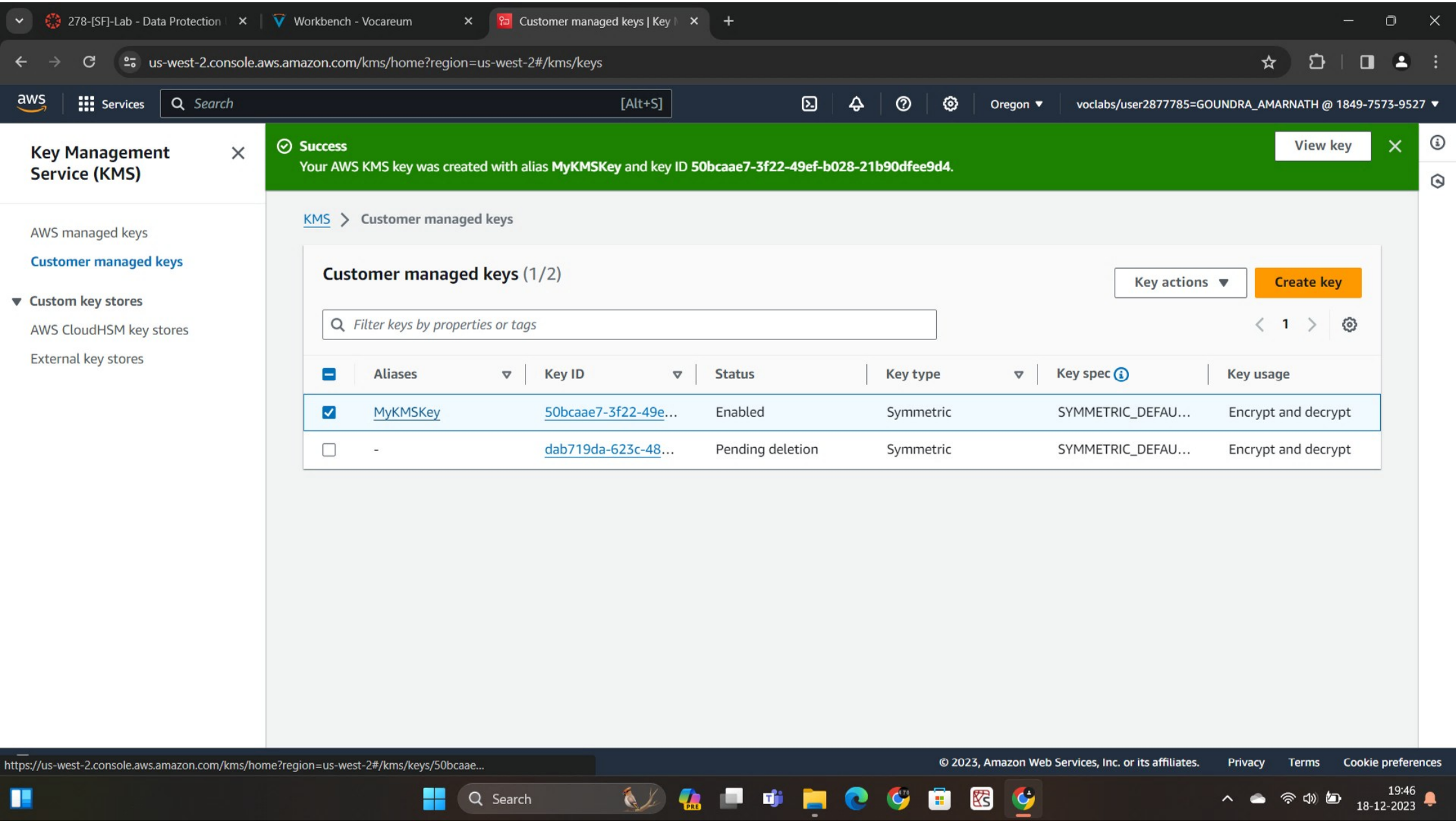
Cancel | Previous | Next

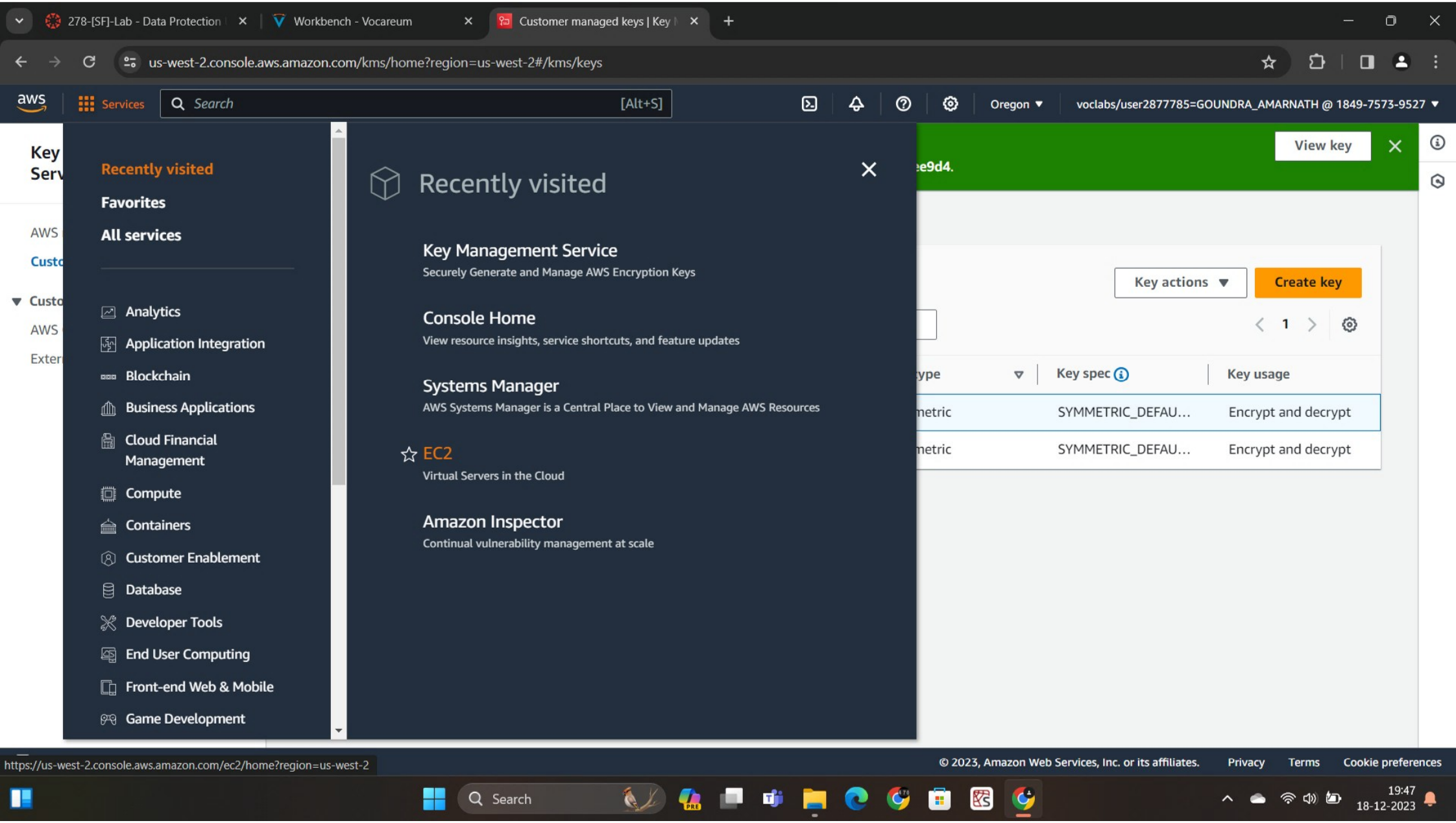
Search

19:44
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Step 3 | Create key | KMS Cons
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/create
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review
Define key administrative permissions
Key administrators (1/12)
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
vocl
1 matches
1
Name
Path
Type
voclabs
/
Role
Key deletion
Allow key administrators to delete this key.
Cancel
Previous
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:45
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Step 4 | Create key | KMS Cons
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/create
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review
Define key usage permissions
Key users (1/12)
Select the IAM users and roles that can use the KMS key in cryptographic operations. Learn more
vocl
1 matches
1
Name
Path
Type
voclabs
/
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
Add another AWS account
Cancel
Previous
Next
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:46
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Customer managed keys | Key
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
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 MyKMSKey and key ID 50bcaae7-3f22-49ef-b028-21b90dfee9d4.
View key
KMS > Customer managed keys
Customer managed keys (1/2)
Key actions
Create key
Filter keys by properties or tags
1
Aliases
Key ID
Status
Key type
Key spec
Key usage
MyKMSKey
50bcaae7-3f22-49e...
Enabled
Symmetric
SYMMETRIC_DEFAU...
Encrypt and decrypt
-
dab719da-623c-48...
Pending deletion
Symmetric
SYMMETRIC_DEFAU...
