Lab

11

Protecting Secrets in Azure with Key Vault

Azure Key Vault service is used for the secure storage of confidential information or secrets such as passwords, API keys, and cryptographic keys.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

In Azure, secrets such as passwords, API keys, and cryptographic keys can be securely stored with Azure Key Vault. This eliminates security risks such as password leakages. This lab demonstrates how a cloud security engineer can securely store passwords in Azure Key Vault and access passwords from both the Azure Portal and Azure PowerShell.

Lab Objectives

This lab demonstrates how to create a resource group and a key vault in Azure to store passwords, store passwords in the key vault, and access passwords from both the Azure portal and PowerShell.

In this lab, you will learn the following:

- Creating a resource group in Azure
- Creating an Azure key vault to store passwords
- Storing passwords in the key vault
- Accessing passwords from the Azure portal and PowerShell

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account
- Administrative privileges

Lab Duration

Time: 15 minutes

Overview of Azure Key Vault

In an Azure environment, secrets such as passwords must be stored securely. Azure Key Vault is used to securely store and enforce access control to cryptographic keys, passwords, and API keys, and it can be used to create policies such that the secrets can only be accessed by authorized users. It also reduces the risk of accidental leakage of secrets. Authorized applications can use a Secret Identifier Uniform Resource Identifier (URI) to access secret passwords.

Lab Tasks

Note: Web applications using cloud environments may undergo frequent updates. For this lab, because we are working on a cloud-based environment, (i.e., Azure), the application interface may be updated with time. Hence, when working on an updated version of Azure, the user interface may differ from that shown in the lab. Consequently, the steps and screenshots demonstrated in this lab might also differ.

Note: Before starting this lab, you should create an Azure Free Account using the following link: https://azure.microsoft.com/free, in case you have already not created it for the previous module. Once the registration is complete, perform the following tasks:

Note: You can also use any existing Azure account but be aware that it may incur significant charges to your account.

TASK 1

Creating a resource group in Azure

1. Launch the **Admin Machine** VM. Log in with the following credentials: user "**Admin**" and password "**admin@123**".

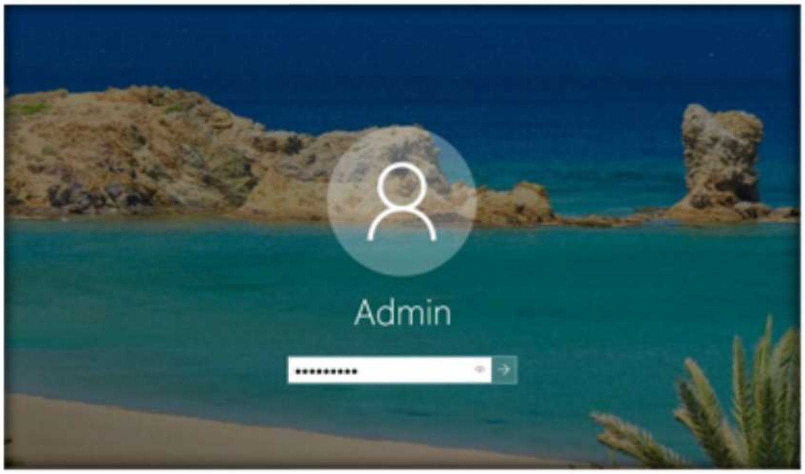


FIGURE 4.11.1: Launch Admin Machine and Log in

2. To open the browser, double-click on the **Google Chrome** icon on the desktop.

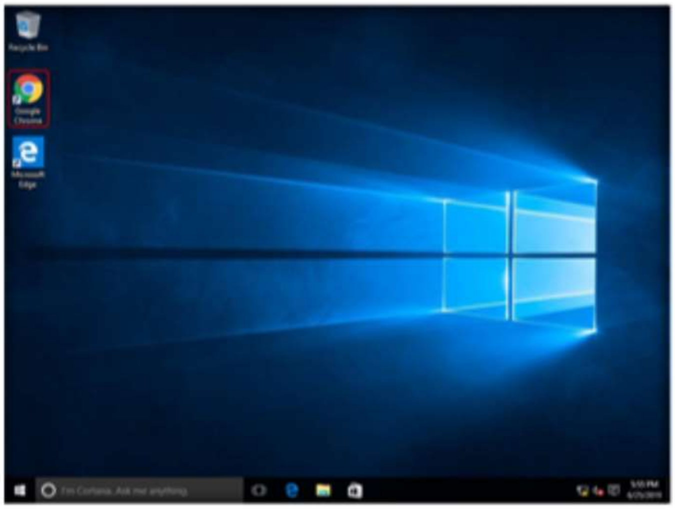
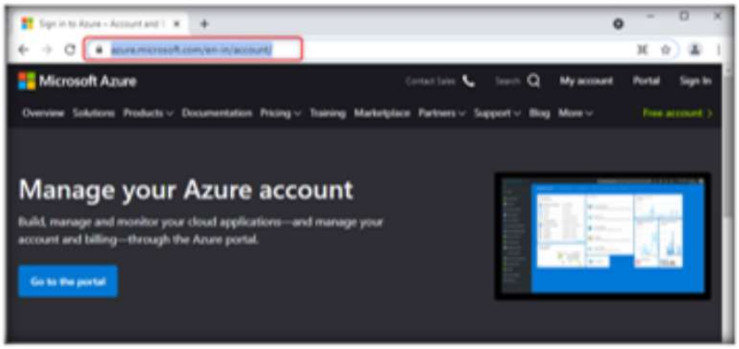


FIGURE 4.11.2: Navigating to the Chrome Browser from Taskbar

3. The **Google Chrome** browser opens. Go to the address bar, type **https://azure.microsoft.com/en-in/account/**, and press **Enter**.

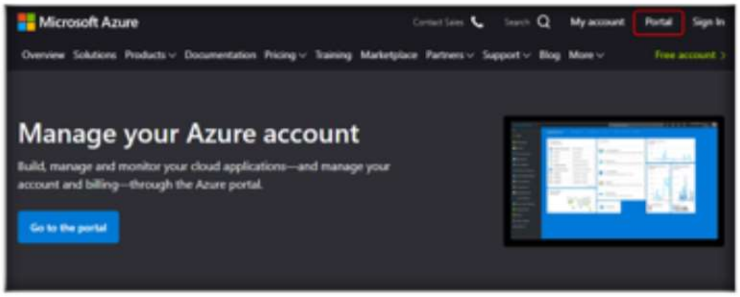


Manage your Azure account

Build, manage and monitor your cloud applications—and manage your account and billing—through the Azure portal.

FIGURE 4.11.3: Entering the URL of Microsoft Azure

4. The **Microsoft Azure** page will appear. Click on **Portal**.

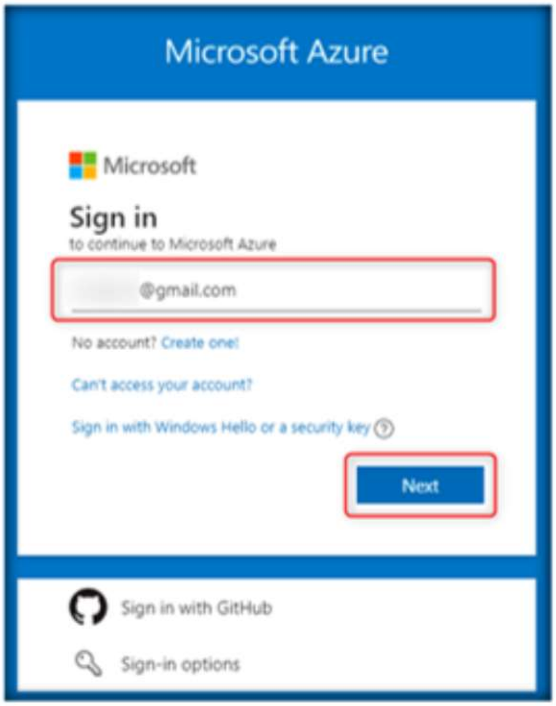


Manage your Azure account

Build, manage and monitor your cloud applications—and manage your account and billing—through the Azure portal.

