



Lab 8

Disabling Anonymous Access to Blob Container in Azure

Microsoft Azure offers Azure Blob Storage for storing large amounts of unstructured data in its storage platform.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

Lab Scenario

To prevent an anonymous access to blob containers, a cloud security administrator should change its access settings from public to private. You should allow only private access to the containers, until and unless there is a need to change the settings.

Lab Objectives

In this lab, you will learn how to create a container with no anonymous access and how to change its access level from public to private.

In this lab you will:

- Create a resource group
- Create a storage account
- Create a container with no anonymous access
- Create a container with anonymous access
- Change the access of the container from public to private

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Lab Duration

Time: 15 minutes

Overview of Blob Container

Azure blob storage is designed to store massive amounts of unstructured data such as images, documents, log files, backups, and audio and video streaming files. The three types of blob storage resources are storage accounts, containers in a storage account, and blobs in a container. With public-access configuration settings, an anonymous user can use the constructor to access the blob containers and will be allowed to access them without any credentials, such as SAS. Hence, when a blob container's access is changed from public to private, an anonymous user will not be allowed to access it.

A container can be changed to public or private if the storage account level access is public. If the storage account level is set to private, then all containers become private by default and cannot be changed to public. The use of a shared access signature token is recommended to enable a controlled access.

Lab Tasks

Note: Web applications in a cloud environment may undergo frequent updates. As we are working on a cloud-based environment for this lab (i.e., Azure), the application interface may be updated with time. Hence, in case you happen to work on an updated version of Azure, the user interface you see on the application might differ from what you see in the lab. Consequently, the steps and screenshots demonstrated in this lab might also differ.

Note: Before starting this lab, you should create a Microsoft Azure account using the following link: <https://azure.microsoft.com/en-in/free/>. Once you have created your Microsoft Azure account, perform the following tasks.

TASK 1

Creating a Resource Group

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

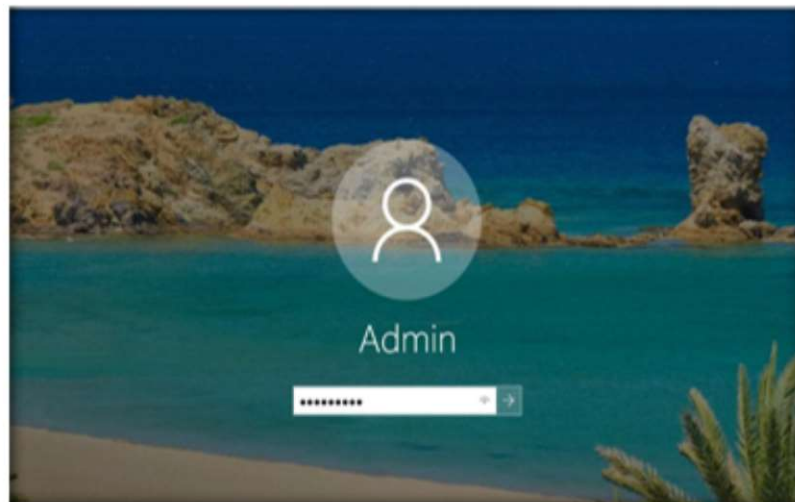


FIGURE 4.9.1: Launch Admin Machine and Log in

Module 04 – Data Security in Cloud

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



FIGURE 4.9.2: 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**.

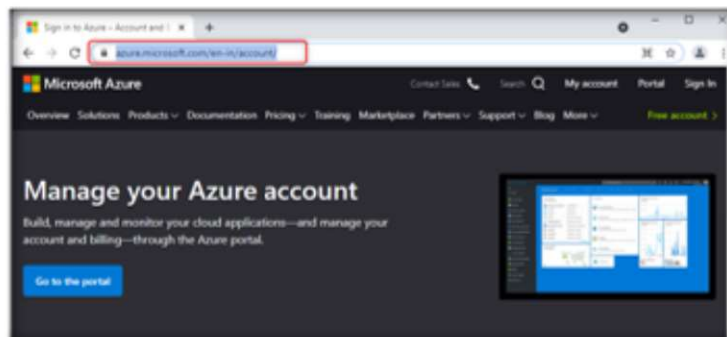


FIGURE 4.9.3: Entering the URL of Microsoft Azure

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

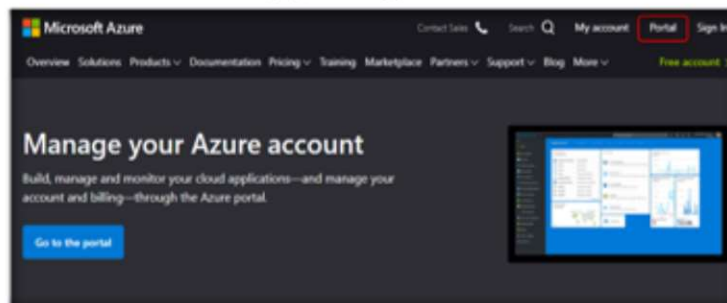


FIGURE 4.9.4: Sign into Azure Portal

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

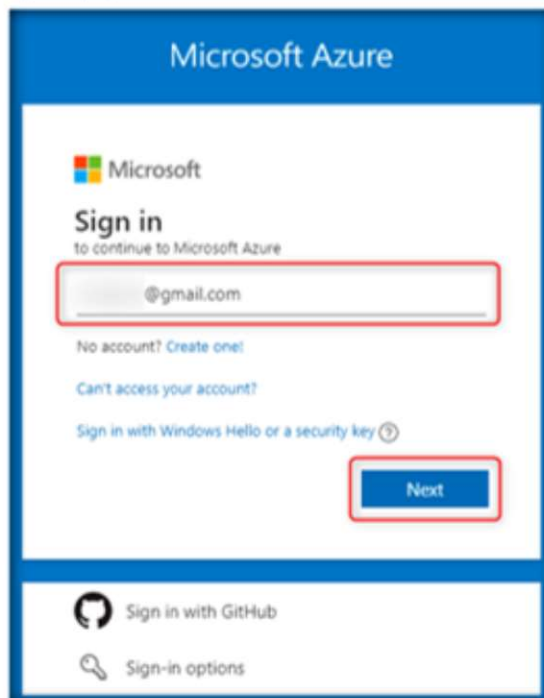


FIGURE 4.9.5: Entering Account ID to continue

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



FIGURE 4.9.6: Sign in to Azure Account

Module 04 – Data Security in Cloud

7. You will be successfully logged in to **Microsoft Azure** portal. In the Azure portal, select and click on **Resource groups**.

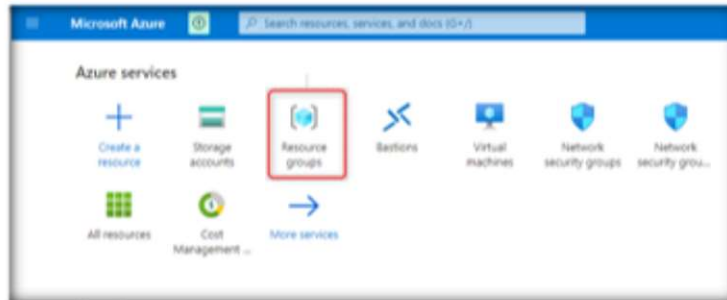


FIGURE 4.9.7: Selecting Resource Groups

8. To create a resource group, click on **+Add** in the **Resource groups** page.

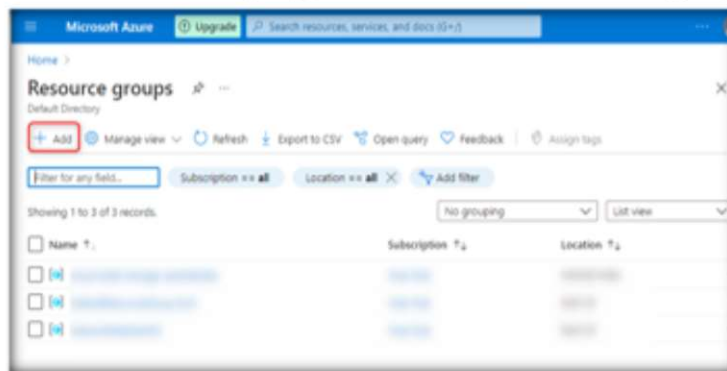


FIGURE 4.9.8: Adding New Resource Group

9. A **Create a resource group** page will open. Enter the resource group name as **ecstorageRG** in the **Resource group** field and select **(US) East US** in the **Region** field. Now, click on the **Next: Tags >** button.