Encrypt and decrypt
https://us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/50bcaae...
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:46
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Customer managed keys | Key
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
Recently visited
Favorites
All services
Analytics
Application Integration
Blockchain
Business Applications
Cloud Financial Management
Compute
Containers
Customer Enablement
Database
Developer Tools
End User Computing
Front-end Web & Mobile
Game Development
Recently visited
Key Management Service
Securely Generate and Manage AWS Encryption Keys
Console Home
View resource insights, service shortcuts, and feature updates
Systems Manager
AWS Systems Manager is a Central Place to View and Manage AWS Resources
EC2
Virtual Servers in the Cloud
Amazon Inspector
Continual vulnerability management at scale
View key
Key actions
Create key
Key spec
Key usage
SYMMETRIC_DEFAU…
Encrypt and decrypt
SYMMETRIC_DEFAU…
Encrypt and decrypt
https://us-west-2.console.aws.amazon.com/ec2/home?region=us-west-2
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
19:47
18-12-2023

15. In the console, enter **EC2** in the search 🔍 bar, and then choose **EC2**.
16. In the **Instances** list, select the check box next for the **File Server** instance, and then choose **Connect**.
17. Choose the **Session Manager** tab, and then choose **Connect**.
18. To change to the home directory and create the AWS credentials file, run the following commands:

```
cd ~
aws configure
```

19. When prompted, configure the following:
    - **AWS Access Key ID**: Enter `1`, and then press Enter.
    - **AWS Secret Access Key**: Enter `1`, and then press Enter.