FIGURE 4.11.4: Sign in to Azure Portal

5. In the **Sign in** page, enter the **Account ID** and click on **Next.**



Microsoft Azure

Microsoft

Sign in

to continue to Microsoft Azure

[redacted]@gmail.com

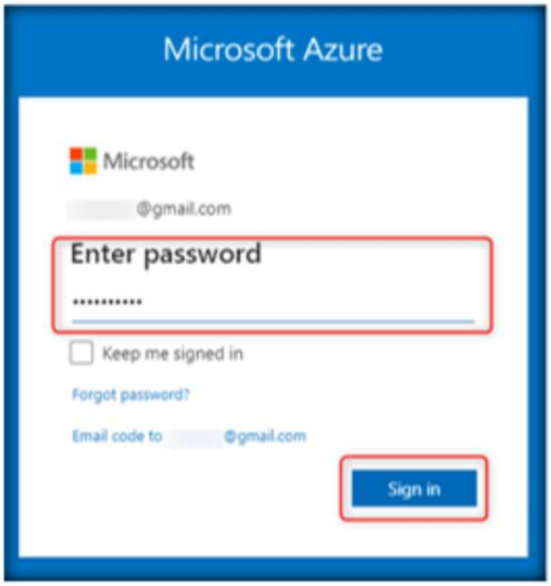
No account? Create one!

Can't access your account?

Sign in with Windows Hello or a security key ⓘ

FIGURE 4.11.5: Entering Account ID to continue

6. In the next window, enter the password and click on **Sign in.**



Microsoft Azure

Microsoft

[redacted]@gmail.com

Enter password

••••••••••

□ Keep me signed in

Forgot password?

Email code to [redacted]@gmail.com

FIGURE 4.11.6: Sign in to Azure Account

7. Now, to create a resource group, click on **Resource groups** under **Azure Services**.

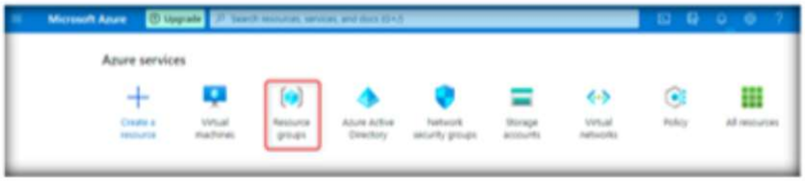
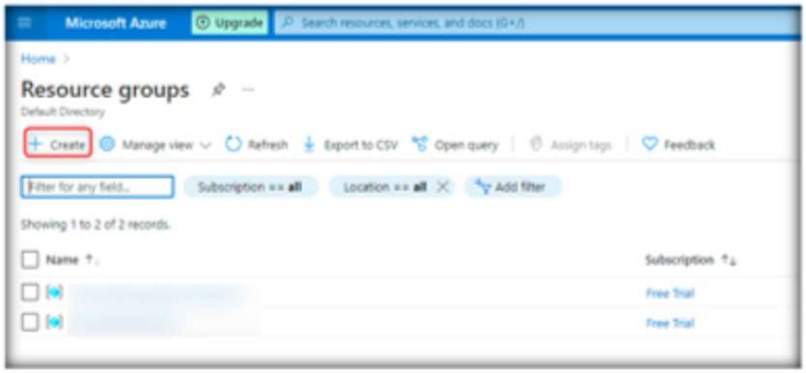


FIGURE 4.11.7: Navigating to Resource Groups

8. In the **Resource groups** window, click on **+Create**.

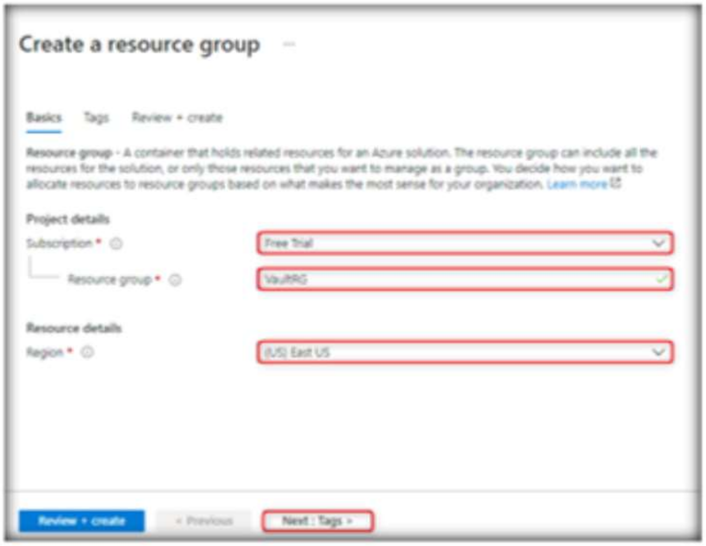


Showing 1 to 2 of 2 records.

Name ↑	Subscription ↑↓
[redacted]	Free Trial
[redacted]	Free Trial

FIGURE 4.11.8: Creating Resource Group

9. In the **Create a resource group** window, select **Free Trial** for **Subscription**. Enter a name for the **Resource group**; here, we have used **VaultRG**. For **Region**, select an appropriate region; here, we have selected **East US**. Click on **Next: Tags >**.



Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

Subscription * : Free Trial

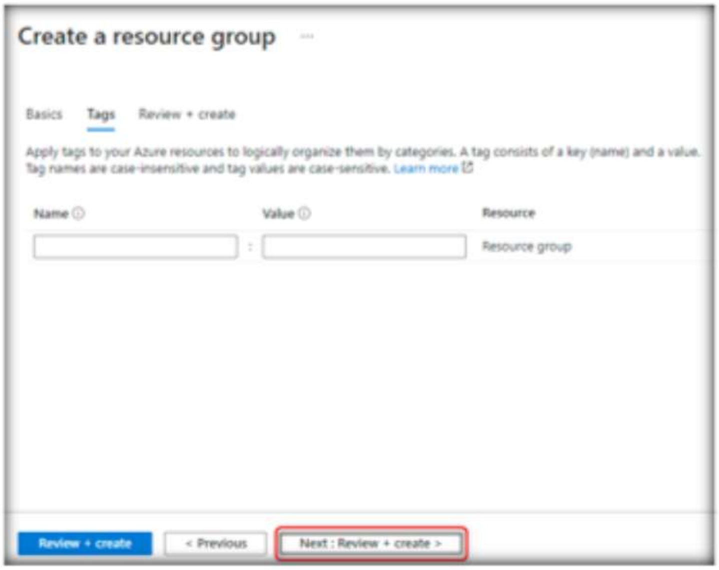
Resource group * : VaultRG

Resource details

Region * : (US) East US

FIGURE 4.11.9: Configuring Resource Group

10. Click on **Next : Review + create >** to continue.

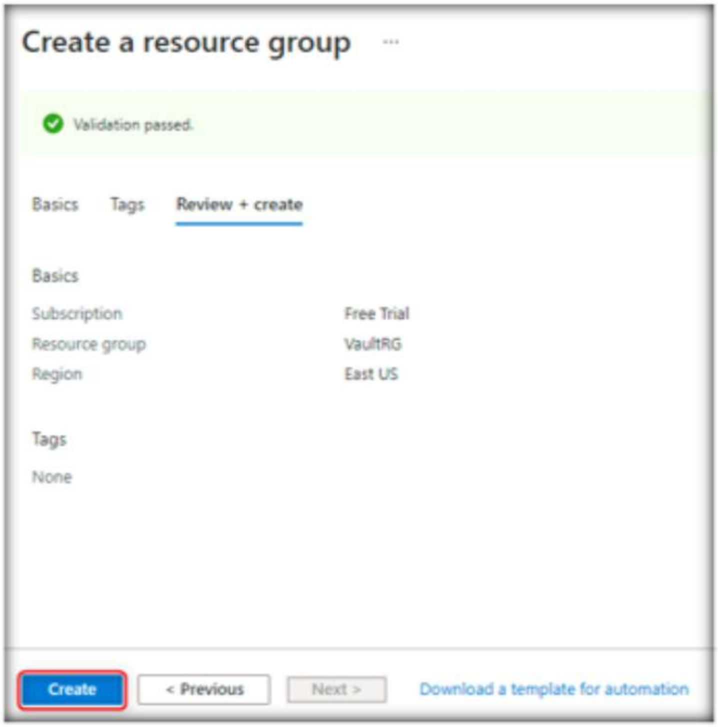


Apply tags to your Azure resources to logically organize them by categories. A tag consists of a key (name) and a value. Tag names are case-insensitive and tag values are case-sensitive. Learn more

Name	Value	Resource
		Resource group

FIGURE 4.11.10: Proceeding with Configuration

11. Click on **Create** to create the resource group.


Create a resource group ···
Basics
Tags
Review + create
Create
< Previous
Next >
Download a template for automation

✅ Validation passed.

Basics

Subscription	Free Trial
Resource group	VaultRG
Region	East US

Tags

None

FIGURE 4.11.11: Creating Resource Group

12. Thus, the resource group is successfully created.

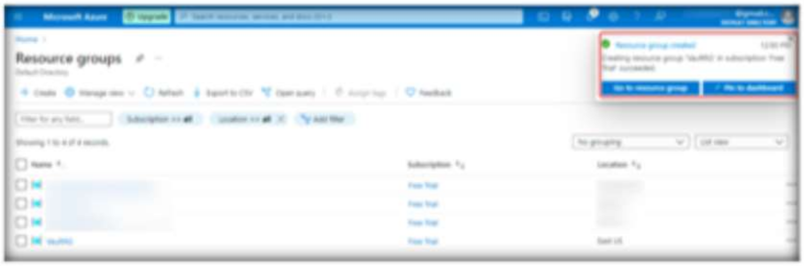


FIGURE 4.11.12: Resource Group Created Successfully

13. Click on **Home** at the top to go back to the Azure home page.

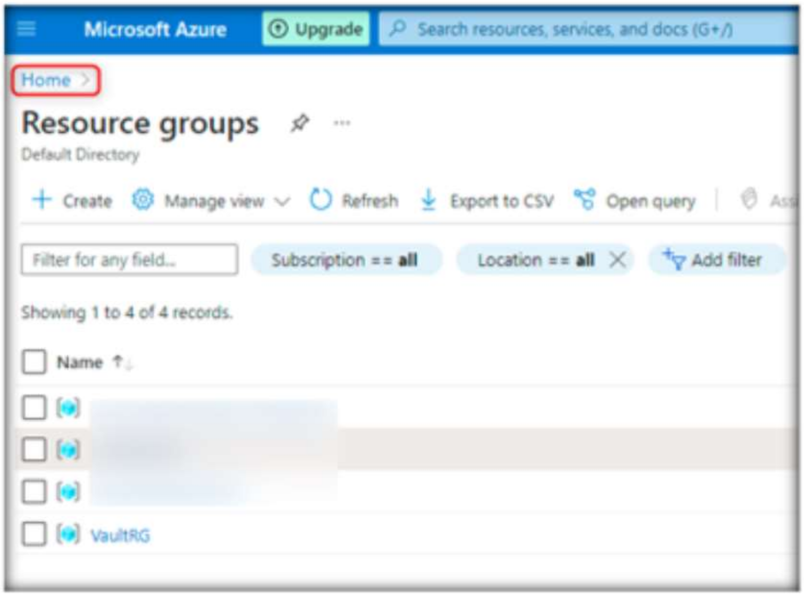


FIGURE 4.11.13: Navigating back to Home Page

TASK 2

Creating an Azure key vault to store passwords

14. Now, create a key vault to securely store the passwords. In the home page of Azure Portal, search for **Key Vault** at the top search bar and select **Key Vault** from the dropdown.

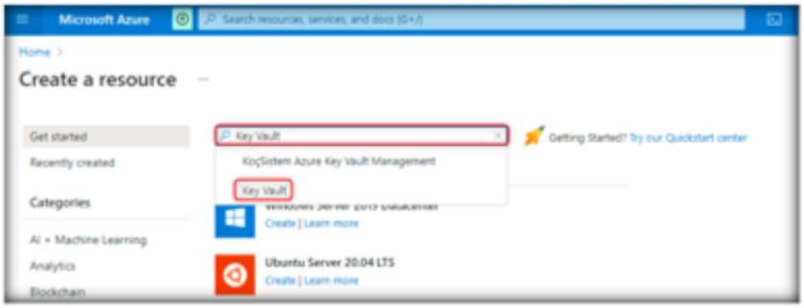
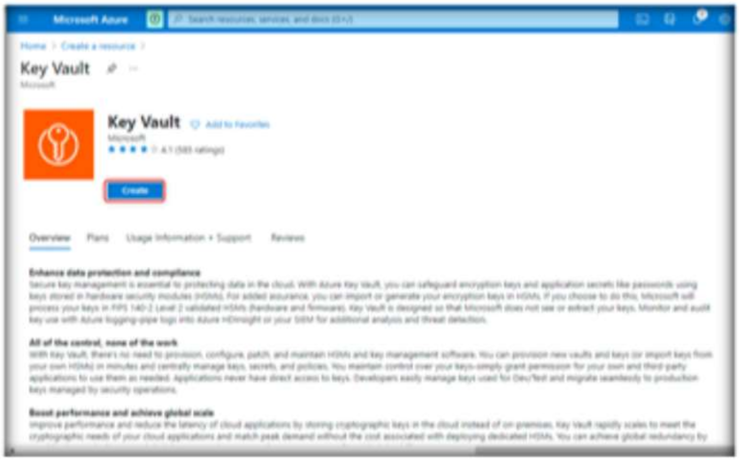


FIGURE 4.11.14: Navigating to Key Vault

15. In the **Key Vault** window, click on **Create**.



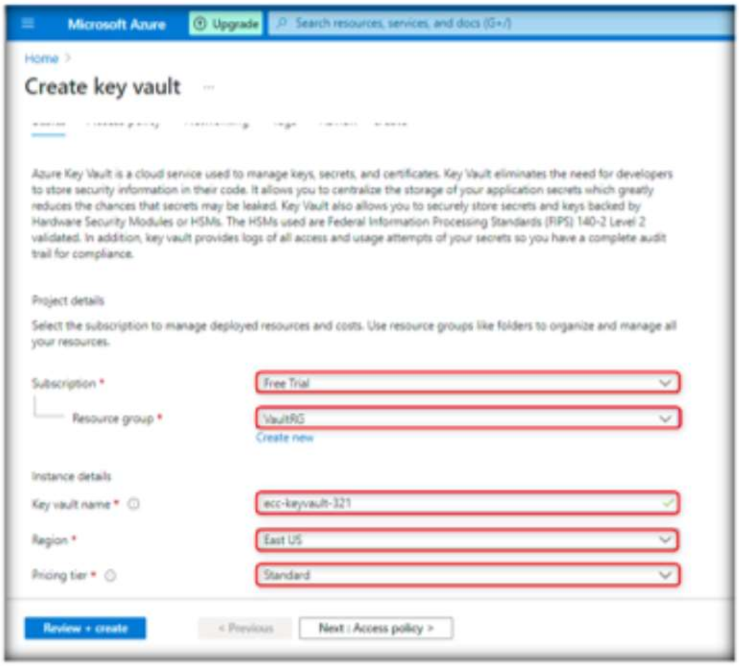
Enhance data protection and compliance
Secure key management is essential to protecting data in the cloud. With Azure Key Vault, you can safeguard encryption keys and application secrets like passwords using keys stored in hardware security modules (HSMs). For added assurance, you can import or generate your encryption keys in HSMs. If you choose to do this, Microsoft will process your keys in FIPS 140-2 Level 2 validated HSMs (hardware and firmware). Key Vault is designed so that Microsoft does not see or extract your keys. Monitor and audit key use with Azure logging-pipe logs into Azure HDInsight or your SIEM for additional analysis and threat detection.