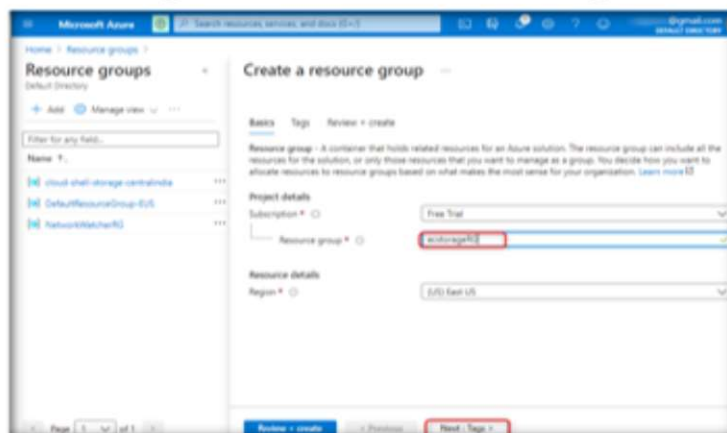


FIGURE 4.9.9: Entering Resource Group Name and Location

10. Leave the **Tags** tab in its default state and click on **Review + create>**.

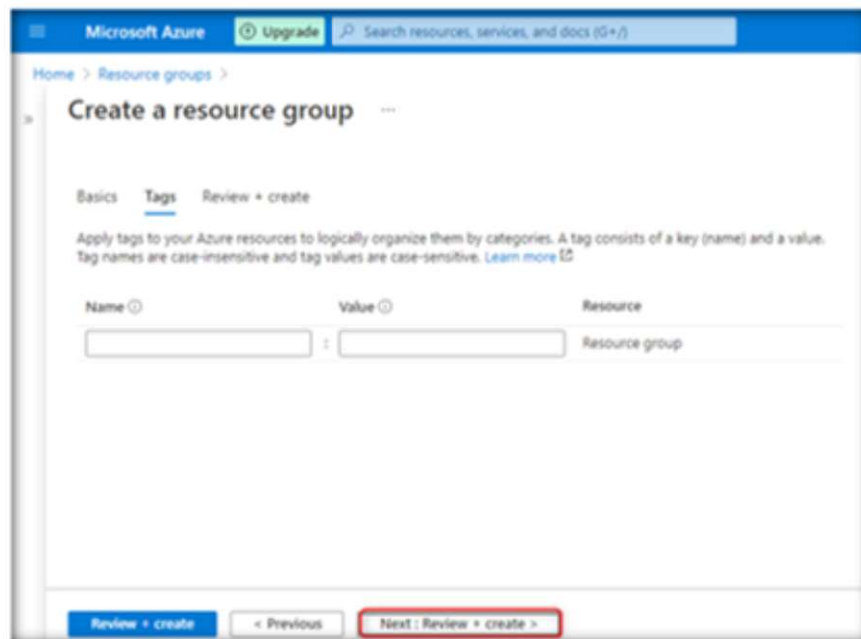


FIGURE 4.9.10: Reviewing and Creating Resource Group

11. After observing the **Validation passed** message, click on the **Create** button.

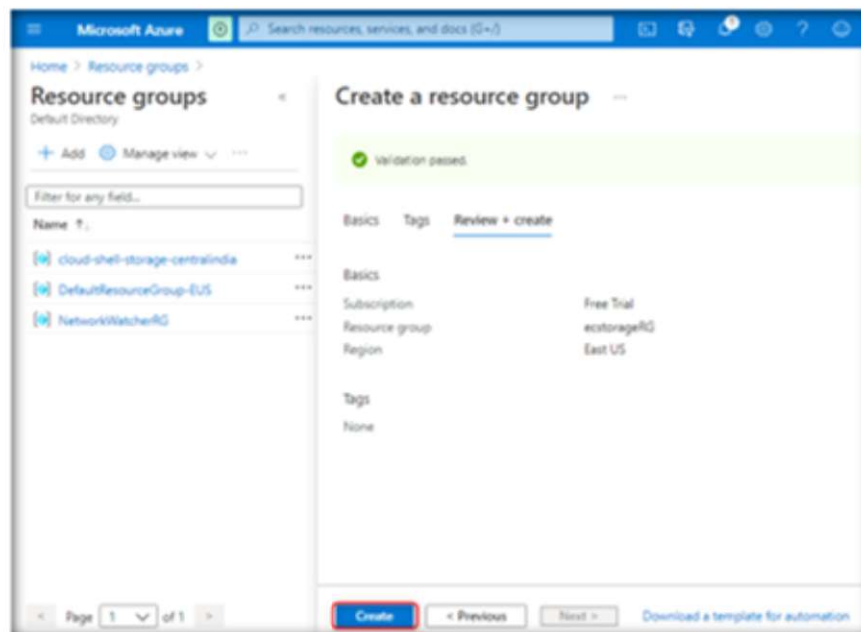


FIGURE 4.9.11: Validation Passed for Creating a Resource Group

12. Resource group **ecstorageRG** has been successfully created.

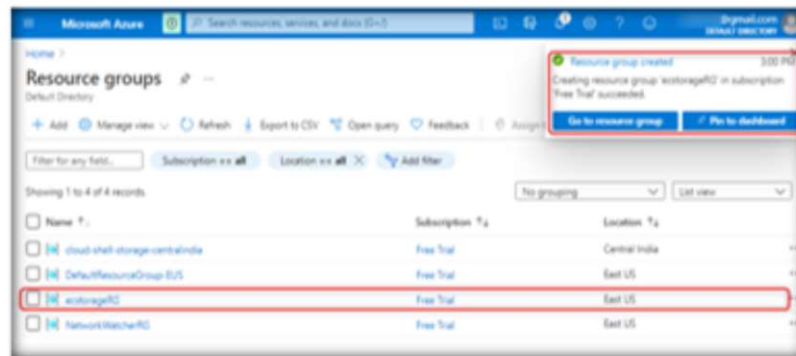


FIGURE 4.9.12: Successfully Creating Resource Group

TASK 2

Creating a Storage Account in the Resource Group

13. Now, to create a storage account, select the **ecstorageRG** resource group.

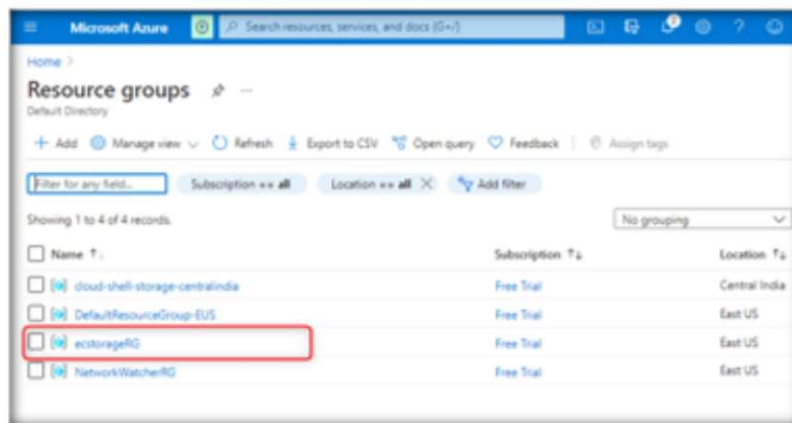


FIGURE 4.9.13: Selecting Resource Group

14. Click on **+Add** in the **ecstorageRG** window.