    - **Default region name**: Copy and paste the Region provided from the Vocareum **AWS Details** page.
    - ***Tip*** *You may need to press Ctrl+Shift+V to paste into Session Manager.*
    - **Default output format**: Press Enter.

    The AWS configuration file is created, and you will update it in a later step. The previous entries of `1` are temporary placeholders.
20. Navigate to the Vocareum console page, and choose the ℹ **AWS Details** button.
21. Next to **AWS CLI**, choose **Show**.
22. Copy and paste the code block, which starts with [default], into a text editor.
23. Return to the browser tab where you are logged in to the File Server.
24. To open the AWS credentials file, run the following command:

278-[SF]-Lab - Data Protection | Workbench - Vocareum | Instances | EC2 | us-west-2

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=2253536&stepid=2253537&hideNavBar=1

AWS | Used $0 of $1 | 00:28 | ▶ Start Lab | ■ End Lab | ℹ AWS Details

15. In the console, enter **EC2** in the search 🔍 bar, and then choose **EC2**.
16. In the **Instances** list, select the check box next for the **File Server** instance, and then choose **Connect**.
17. Choose the **Session Manager** tab, and then choose **Connect**.
18. To change to the home directory and create the AWS credentials file, run the following commands:

```
cd ~
aws configure
```

19. When prompted, configure the following:
    - **AWS Access Key ID**: Enter `1`, and then press Enter.
    - **AWS Secret Access Key**: Enter `1`, and then press Enter.
    - **Default region name**: Copy and paste the Region provided from the Vocareum **AWS Details** page.
    - ***Tip*** *You may need to press Ctrl+Shift+V to paste into Session Manager.*
    - **Default output format**: Press Enter.