All of the control, none of the work
With Key Vault, there's no need to provision, configure, patch, and maintain HSMs and key management software. You can provision new vaults and keys (or import keys from your own HSMs) in minutes and centrally manage keys, secrets, and policies. You maintain control over your keys-simply grant permission for your own and third-party applications to use them as needed. Applications never have direct access to keys. Developers easily manage keys used for Dev/Test and migrate seamlessly to production keys managed by security operations.

Boost performance and achieve global scale
Improve performance and reduce the latency of cloud applications by storing cryptographic keys in the cloud instead of on-premises. Key Vault rapidly scales to meet the cryptographic needs of your cloud applications and match peak demand without the cost associated with deploying dedicated HSMs. You can achieve global redundancy by

FIGURE 4.11.15: Creating Key Vault

16. The **Create key vault** window appears. For **Subscription**, select **Free trial** from the dropdown. Select the **Resource group (Vault RG)** created by you in the previous task from the dropdown. Under **Instance details**, enter a unique name that includes alphanumeric characters for **Key vault name**; here, we have used **ecc-keyvault-321**. Select an appropriate **Region**; here, we have selected **East US**. For **Pricing Tier**, select **Standard** from the dropdown.



Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Free Trial

Resource group * VaultRG

Create new

Instance details

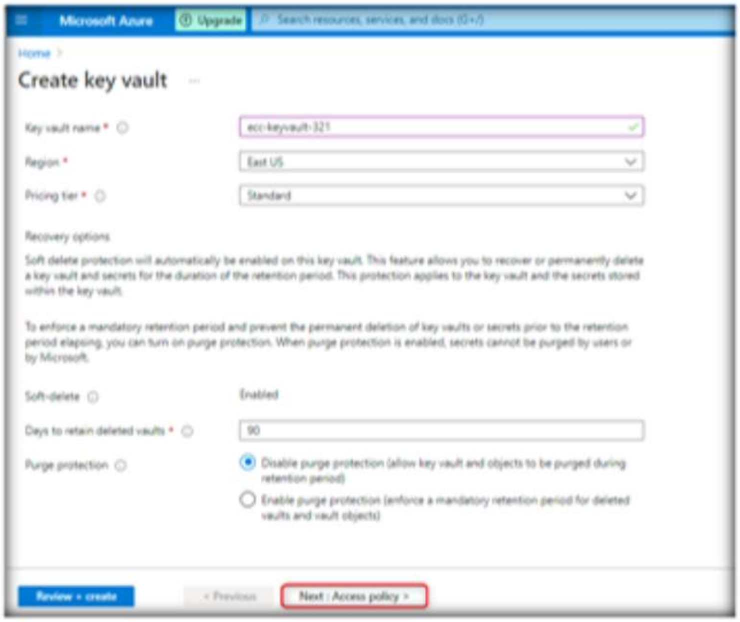
Key vault name * ecc-keyvault-321

Region * East US

Pricing tier * Standard

FIGURE 4.11.16: Configuring Key Vault

17. Do not change other default settings. Click on **Next : Access policy >**.



Create key vault

Key vault name * : ecc-keyvault-321

Region * : East US

Pricing tier * : Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

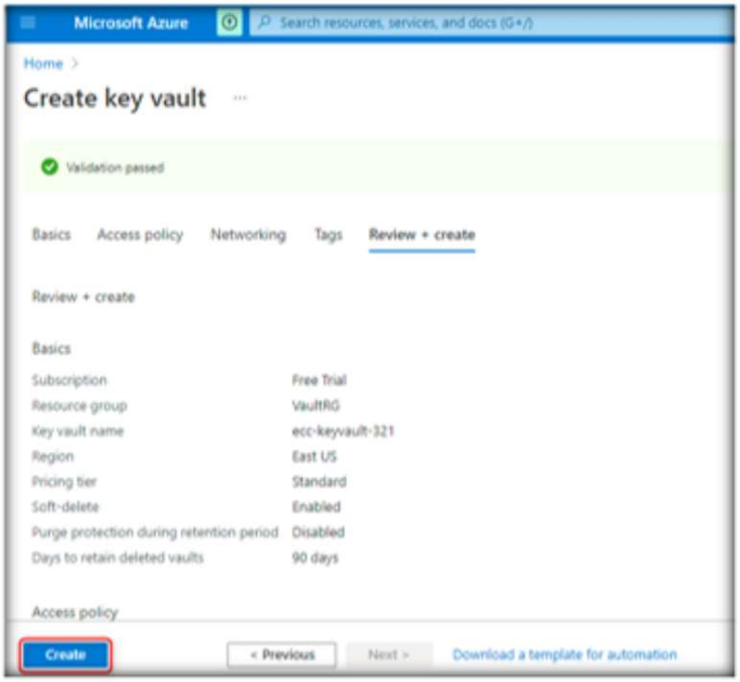
Soft-delete: Enabled

Days to retain deleted vaults * : 90

Purge protection:
● Disable purge protection (allow key vault and objects to be purged during retention period)
○ Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

FIGURE 4.11.17: Proceeding with Configuration

18. In the **Review + create** tab, verify the configuration. Click on **Create**.



Create key vault

Validation passed

Review + create

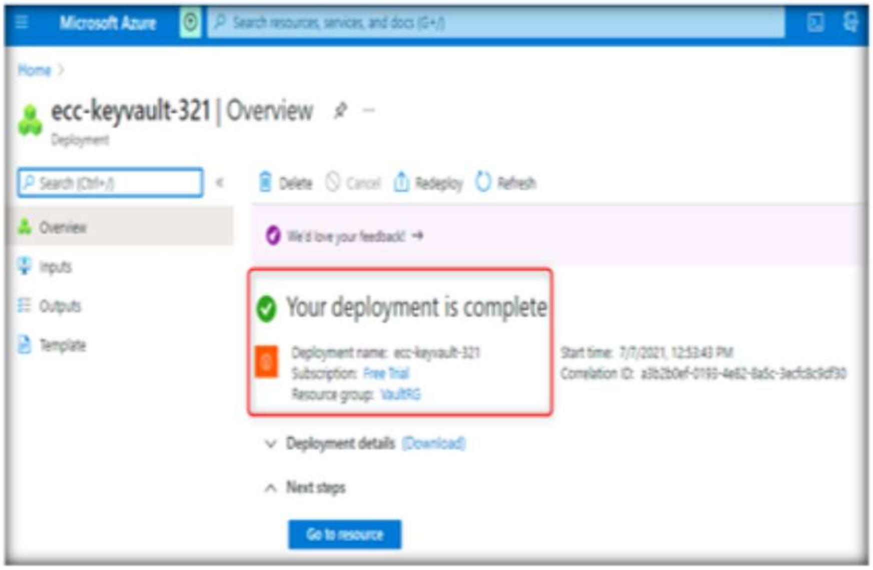
Basics

Subscription	Free Trial
Resource group	VaultRG
Key vault name	ecc-keyvault-321
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access policy