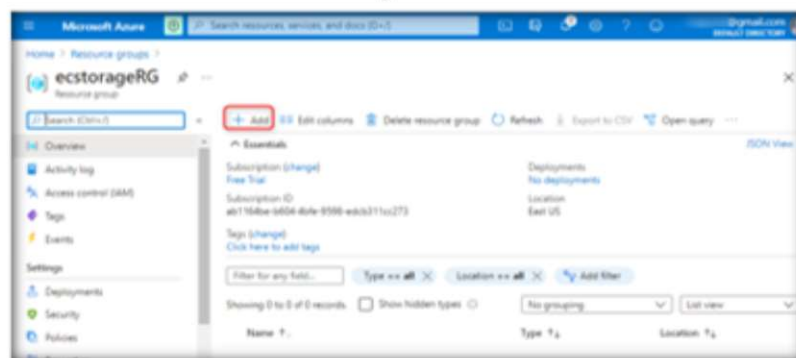


FIGURE 4.9.14: Creating a New Storage Account

Module 04 – Data Security in Cloud

15. A **Create a resource** window will open. In the search box, type storage account, and then navigate and click on **Storage account**.

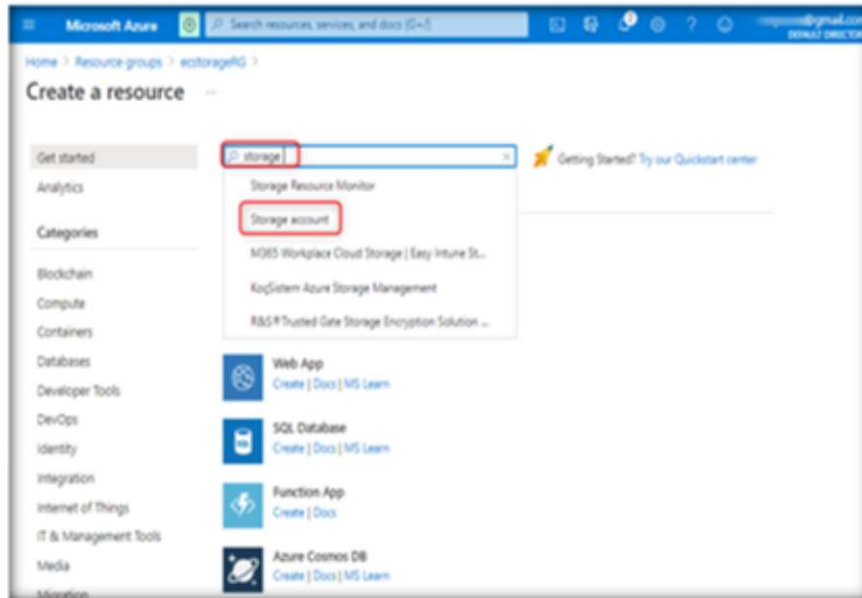


FIGURE 4.9.15: Searching and Selecting Storage Account

16. In the **Storage account** window that opens, click on the **Create** button.

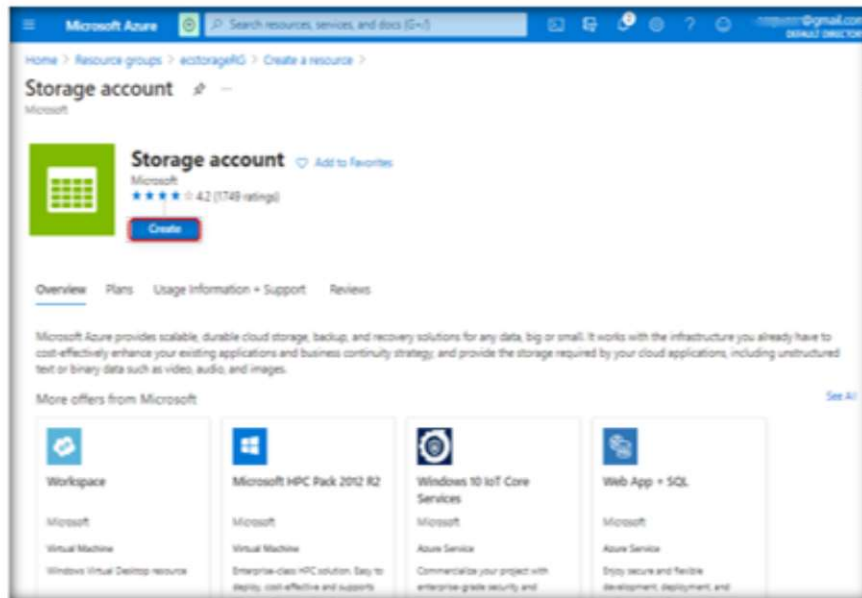


FIGURE 4.9.16: Creating a Storage Account

17. A **Create a storage account** window will open. In the **Resource group** field, click on the dropdown and select **ecstorageRG**.

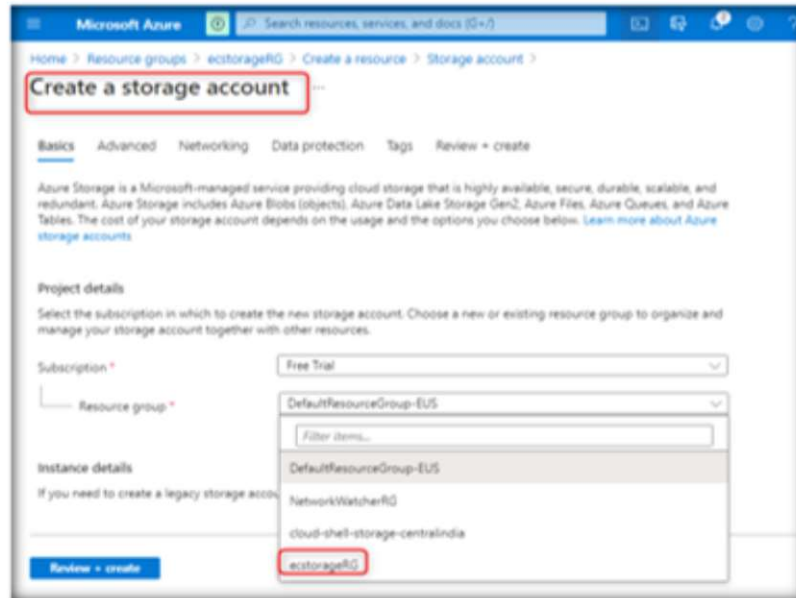


FIGURE 4.9.17: Selecting Resource Group for Storage Account

18. Type the **Storage account name** (here, we have entered **productstorage1225**), leave other options in their default state, and then click on the **Next: Advanced >** button.