    The AWS configuration file is created, and you will update it in a later step. The previous entries of `1` are temporary placeholders.
20. Navigate to the Vocareum console page, and choose the ℹ **AWS Details** button.
21. Next to **AWS CLI**, choose **Show**.
22. Copy and paste the code block, which starts with [default], into a text editor.
23. Return to the browser tab where you are logged in to the File Server.
24. To open the AWS credentials file, run the following command:

Close

Cloud Access

AWS CLI: Show

Cloud Labs

Remaining session time: 00:27:04(28 minutes)
Session started at: 2023-12-18T06:10:44-0800
Session to end at: 2023-12-18T06:55:44-0800

Accumulated lab time: 01:40:00 (100 minutes)

No running instance

SSH key Show Download PEM Download PPK

AWS SSO Download URL

Region us-west-2

Search

19:58
18-12-2023

278-[SF]-Lab - Data Protection | Workbench - Vocareum | Instances | EC2 | us-west-2

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=2253536&stepid=2253537&hideNavBar=1

AWS | Used $0 of $1 | 00:27 | ▶ Start Lab | ■ End Lab | ℹ AWS Details

- **Default region name**: Copy and paste the Region provided from the Vocareum **AWS Details** page.
- ***Tip*** *You may need to press Ctrl+Shift+V to paste into Session Manager.*
- **Default output format**: Press Enter.

The AWS configuration file is created, and you will update it in a later step. The previous entries of `1` are temporary placeholders.

20. Navigate to the Vocareum console page, and choose the ℹ **AWS Details** button.
21. Next to **AWS CLI**, choose **Show**.
22. Copy and paste the code block, which starts with [default], into a text editor.
23. Return to the browser tab where you are logged in to the File Server.
24. To open the AWS credentials file, run the following command:

```
vi ~/.aws/credentials
```

25. In the ~/.aws/credentials file, type `dd` multiple times to delete the contents of the file.
26. Paste in the code block that you copied from Vocareum.

    The AWS credentials file should now look similar to the following:

    
    Example of AWS credentials file contents.

    The AWS credentials file includes the following: aws_access_key_id, aws_secret_access_key, and aws_session_token. The credentials used are from the AWS Details section.
27. To save and close the file, press Escape, type `:wq` and then press Enter.
28. To view the updated contents of the file, run the following command:

Close

Cloud Access

AWS CLI:

Copy and paste the following into ~/.aws/credentials

```
[default]
aws_access_key_id=ASIASWELJZKDS7WBUZEQ
aws_secret_access_key=hOVOPRHoLhT36YVPOQRWv0XldjGL4hcThY
AbiudO
aws_session_token=FwoGZXIvYXdzEFgaDKGHZnyPguw3xM58diLBAS
kK0FWP57p8PVpD9EhxcxXZWVGF9zto277Onww2UuE0wMeGuzf9zK7FYZ
vF31RrcW98VrfKeU9CF0ahQsimRf1djdfAS9wR8RWpjjO/mmBUD8biIL
Aws6HWZ5lU+gghT1Edoll2BU7oH6JWunkTCnsaDHUDGVeoeuT5KQt/ic
Ax4OsQuwSzDngmKQ5tuyFaLLoTxZFQEjKDe3PqZZYHd/cU2I7qhE6pQL
53ioX6QLAehI/F078OdWKglCobGbIa7yco5aWBrAYyLbSKnHH44c4dGY
9eAiDQjpesLuCWBIGpx3AazZI5SHqVGugzUckVPDOYkMERgw==
```

Cloud Labs

Remaining session time: 00:26:16(27 minutes)
Session started at: 2023-12-18T06:10:44-0800
Session to end at: 2023-12-18T06:55:44-0800

Accumulated lab time: 01:41:00 (101 minutes)

No running instance

SSH key Show Download PEM Download PPK

AWS SSO Download URL

Region us-west-2

Search

19:59
18-12-2023

278-[SF]-Lab - Data Protection | Workbench - Vocareum | Instances | EC2 | us-west-2

labs.vocareum.com/main/main.php?m=clabide&mode=s&asnid=2253536&stepid=2253537&hideNavBar=1