FIGURE 4.11.18: Creating Key Vault

19. Thus, the key vault is successfully created.



ecc-keyvault-321 | Overview

Deployment

Your deployment is complete

Deployment name: ecc-keyvault-321
Subscription: Free Trial
Resource group: VaultRG

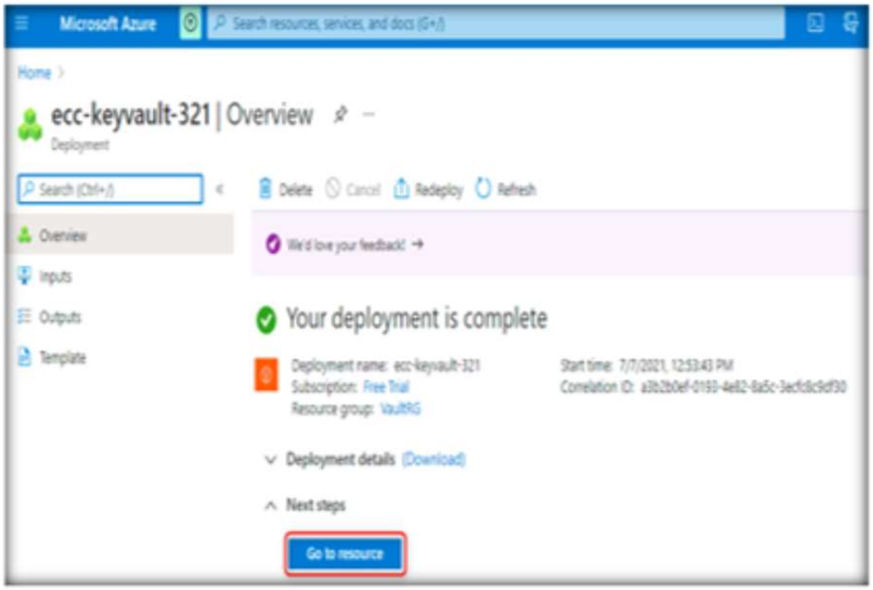
Start time: 7/7/2021, 12:53:43 PM
Correlation ID: a3b2b0ef-0193-4e82-8a5c-3ecfc8c9df30

FIGURE 4.11.19: Key Vault Created Successfully

TASK 3

Storing passwords in the key vault

20. Now, you have created the key vault to store passwords securely. To store a password in this key vault, click on **Go to resource** in the key vault deployment details window.



ecc-keyvault-321 | Overview

Deployment

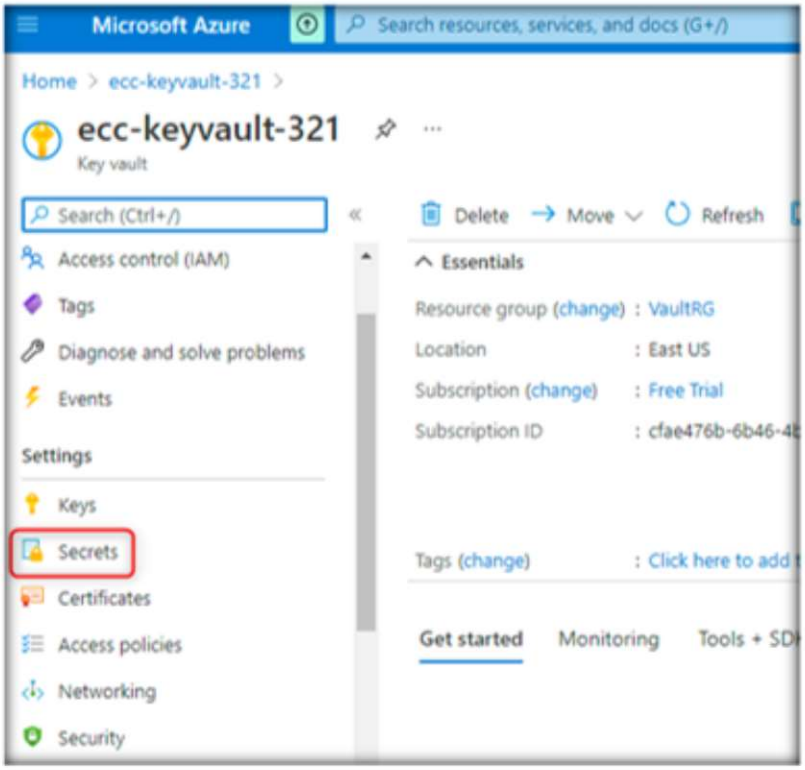
Your deployment is complete

Deployment name: ecc-keyvault-321
Subscription: Free Trial
Resource group: VaultRG

Start time: 7/7/2021, 12:53:43 PM
Correlation ID: a3b2b0ef-0193-4e82-8a5c-3ecfc8c9df30

FIGURE 4.11.20: Navigating to the Key Vault

21. In the left pane of the key vault (**ecc-keyvault-321**) window, click on **Secrets** under **Settings**.



Resource group (change) : VaultRG

Location : East US

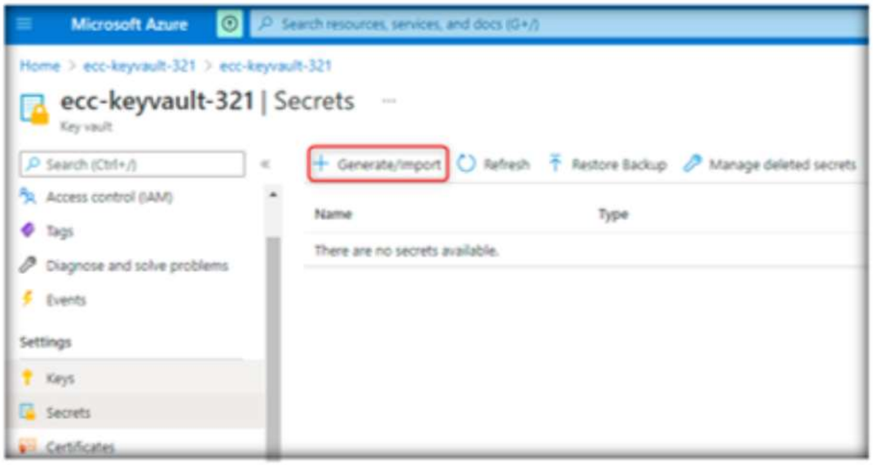
Subscription (change) : Free Trial

Subscription ID : cfae476b-6b46-4

Tags (change) : Click here to add

FIGURE 4.11.21: Navigating to Secrets

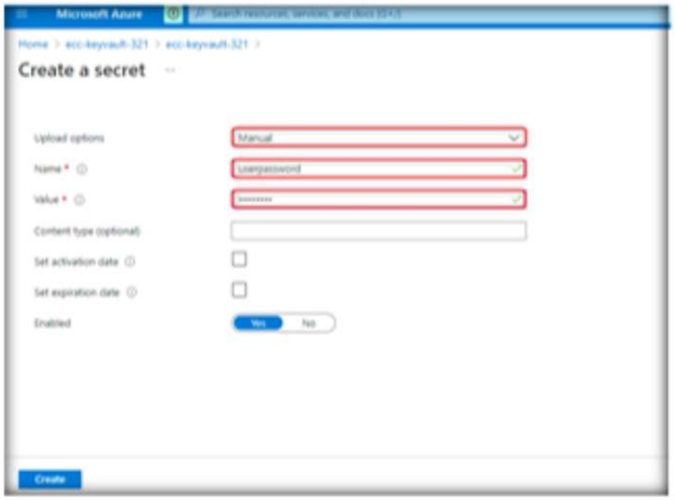
22. Click on **Generate/Import** to add a password.