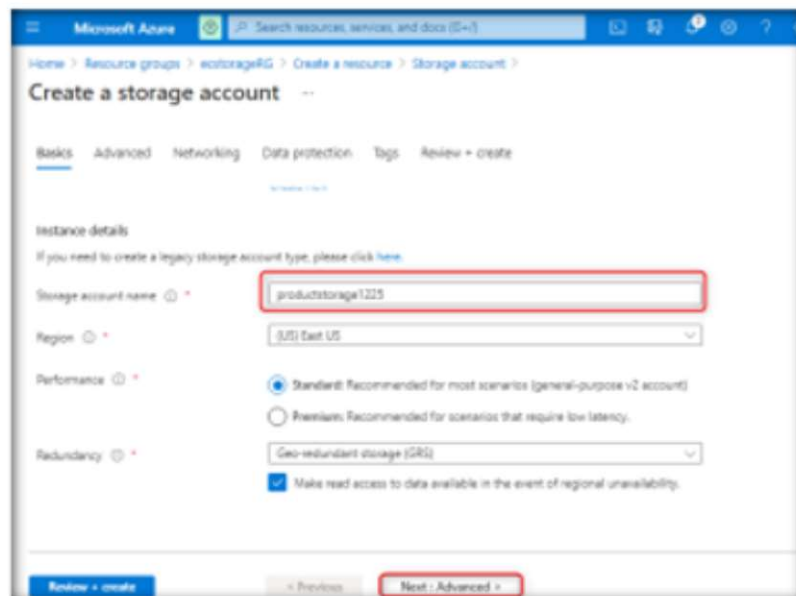


FIGURE 4.9.18: Entering the Name of the Storage Account

19. In the **Advanced** tab, leave everything in their default state and click on the **Next: Networking >** button.

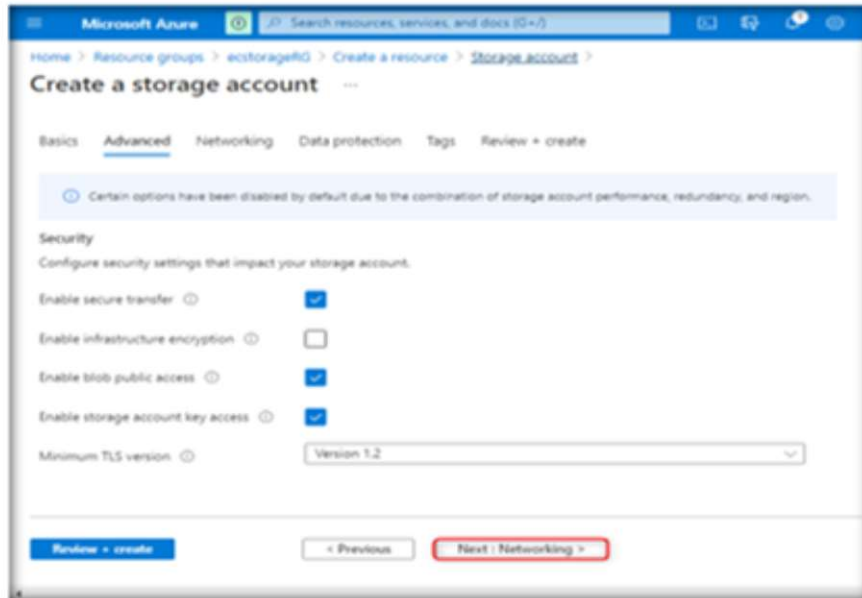


FIGURE 4.9.19: Leaving Everything in Default State in Advanced Tab

20. In the **Networking** tab, leave everything in their default state and click on **Next: Data protection >**.

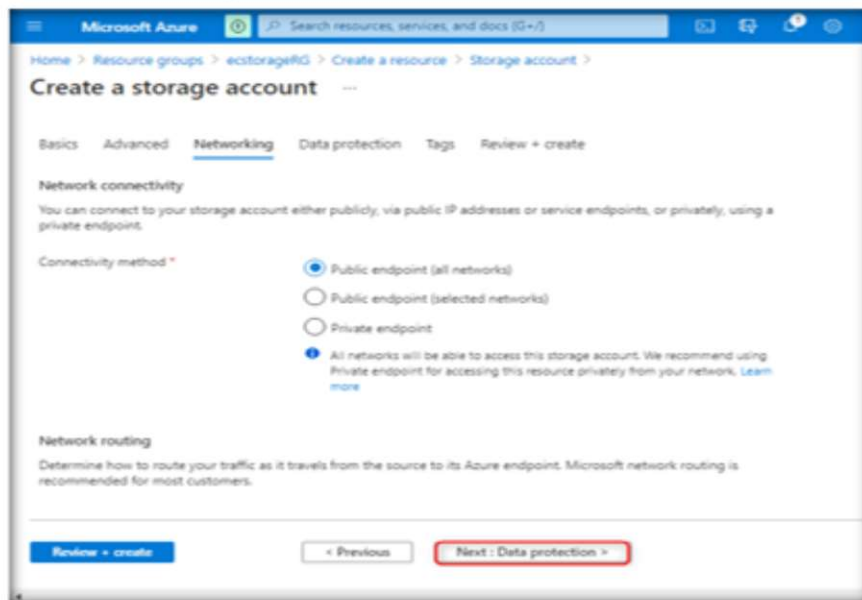


FIGURE 4.9.20: Leaving Everything in Default State in Networking Tab

Module 04 – Data Security in Cloud

21. In the **Data protection** tab, leave everything in their default state and click on **Next: Tags >**.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Data protection' tab is selected. Under the 'Recovery' section, the following options are visible:

- ☐ **Enable point-in-time restore for containers**
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)
- ☒ **Enable soft delete for blobs**
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)
Days to retain deleted blobs:
- ☒ **Enable soft delete for containers**
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)
Days to retain deleted containers:

At the bottom, the 'Next: Tags >' button is highlighted with a red rectangle.

FIGURE 4.9.21: Leaving Everything in Default State in Data Protection Tab

22. In the **Tags** tab, leave everything in their default state and click on **Next: Review + create >**.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal, with the 'Tags' tab selected. It displays a table for adding tags:

Name	Value	Resource
<input type="text"/>	<input type="text"/>	<input type="text" value="All resources selected"/>

At the bottom, the 'Next: Review + create >' button is highlighted with a red rectangle.