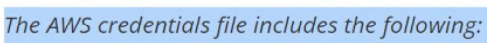
AWS | Used $0 of $1 | 00:27 | ▶ Start Lab | ■ End Lab | ℹ AWS Details

24. To open the AWS credentials file, run the following command:

```
vi ~/.aws/credentials
```

25. In the ~/.aws/credentials file, type `dd` multiple times to delete the contents of the file.
26. Paste in the code block that you copied from Vocareum.

    The AWS credentials file should now look similar to the following:

    
    Example of AWS credentials file contents.

    The AWS credentials file includes the following: aws_access_key_id, aws_secret_access_key, and aws_session_token. The credentials used are from the AWS Details section.
27. To save and close the file, press Escape, type `:wq` and then press Enter.
28. To view the updated contents of the file, run the following command:

```
cat ~/.aws/credentials
```

    Now you will install the AWS Encryption CLI and export your path. By doing this, you will be able to run the commands to encrypt and decrypt data.
29. To install the AWS Encryption CLI and set your path, run the following commands:

```
pip3 install aws-encryption-sdk-cli
export PATH=$PATH:/home/ssm-user/.local/bin
```

Summary of task 2

Close

Cloud Access

AWS CLI:

Copy and paste the following into ~/.aws/credentials

```
[default]
aws_access_key_id=ASIASWELJZKDS7WBUZEQ
aws_secret_access_key=hOVOPRHoLhT36YVPOQRWv0XldjGL4hcThY
AbiudO
aws_session_token=FwoGZXIvYXdzEFgaDKGHZnyPguw3xM58diLBAS
kK0FWP57p8PVpD9EhxcxXZWVGF9zto277Onww2UuE0wMeGuzf9zK7FYZ
vF31RrcW98VrfKeU9CF0ahQsimRf1djdfAS9wR8RWpjjO/mmBUD8biIL
Aws6HWZ5lU+gghT1Edoll2BU7oH6JWunkTCnsaDHUDGVeoeuT5KQt/ic
Ax4OsQuwSzDngmKQ5tuyFaLLoTxZFQEjKDe3PqZZYHd/cU2I7qhE6pQL
53ioX6QLAehI/F078OdWKglCobGbIa7yco5aWBrAYyLbSKnHH44c4dGY
9eAiDQjpesLuCWBIGpx3AazZI5SHqVGugzUckVPDOYkMERgw==
```

Cloud Labs

Remaining session time: 00:26:16(27 minutes)
Session started at: 2023-12-18T06:10:44-0800
Session to end at: 2023-12-18T06:55:44-0800

Accumulated lab time: 01:41:00 (101 minutes)

No running instance

SSH key Show Download PEM Download PPK

AWS SSO Download URL

Region us-west-2

Search

19:59
18-12-2023

Task 3: Encrypt and decrypt data

In this task, you will create a text file with mock sensitive data in it. You will then use encryption to secure the file contents. Then, you will decrypt the data and view the file contents.

30. To create the text file, run the following commands:

```
touch secret1.txt secret2.txt secret3.txt
echo 'TOP SECRET 1!!!' > secret1.txt
```