There are no secrets available.

FIGURE 4.11.22: Adding Secret

23. In the **Create a secret** window, under **Upload**, select **Manual** from the dropdown. For **Name**, enter a name for the secret; here, we used **userpassword**. In the **Value** field, enter the secret (here, password) that you want to store securely. We entered the password "**user@123**" in the **Value** field.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > ecc-keyvault-321 > ecc-keyvault-321 >
Create
Yes
No

Create a secret

Upload options: Manual

Name *: userpassword

Value *: ••••••••

Content type (optional):

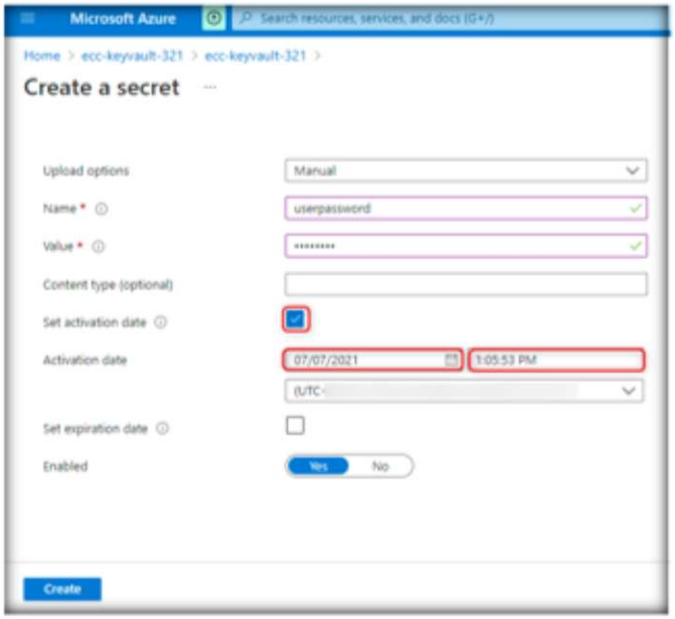
Set activation date: □

Set expiration date: □

Enabled: Yes

FIGURE 4.11.23: Creating Secret

24. Now, to set an activation date for access to the secret, enable the checkbox for **Set activation date**. Then, extra configuration options appear. In the **Activation date** field, set the date and time.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > ecc-keyvault-321 > ecc-keyvault-321 >
Create
Yes
No

Create a secret

Upload options: Manual

Name *: userpassword

Value *: ••••••••

Content type (optional):

Set activation date: ☑

Activation date: 07/07/2021 1:05:53 PM

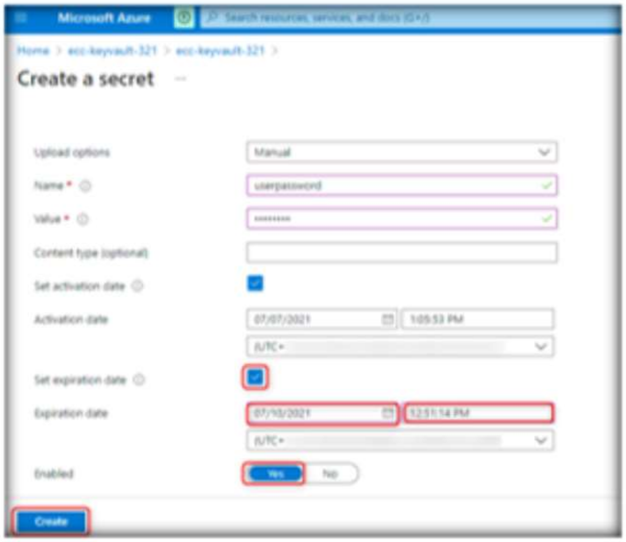
(UTC-

Set expiration date: □

Enabled: Yes

FIGURE 4.11.24: Configuring Activation Date

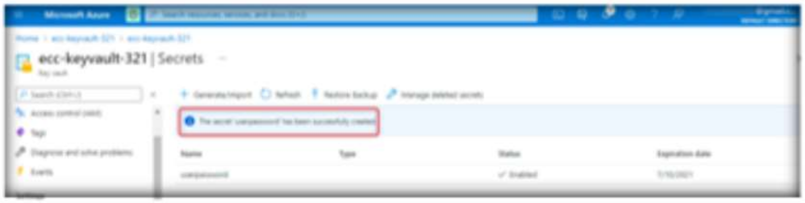
25. Now, to set an expiration date for access to the secret, enable the checkbox for **Set expiration date**. In the **Expiration date** field, set the date and time. Here, we have configured a three month expiration period. Toggle **Enabled** to **Yes** and click on **Create**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > ecc-keyvault-321 > ecc-keyvault-321 >
Create a secret
Create

Upload options: Manual
Name *: userpassword
Value *: ••••••••
Content type (optional):
Set activation date: ☑
Activation date: 07/07/2021 1:05:53 PM (UTC+
Set expiration date: ☑
Expiration date: 07/10/2021 12:51:14 PM (UTC+
Enabled: [✓ Yes] No

FIGURE 4.11.25: Creating Secret

26. Thus, the secret password is added successfully to the key vault.



The secret 'userpassword' has been successfully created.

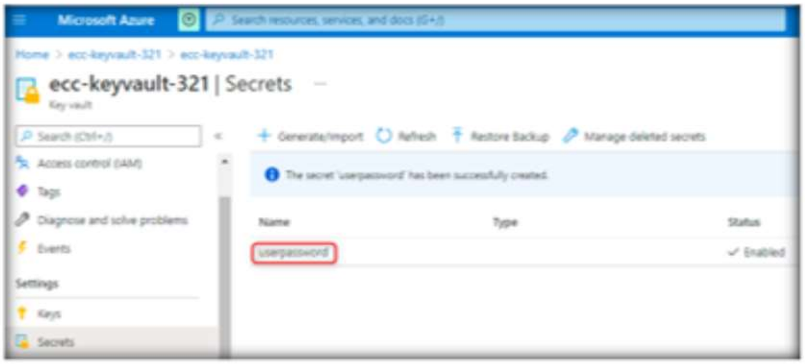
Name	Type	Status	Expiration date
userpassword		✓ Enabled	7/10/2021

FIGURE 4.11.26: Secret Created Successfully

TASK 4

Accessing the password from the Azure portal and shell

27. Now, to view the stored secret, i.e., password, from the Azure portal, click on the name (**userpassword**) of the secret.

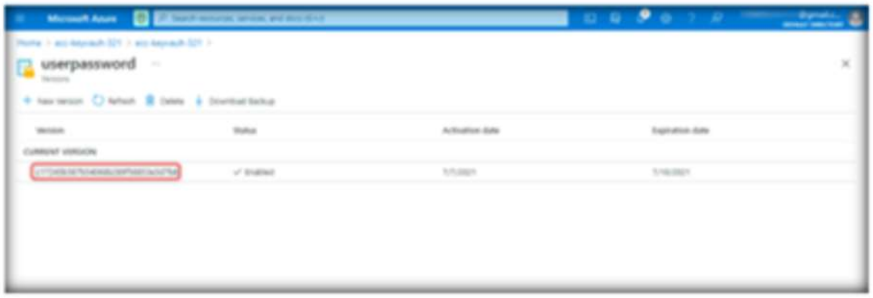


The secret 'userpassword' has been successfully created.