FIGURE 4.9.22: Leaving Everything in Default State in Tags Tab

23. After you see the **Validation passed** message, click on the **Create** button.

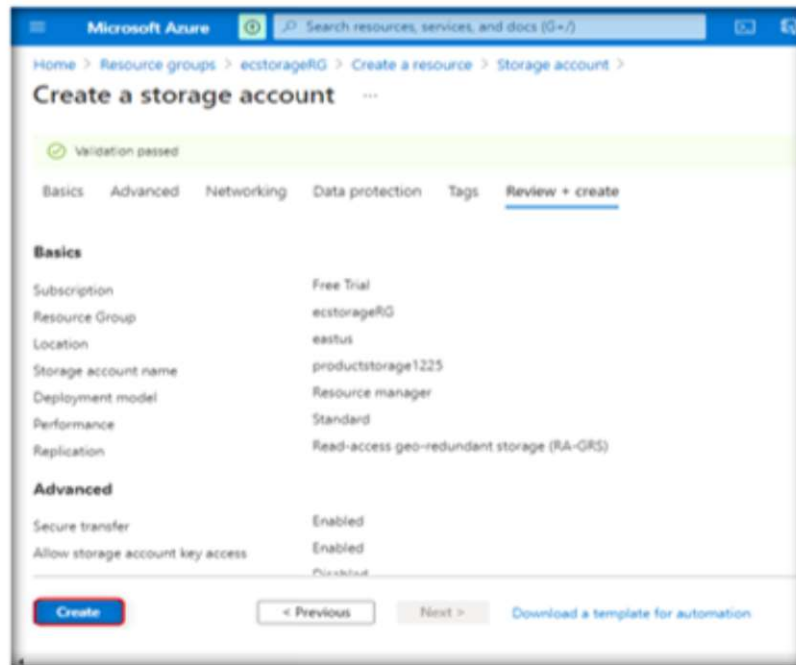


FIGURE 4.9.23: Passing the Validation

24. Wait for a few seconds for the storage account to be deployed.

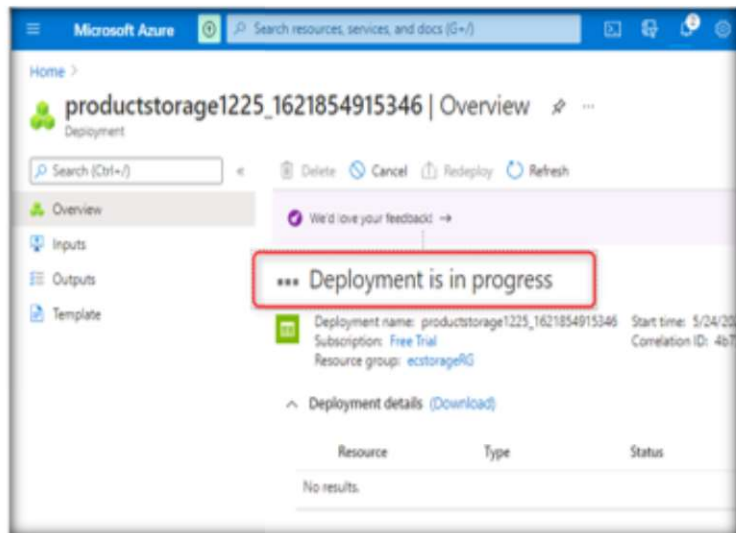


FIGURE 4.9.24: Storage Account Deployment Status

25. After the deployment is complete, click on the **Go to resource** button.

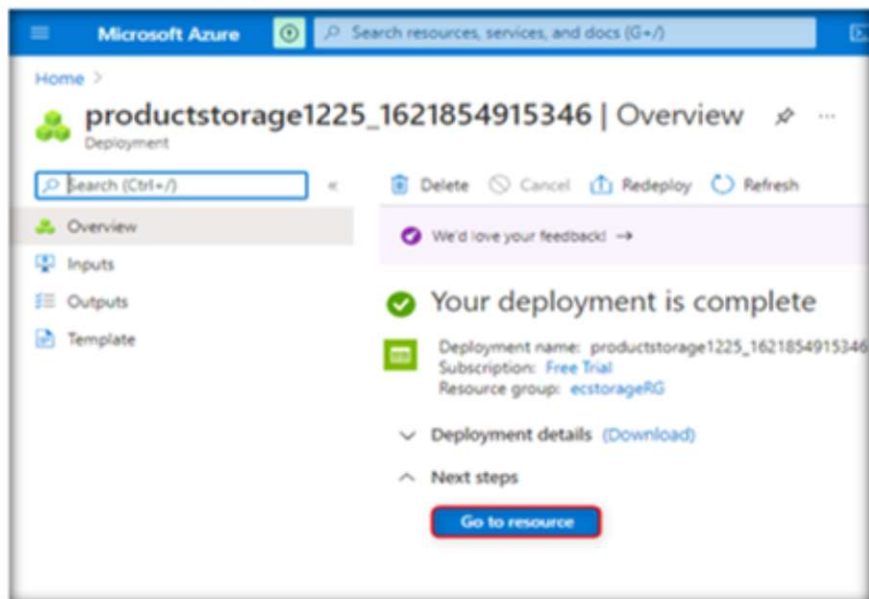


FIGURE 4.9.25: Successful Deployment of Storage Account

26. The **storage account** is now successfully **created**.

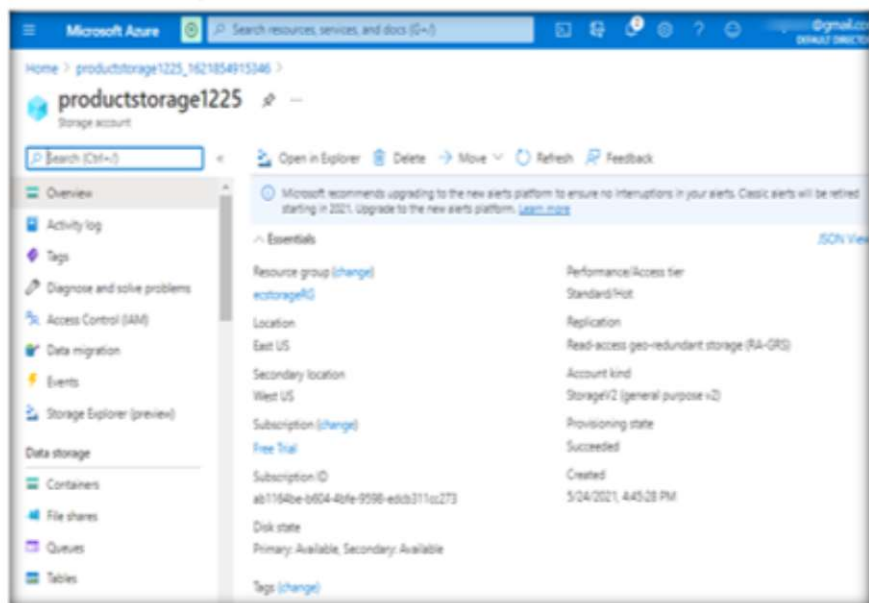


FIGURE 4.9.26: Successfully Creation of New Storage Account

TASK 3
Creating a Container with no Anonymous Access

27. Now, to create a private container with anonymous access in the storage account (**productstorage1225** in this lab), navigate and click on **Containers** in the left pane under **Data storage**.