31. To view the contents of the **secret1.txt** file, run the following command:

```
cat secret1.txt
```

32. To create a directory to output the encrypted file, run the following command:

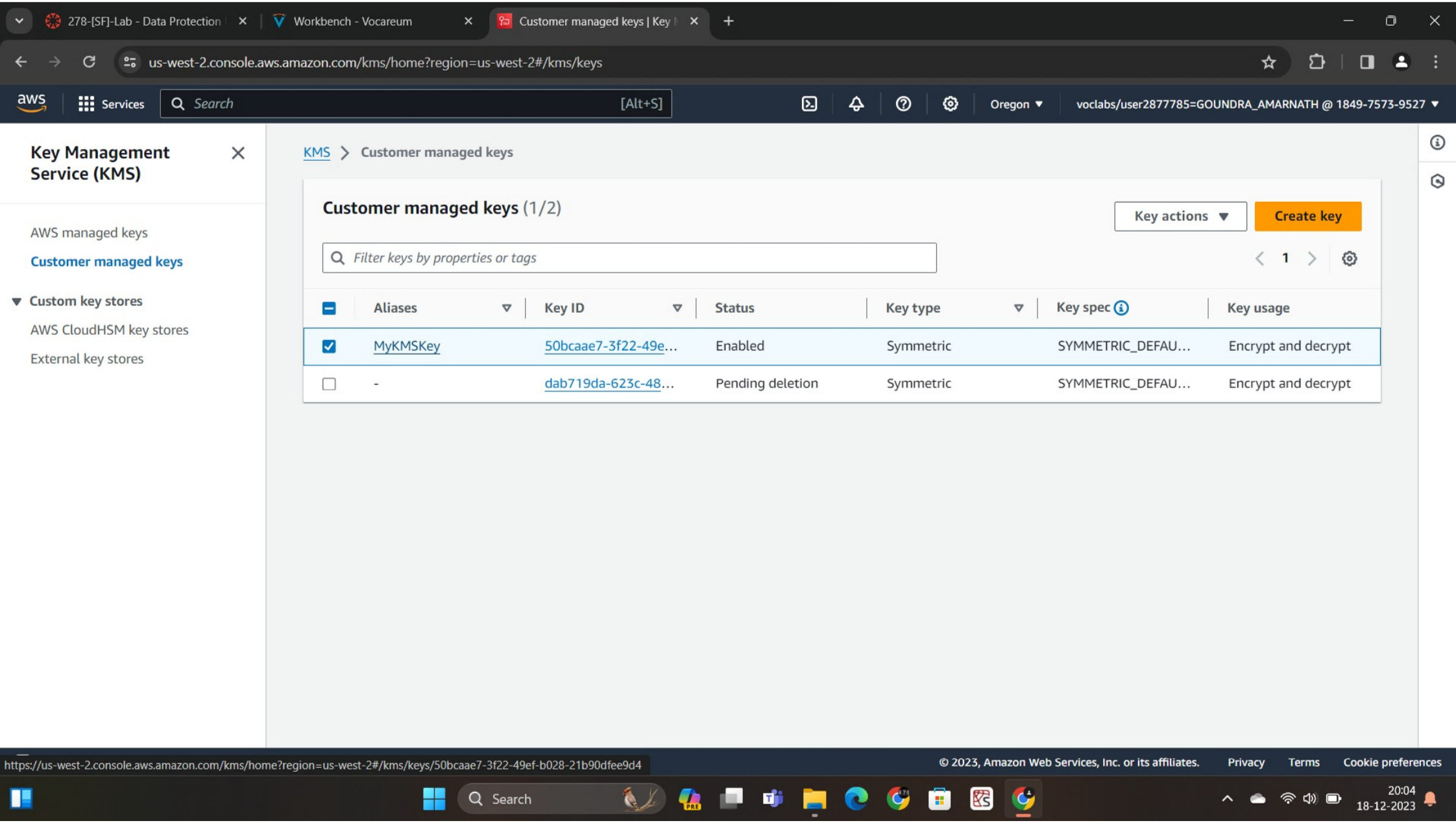
```
mkdir output
```

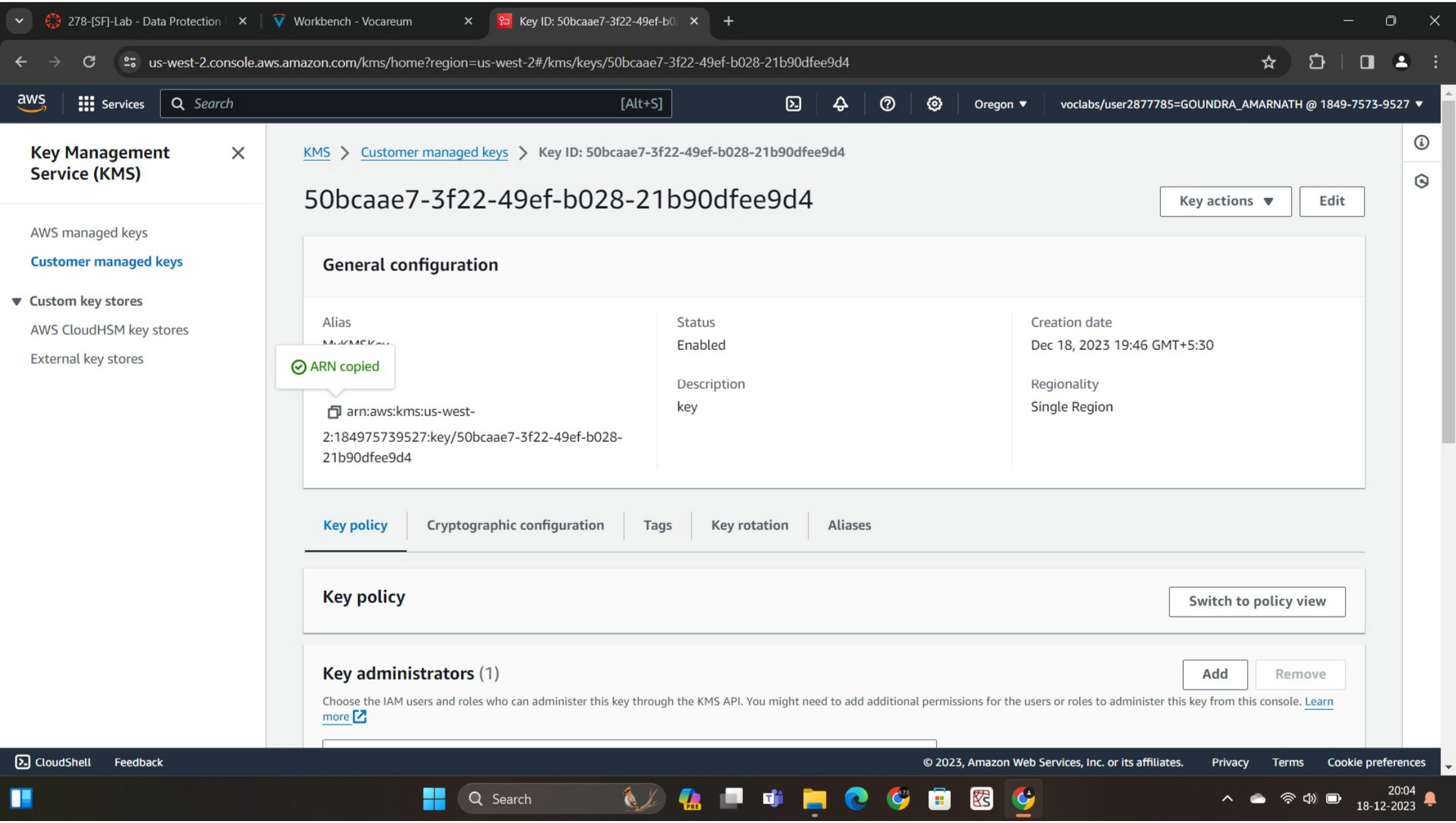
33. Copy and paste the following command to a text editor:

```
keyArn=(KMS ARN)
```

34. In the text editor, replace **(KMS ARN)** with the AWS KMS ARN that you copied in task 1.
35. Run the updated command in the File Server terminal.

    This command saves the ARN of an AWS KMS key in the **$keyArn** variable. When you encrypt by using an AWS KMS key, you can identify it by using a key ID, key ARN, alias name, or alias ARN.