Name	Type	Status
userpassword		✓ Enabled

FIGURE 4.11.27: Viewing Secret

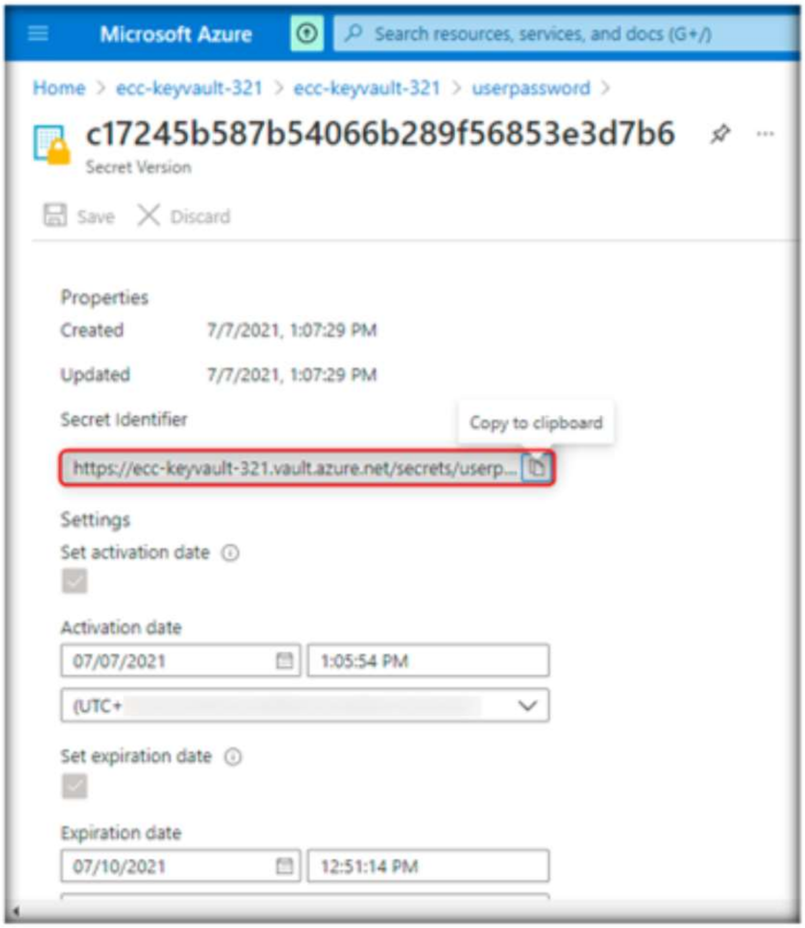
28. The **Version** pane for the secret appears. Click on the **CURRENT VERSION** whose **Status** is **Enabled** to view the secret.



Version	Status	Activation date	Expiration date
CURRENT VERSION			
c17245b587b54066b289f56853e3d7b6	✓ Enabled	7/7/2021	7/10/2021

FIGURE 4.11.28: Viewing Secret

29. You will see a link under **Secret Identifier**. This is the URI that can be used by authorized applications to access the secret.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > ecc-keyvault-321 > ecc-keyvault-321 > userpassword >
Save
Discard
Copy to clipboard

c17245b587b54066b289f56853e3d7b6

Secret Version

Properties

Created 7/7/2021, 1:07:29 PM

Updated 7/7/2021, 1:07:29 PM

Secret Identifier

https://ecc-keyvault-321.vault.azure.net/secrets/userp...

Settings

Set activation date ☑

Activation date

07/07/2021 1:05:54 PM

(UTC+

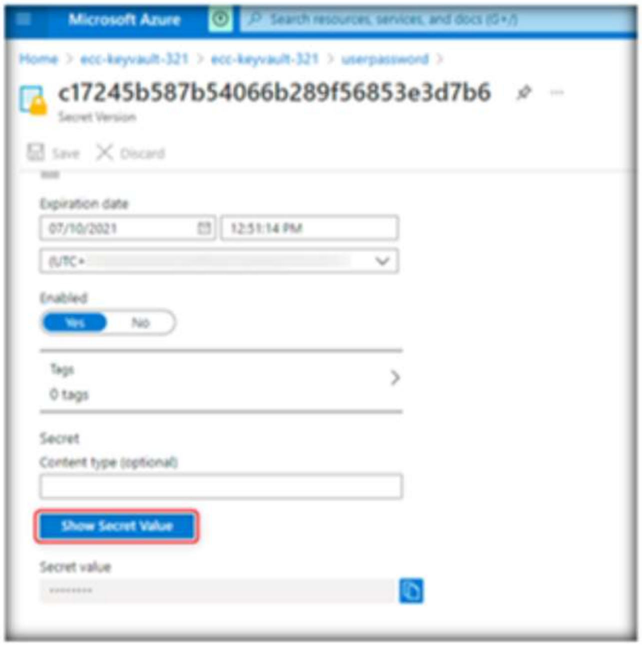
Set expiration date ☑

Expiration date

07/10/2021 12:51:14 PM

FIGURE 4.11.29: Secret Identifier URI

30. Now, to view the secret, under **Secret**, click on **Show Secret Value**.



Home > ecc-keyvault-321 > ecc-keyvault-321 > userpassword >

c17245b587b54066b289f56853e3d7b6

Secret Version

Expiration date: 07/10/2021 12:51:14 PM

(UTC+

Enabled: Yes No

Tags: 0 tags

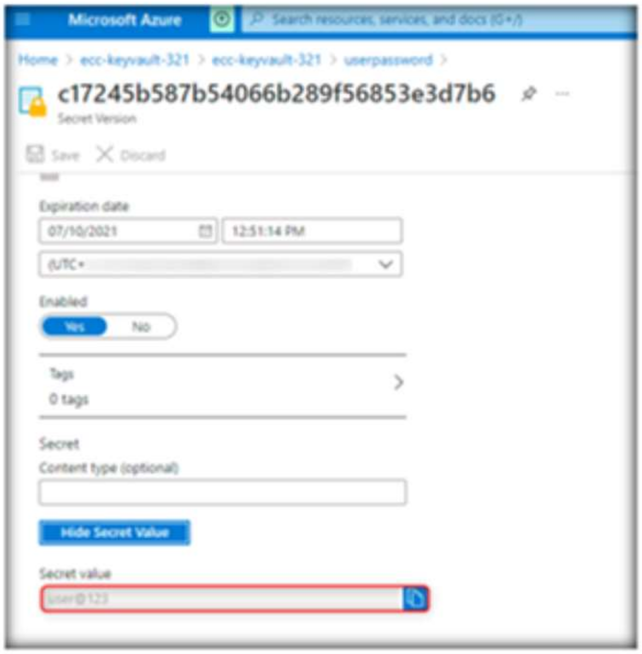
Secret

Content type (optional)

Secret value: ••••••••

FIGURE 4.11.30: Viewing Secret Value

31. You will see the stored secret under **Secret Value**.



Home > ecc-keyvault-321 > ecc-keyvault-321 > userpassword >

c17245b587b54066b289f56853e3d7b6

Secret Version

Expiration date: 07/10/2021 12:51:14 PM

(UTC+

Enabled: Yes No

Tags: 0 tags

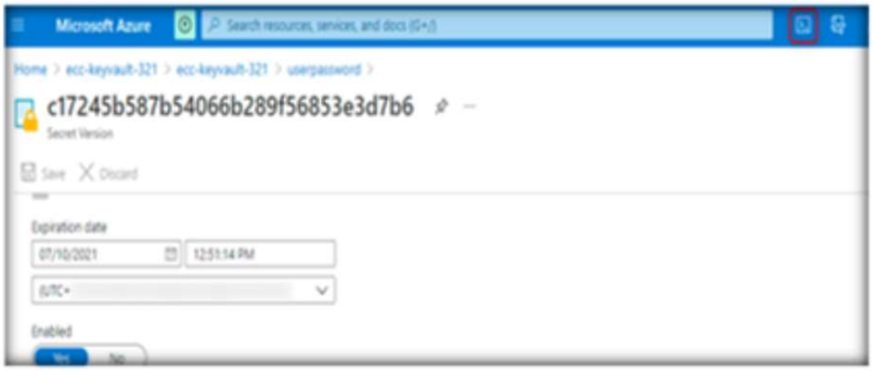
Secret

Content type (optional)