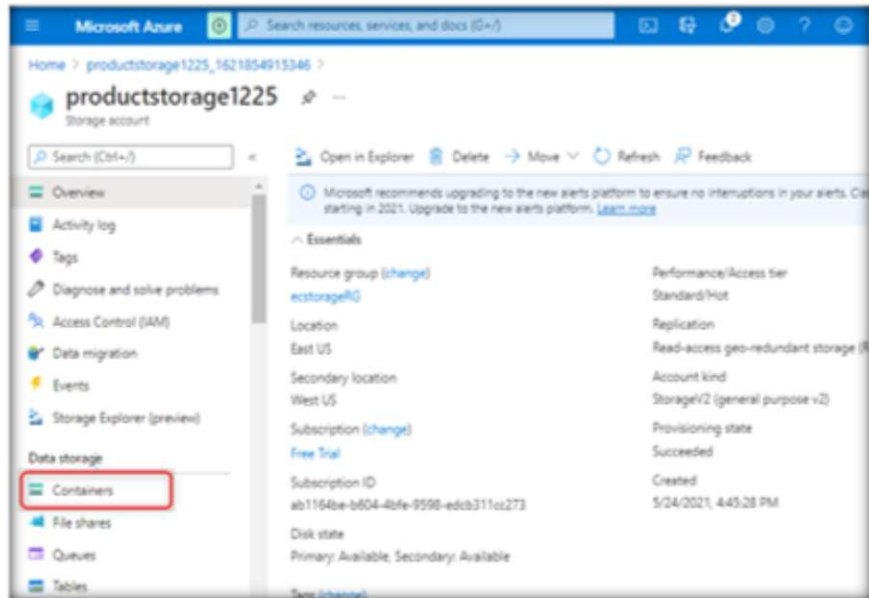


FIGURE 4.9.27: Selecting Containers in Storage Account

28. Click on **+ Container**.

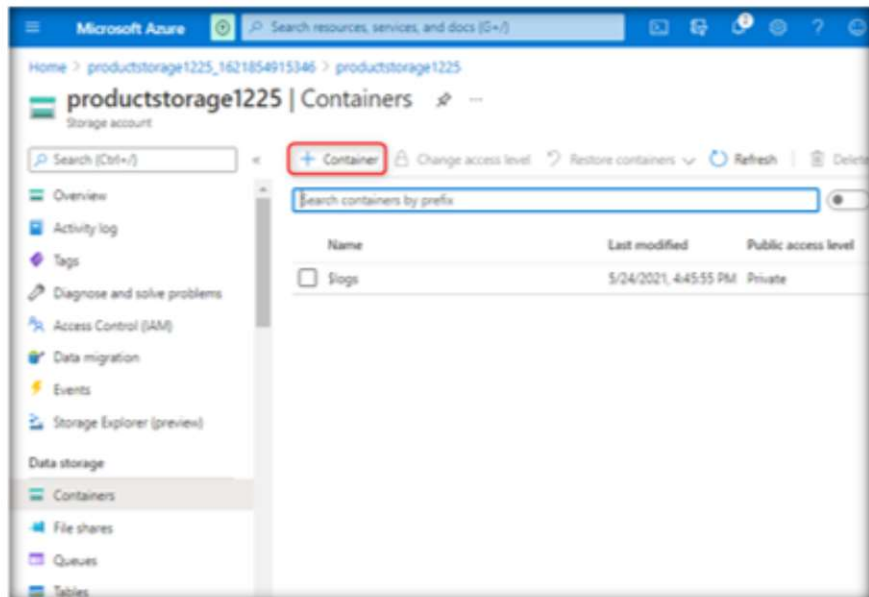


FIGURE 4.9.28: Creating a New Container

Module 04 – Data Security in Cloud

29. A **New container** window will open. Here, enter the name of the container (here, we have used **testcontainer11**) and click on the dropdown under **Public access level** and select **Private (no anonymous access)**. Then, click on the **Create** button.

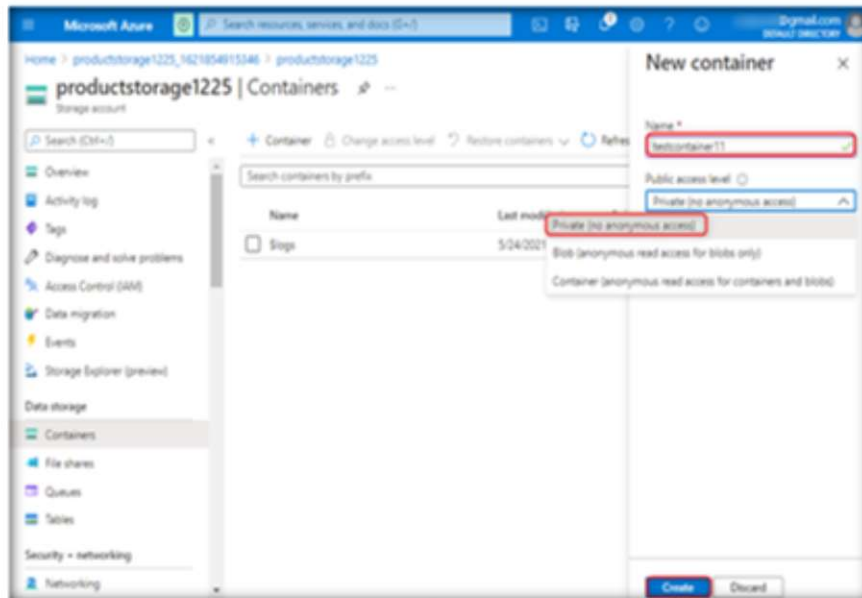


FIGURE 4.9.29: Filling Container Details in New Container Window

30. A private container without anonymous access is successfully created now.

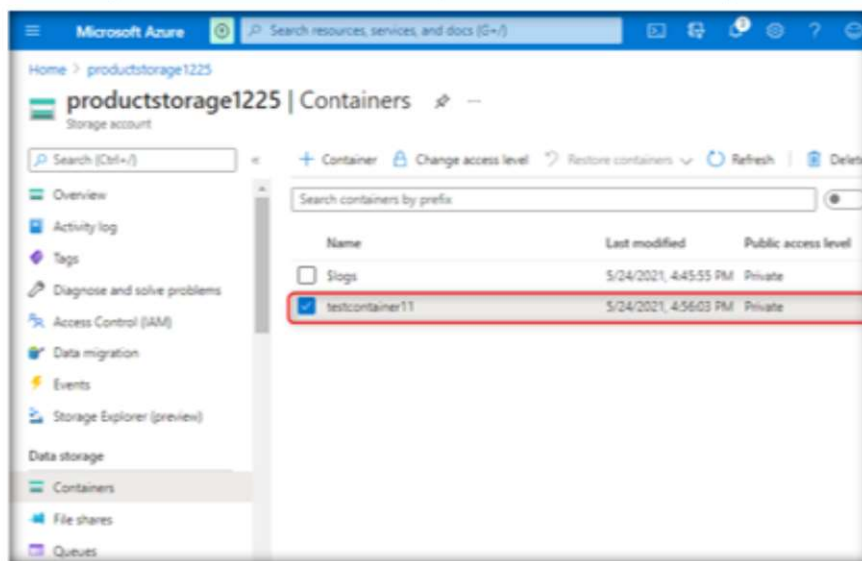


FIGURE 4.9.30: Successfully Creating Container with No Anonymous Access

TASK 4
Creating a Container with Anonymous Access

31. Now, we will create another container with anonymous read access. Click on **+ Container** in the **productstorage1225** window.

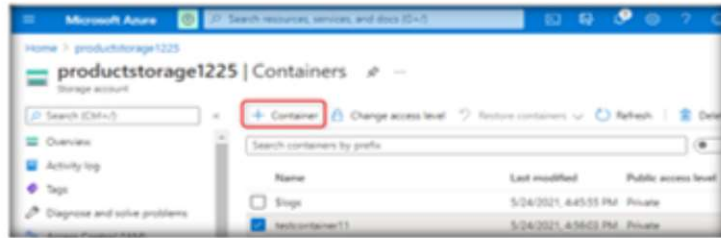


FIGURE 4.9.31: Creating a New Container

32. A **New container** window will open. Here, enter the name of the container (we have used **testcontainer22**) and click on the dropdown under **Public access level** and select **Container (anonymous read access for containers and blobs)**.