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Customer managed keys | Key
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
Key Management Service (KMS)
AWS managed keys
Customer managed keys
Custom key stores
AWS CloudHSM key stores
External key stores
KMS > Customer managed keys
Customer managed keys (1/2)
Key actions
Create key
Filter keys by properties or tags
1
Aliases
Key ID
Status
Key type
Key spec
Key usage
MyKMSKey
50bcaae7-3f22-49e...
Enabled
Symmetric
SYMMETRIC_DEFAU...
Encrypt and decrypt
-
dab719da-623c-48...
Pending deletion
Symmetric
SYMMETRIC_DEFAU...
Encrypt and decrypt
https://us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/50bcaae7-3f22-49ef-b028-21b90dfee9d4
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
20:04
18-12-2023


278-[SF]-Lab - Data Protection
Workbench - Vocareum
Key ID: 50bcaae7-3f22-49ef-b0
us-west-2.console.aws.amazon.com/kms/home?region=us-west-2#/kms/keys/50bcaae7-3f22-49ef-b028-21b90dfee9d4
aws
Services
Search
[Alt+S]
Oregon
voclabs/user2877785=GOUNDRA_AMARNATH @ 1849-7573-9527
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: 50bcaae7-3f22-49ef-b028-21b90dfee9d4
50bcaae7-3f22-49ef-b028-21b90dfee9d4
Key actions
Edit
General configuration
Alias
ARN copied
arn:aws:kms:us-west-2:184975739527:key/50bcaae7-3f22-49ef-b028-21b90dfee9d4
Status
Enabled
Description
key
Creation date
Dec 18, 2023 19:46 GMT+5:30
Regionality
Single Region
Key policy
Cryptographic configuration
Tags
Key rotation
Aliases
Key policy
Switch to policy view
Key administrators (1)
Add
Remove
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
CloudShell
Feedback
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
Search
20:04
18-12-2023

36. To encrypt the **secret1.txt** file, run the following command:

```
aws-encryption-cli --encrypt \
                   --input secret1.txt \
                   --wrapping-keys key=$keyArn \
                   --metadata-output ~/metadata \
                   --encryption-context purpose=test \
                   --commitment-policy require-encrypt-require-decrypt \
                   --output ~/output/.
```

The following information describes what this command does:

- The first line encrypts the file contents. The command uses the **--encrypt** parameter to specify the operation and the **--input** parameter to indicate the file to encrypt.
- The **--wrapping-keys** parameter, and its required *key* attribute, tell the command to use the AWS KMS key that is represented by the key ARN.
- The **--metadata-output** parameter is used to specify a text file for the metadata about the encryption operation.
- As a best practice, the command uses the **--encryption-context** parameter to specify an encryption context.
- The **–commitment-policy** parameter is used to specify that the key commitment security feature should be used to encrypt and decrypt.
- The value of the **--output** parameter, *~/output/.*, tells the command to write the output file to the output directory.

💬 When the encrypt command succeeds, it does not return any output.

37. To determine whether the command succeeded, run the following command:

```
echo $?
```

When the encrypt command succeeds, it does not return any output.

37. To determine whether the command succeeded, run the following command:

```
echo $?
```

If the command succeeded, the value of **$?** is **0**. If the command failed, the value is nonzero.

38. To view the newly encrypted file location, run the following command:

```
ls output
```

The output should look like the following:

```
secret1.txt.encrypted
```

39. To view the contents of the newly encrypted file, run the following command:

```
cd output
cat secret1.txt.encrypted
```

ℹ The encryption and decryption process takes data in *plaintext*, which is readable and understandable, and manipulates its form to create *ciphertext*, which is what you are now seeing.

When data has been transformed into ciphertext, the plaintext becomes inaccessible until it's decrypted.

Symmetric Key

```
aws-encryption-cli --decrypt \
                   --input secret1.txt.encrypted \
                   --wrapping-keys key=$keyArn \
                   --commitment-policy require-encrypt-require-decrypt \
                   --encryption-context purpose=test \
                   --metadata-output ~/metadata \
                   --max-encrypted-data-keys 1 \
                   --buffer \
                   --output .
```

42. To view the new file location, run the following command:

```
ls
```

The **secret1.txt.encrypted.decrypted** file contains the decrypted contents from the **secret1.txt.encrypted** file.

43. To view the contents of the decrypted file, run the following command:

```
cat secret1.txt.encrypted.decrypted
```

After successful decryption, you can now see the original *plaintext* contents of the **secret1.txt**.

Symmetric Key