Secret value: user@123

FIGURE 4.11.31: Viewing the Secret

32. Now, to view the secret in Azure PowerShell, click on the power shell icon at the top right corner of the console.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > ecc-keyvault-321 > ecc-keyvault-321 > userpassword >
c17245b587b54066b289f56853e3d7b6
Secret Version
Save
Discard
Yes
No

Expiration date: 07/10/2021 12:51:14 PM

(UTC+

Enabled

FIGURE 4.11.32: Opening PowerShell

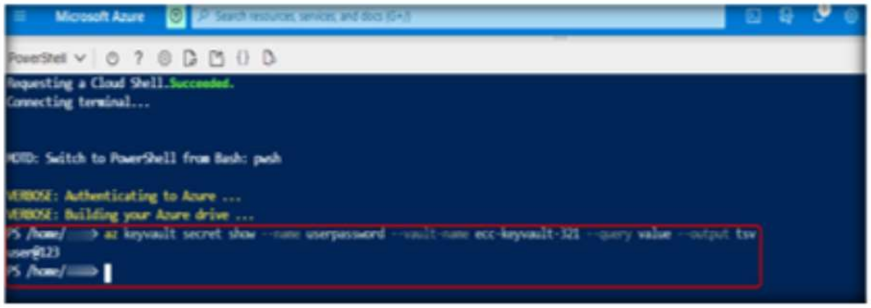
33. In the Azure PowerShell window, type the following command and press **Enter** to view the stored secret in the key vault.

```
az keyvault secret show --name <secret_name> --
vault-name <vault_name> --query value --output
tsv
```

Here, replace <secret_name> with the name of your secret and <vault_name> with the name of the key vault. For e.g., here, we have used the following command.

```
az keyvault secret show --name userpassword --
vault-name ecc-keyvault-321 --query value --
output tsv
```

The stored secret (i.e., password) is displayed as output.



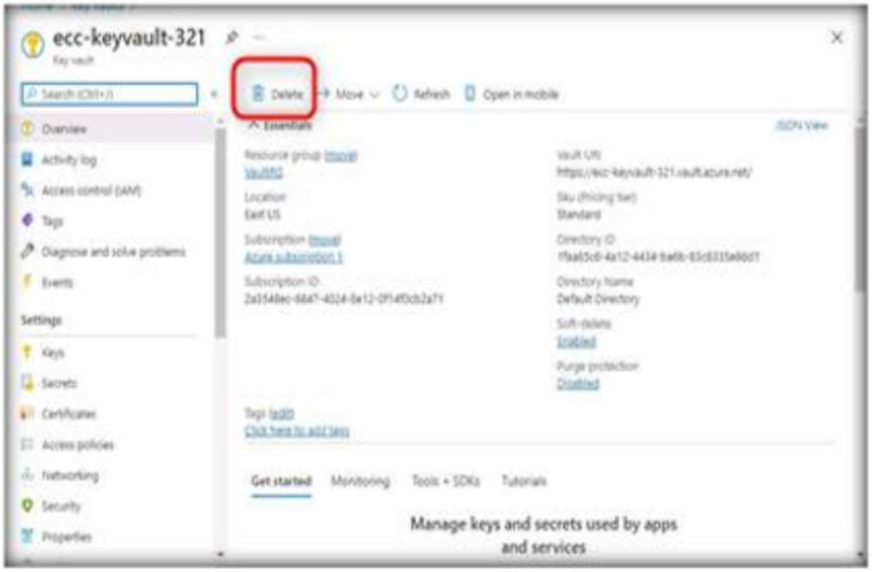
```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...


MOTD: Switch to PowerShell from Bash: pwsh

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/[redacted]> az keyvault secret show --name userpassword --vault-name ecc-keyvault-321 --query value --output tsv
user@123
PS /home/[redacted]>
```

FIGURE 4.11.33: Viewing Secret in PowerShell

34. Thus, a cloud security engineer can use the Azure Key Vault service to securely store and access secrets such as passwords.

Caution: Ensure you delete, shut down, or terminate all resources created and used in this lab to prevent their billing.

35. Navigate to **Key vaults** in Azure portal. Click on the name of the key vault (**ecc-keyvault-321**) in the **Key vaults** window. Click on **Delete** in the key vault (**ecc-keyvault-321**) details window that opens.



Resource group (move): VaultRG

Location: East US

Subscription (move): Azure subscription 1

Subscription ID: 2a3548ec-6847-4024-8e12-0f14f0cb2a71

Tags (edit): Click here to add tags

Vault URI: https://ecc-keyvault-321.vault.azure.net/

Sku (Pricing tier): Standard

Directory ID: [illegible]

Directory Name: Default Directory

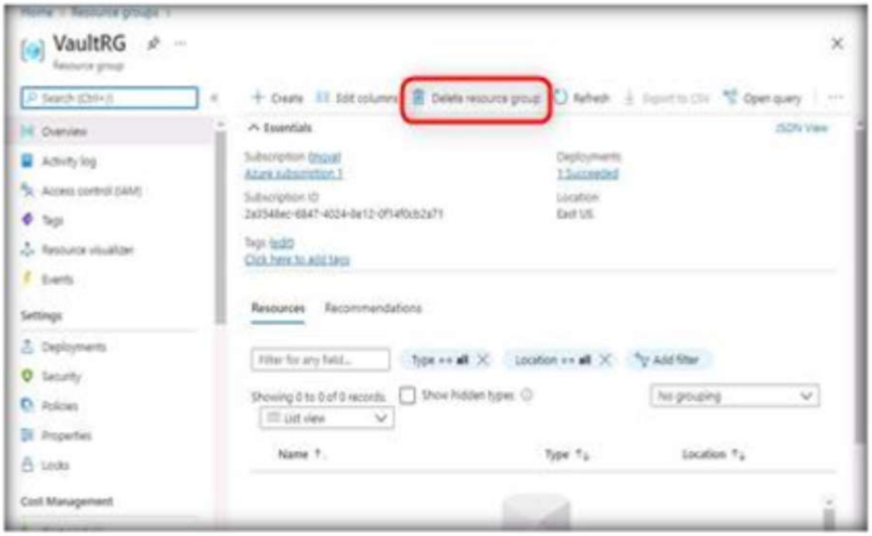
Soft-delete: Enabled

Purge protection: Disabled

Manage keys and secrets used by apps and services

FIGURE 4.11.34: Deleting Key vault

36. Navigate to **Resource groups** in Azure Portal. Click on the name of the resource group (**VaultRG**). Click on **Delete resource group** in the resource group details window that opens.



Subscription (move): Azure subscription 1

Subscription ID: 2a3548ec-6847-4024-8e12-0f14f0cb2a71

Tags (edit): Click here to add tags

Deployments: 1 Succeeded

Location: East US

Showing 0 to 0 of 0 records.

FIGURE 4.11.35: Deleting Resource Group

Lab Analysis

Analyze and document the results of this lab exercise. Provide your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.