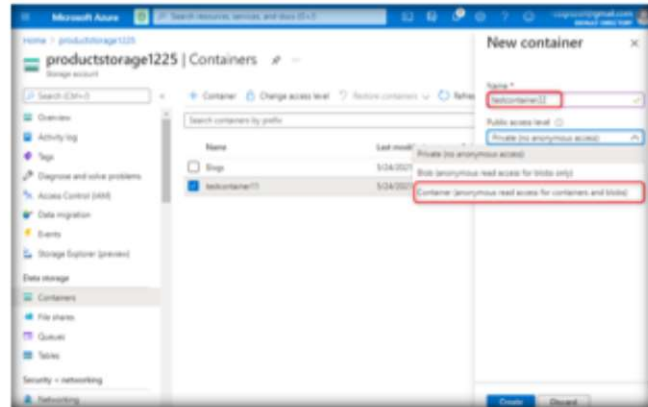


FIGURE 4.9.32: Entering Details in New Container Window

33. Click on the **Create** button.

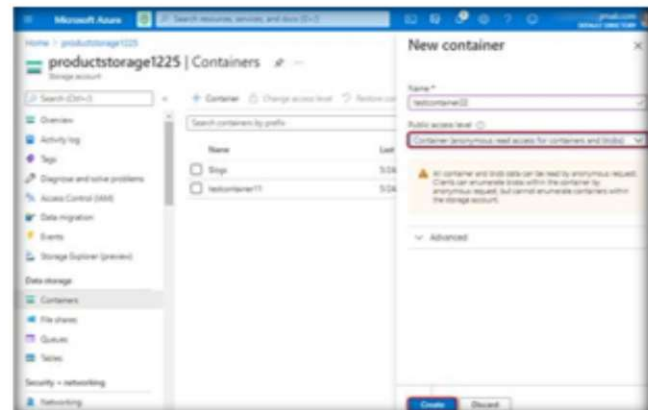


FIGURE 4.9.33: Creating Container with Anonymous Access

Module 04 – Data Security in Cloud

34. Now, **testcontainer22** has anonymous read access.

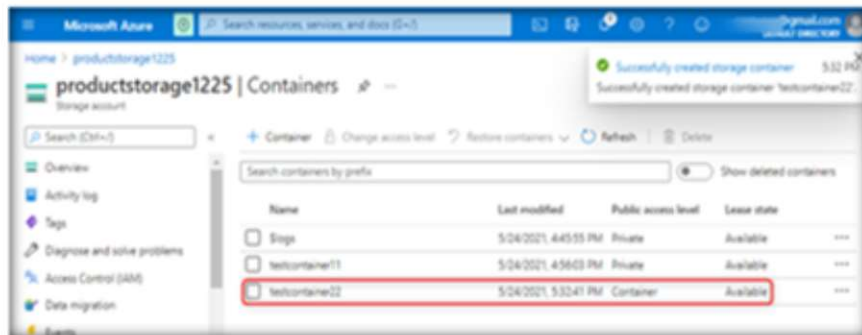


FIGURE 4.9.34: Successfully Created a Container Having Anonymous Read Access

35. Now, select and click on **testcontainer22**.

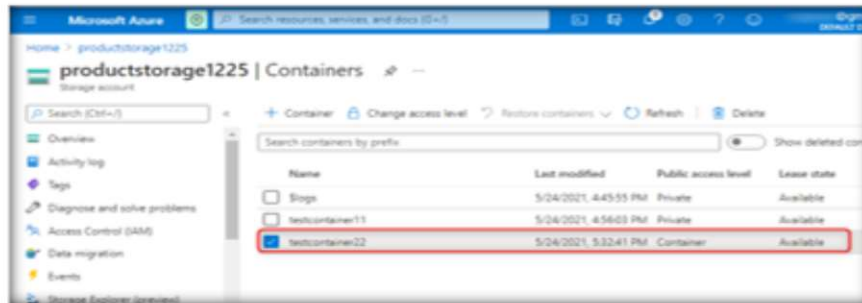


FIGURE 4.9.35: Selecting the Container with Public Access

36. In the **testcontainer22** container, click on the **Change access level** icon.

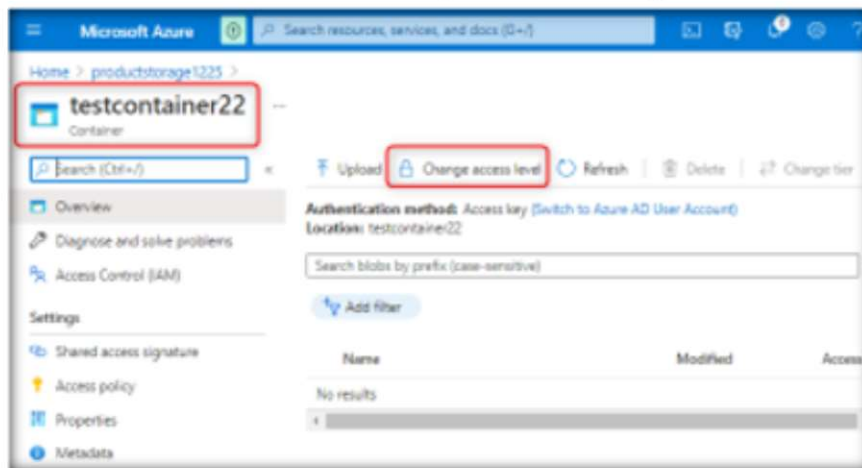


FIGURE 4.9.36: Changing Access Level

TASK 5

Changing Access Level of the Container from Public to Private

Module 04 – Data Security in Cloud

37. Click on the **Public access level** field dropdown, and then navigate and select **Private (no anonymous access)**.

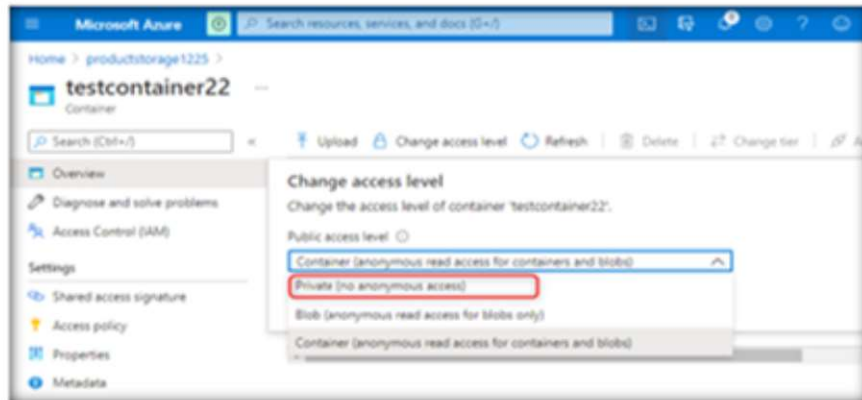


FIGURE 4.9.37: Selecting Private (no anonymous access) for the Container

38. Click on the **OK** button.

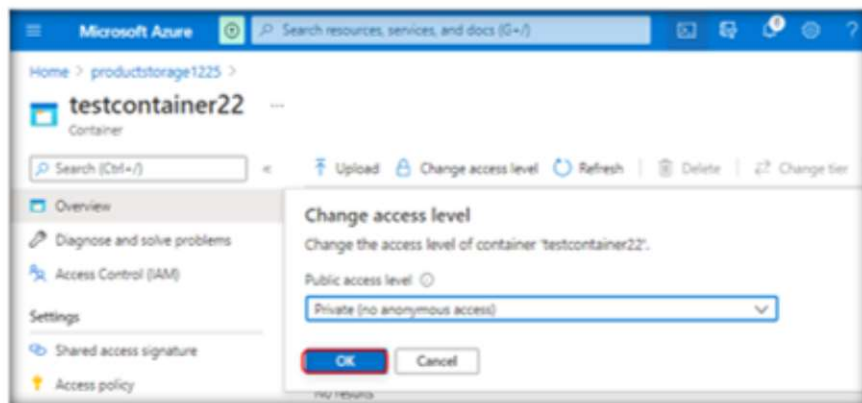


FIGURE 4.9.38: Confirming Change in Access Level

39. Click on **productstorage1225**.

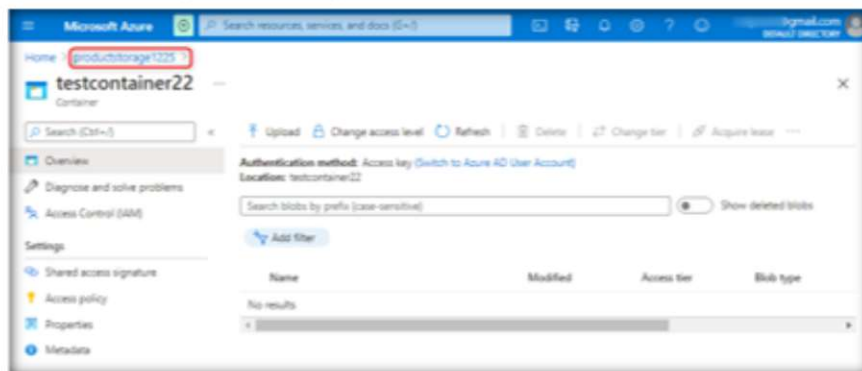


FIGURE 4.9.39: Going Back to Storage Account

40. You will observe that the public access level of **testcontainer22** is changed to **Private**.

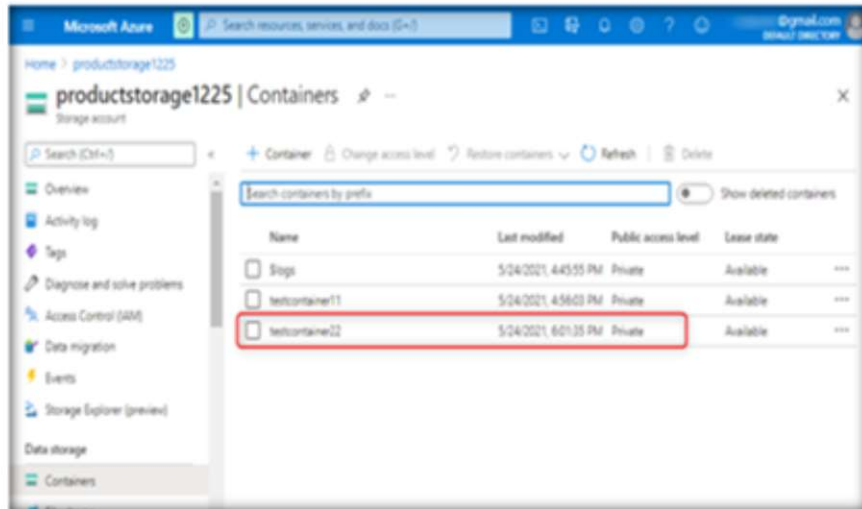


FIGURE 49.40: Checking the Change in Access Level

41. This way, a cloud security engineer can prevent anonymous access to blob containers by changing the access level from public to private.

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

42. Select the checkboxes for both the containers (**testcontainer11** and **testcontainer22**). Click on the **Delete** button at the top of the container window.

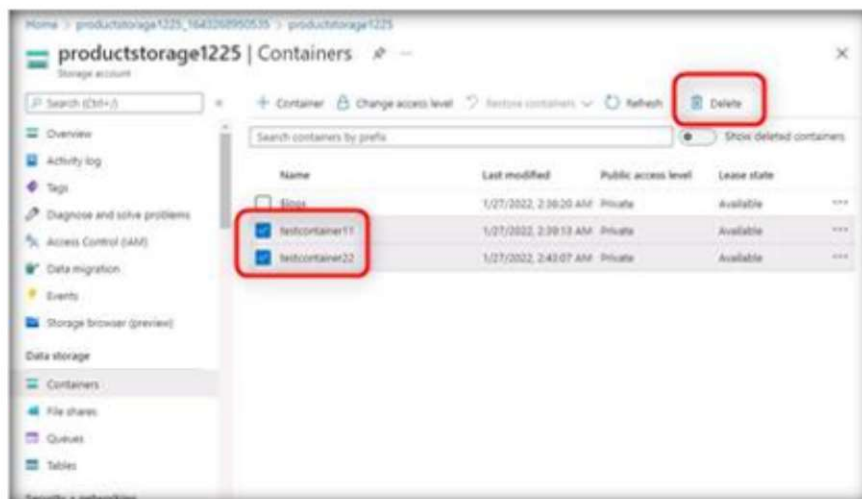


FIGURE 49.41: Deleting Container

Module 04 – Data Security in Cloud

43. Navigate to **Storage accounts** in the Azure portal. Select the checkbox for the storage account (**productstorage1225**) and click on the **Delete** button at the top of the **Storage accounts** window.

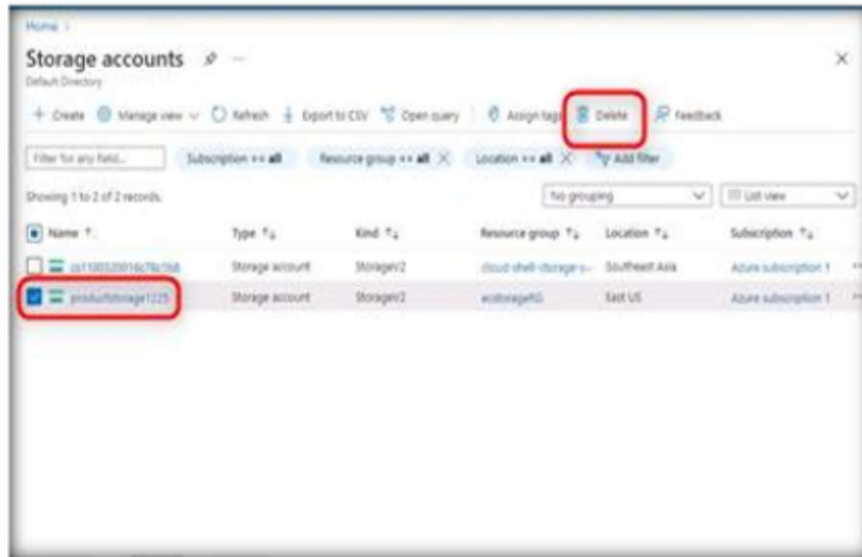


FIGURE 4.9.42: Deleting Storage Account

44. Navigate to **Resource groups** in the Azure portal. Click on the name of the resource group (**ecstorageRG**). Click on **Delete resource group** in the **Overview** window to delete the resource group.

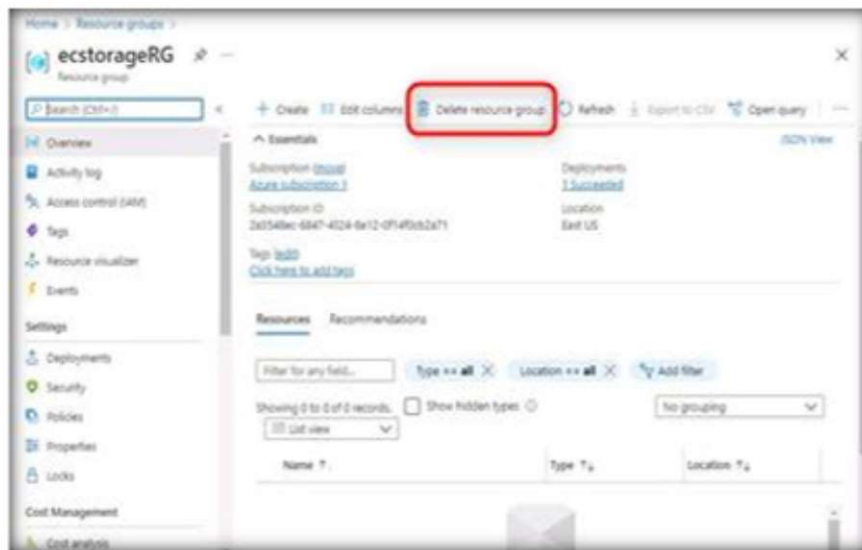


FIGURE 4.9.43: Deleting Resource Group

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.
